Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1

Dawn Cappelli
Andrew Moore
Randall Trzeciak
Timothy J. Shimeall

January 2009

This work was funded by

Software Engineering Institute | Carnegie Mellon

Table of Contents

INTRODUCTION

In 2005, the first version of the *Common Sense Guide to Prevention and Detection of Insider Threats* was published by Carnegie Mellon University's CyLab. The document was based on the insider threat research performed by CERT, primarily the *Insider Threat Study*[1] conducted jointly with the U.S. Secret Service. It contained a description of twelve practices that would have been effective in preventing or detecting malicious insider activity in 150 actual cases collected as part of the study. The 150 cases occurred in critical infrastructure sectors in the U.S. between 1996 and 2002.

A second edition of the guide was released in July of 2006. The second edition included a new type of analysis – by type of malicious insider activity. It also included a new section that presented a high-level picture of different types of insider threats: fraud, theft of confidential or proprietary information, and sabotage. also In addition, it contained new and updated practices based on new CERT insider threat research funded by Carnegie Mellon CyLab[2] and the U.S. Department of Defense Personnel Security Research Center.[3] Those projects involved a new type of analysis of the insider threat problem focused on determining high-level patterns and trends in the cases. Specifically, those projects examined the complex interactions, relative degree of risk, and unintended consequences of policies, practices, technology, insider psychological issues, and organizational culture over time.

This third edition of the Common Sense Guide once again reflects new insights from ongoing research at CERT. CyLab has funded the CERT Insider Threat Team to collect and analyze new insider threat cases on an ongoing basis. The purpose of this ongoing effort is to maintain a current state of awareness of the methods being used by insiders to commit their attacks, as well as new organizational issues influencing them to attack. This version of the guide includes new and updated practices based on an analysis of approximately 100 recent insider threat cases that occurred from 2003 to 2007 in the U.S.

In this edition of the guide, CERT researchers also present new findings derived from looking at insider crimes in a new way. These findings are based on CERT's analysis of 118 theft and fraud cases, which revealed a surprising finding. The intent of the research was to analyze cases of insider theft and insider fraud to identify patterns of insider behavior, organizational events or conditions, and technical issues across the cases. The patterns identified separated the crimes into two different classes than originally expected:

- Theft or modification of information for financial gain – This class includes cases where insiders used their access to organization systems either to steal

[1] See http://www.cert.org/insider_threat/study.html for more information on the *Insider Threat Study*.
[2] A report describing the MERIT model of insider IT Sabotage, funded by CyLab, can be downloaded at http://www.cert.org/archive/pdf/08tr009.pdf.
[3] A report describing CERT's insider threat research with the Department of Defense can be downloaded from http://www.cert.org/archive/pdf/06tr026.pdf.

information that they sold to outsiders, or to modify information for financial gain for themselves or others.

- Theft of information for business advantage - This class includes cases where insiders used their access to organization systems to obtain information that they used for their own personal business advantage, such as obtaining a new job or starting their own business.

It is important that organizations recognize the differences in the types of employees who commit each type of crime, as well as how each type of incident evolves over time: theft or modification for financial gain, theft for business advantage, IT sabotage, and miscellaneous (incidents that do not fall into any of the three above categories). This version of the guide presents patterns and trends observed in each type of malicious activity. There have been minor updates to the IT sabotage information in this guide; however, the most significant enhancements in this edition were made to the theft and modification sections.

Some new practices were added in this edition that did not exist in the second edition. In addition, every practice from the second edition has been modified—some significantly, others to a lesser degree—to reflect new insights from the past year's research at CERT. Case examples from the second edition were retained in this edition for the benefit of new readers. However, a *Recent Findings* section was included for all updated practices. It details recent cases that highlight new issues not covered in the previous edition of this guide.

What is Meant by "Insider Threat?"

CERT's definition of a malicious insider is

> A current or former employee, contractor, or business partner who
>
> - has or had authorized access to an organization's network, system, or data and
> - intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

Note that one type of insider threat is excluded from this guide: cases of espionage involving classified national security information.

The scope of insider threats has been expanding beyond the traditional threat posed by a current of former employee. Specifically, the CERT team has noted the following important new issues in the expanding scope of insider threat.

Collusion with outsiders: Insider threat has expanded beyond the organizational boundary. Half of the insiders who stole or modified information for financial gain were actually recruited by outsiders, including organized crime and foreign organizations or governments. It is important to pay close attention to the section of the guide titled "Theft or Modification of Information for Financial Gain" It will help you understand the types of employees who may be susceptible to recruitment.

Business partners: A recent trend noted by the CERT research team is the increase in the number of insider crimes perpetrated not by employees, but by employees of trusted business partners who have been given authorized access to their clients' networks, systems, and data. Suggestions for countering this threat are presented in Practice 1.

Mergers and acquisitions: A recent concern voiced to the CERT team by industry is the heightened risk of insider threat in organizations being acquired by another organization. It is important that organizations recognize the increased risk of insider threat both within the acquiring organization, and in the organization being acquired, as employees endure stress and an uncertain organizational climate. Readers involved in an acquisition should pay particular attention to most of the practices in this guide.

Cultural differences: Many of the patterns of behavior observed in CERT's insider threat modeling work are reflected throughout this guide. However, it is important for readers to understand that cultural issues could influence employee behaviors; those same behavioral patterns might not be exhibited in the same manner by people who were raised or spent extensive time outside of the U.S.

Issues outside the U.S: CERT's insider threat research is based on cases that occurred inside the United States. It is important for U.S. companies operating branches outside the U.S. to understand that, in addition to the cultural differences influencing employee behavior, portions of this guide might also need to be tailored to legal and policy differences in other countries.

Are insiders really a threat?

The threat of attack from insiders is real and substantial. The 2007 E-Crime Watch Survey™ conducted by the United States Secret Service, the CERT® Coordination Center (CERT/CC), Microsoft, and CSO Magazine,[4] found that in cases where respondents could identify the perpetrator of an electronic crime, 31% were committed by insiders. In

[4] http://www.cert.org/archive/pdf/ecrimesummary07.pdf

addition, 49% of respondents experienced at least one malicious, deliberate insider incident in the previous year. The impact from insider attacks can be devastating. One employee working for a manufacturer stole blueprints containing trade secrets worth $100 million, and sold them to a Taiwanese competitor in hopes of obtaining a new job with them.

Over the past several years, Carnegie Mellon University has been conducting a variety of research projects on insider threat. One of the conclusions reached is that insider attacks have occurred across all organizational sectors, often causing significant damage to the affected organizations. Examples of these acts include the following:

- "Low-tech" attacks, such as modifying or stealing confidential or sensitive information for personal gain.
- Theft of trade secrets or customer information to be used for business advantage or to give to a foreign government or organization.
- Technically sophisticated crimes that sabotage the organization's data, systems, or network.

Damages in many of these crimes are not only financial—widespread public reporting of the event can also severely damage the organization's reputation.

Insiders have a significant advantage over others who might want to harm an organization. Insiders can bypass physical and technical security measures designed to prevent unauthorized access. Mechanisms such as firewalls, intrusion detection systems, and electronic building access systems are implemented primarily to defend against external threats. However, not only are insiders aware of the policies, procedures, and technology used in their organizations, but they are often also aware of their vulnerabilities, such as loosely enforced policies and procedures or exploitable technical flaws in networks or systems.

CERT's research indicates that use of many widely accepted best practices for information security could have prevented many of the insider attacks examined. Part of CERT's research of insider threat cases entailed an examination of how each organization could have prevented the attack or at the very least detected it earlier. Previous editions of the Common Sense Guide identified existing best practices critical to the mitigation of the risks posed by malicious insiders. This edition identifies additional best practices based on new methods and contextual factors in recent cases, and also presents some new suggestions for countering insider threat based on findings that could not be linked to established best practices.

Based on our research to date, the practices outlined in this report are the most important for mitigating insider threats.

Who should read this report?

This guide is written for a diverse audience. Decision makers across an organization can benefit from reading it. Insider threats are influenced by a combination of technical, behavioral, and organizational issues, and must be addressed by policies, procedures, and technologies. Therefore, it is important that management, human resources, information technology, software engineering, legal, security staff, and the "owners" of critical data understand the overall scope of the problem and communicate it to all employees in the organization.

The guide outlines practices that should be implemented throughout organizations to prevent insider threats. It briefly describes each practice, explains why it should be implemented, and provides one or more actual case examples illustrating what could happen if it is not, as well as how the practice could have prevented an attack or facilitated early detection.

Much has been written about the implementation of these practices (a list of references on this topic is provided at the end of this guide). This report provides a synopsis of those practices, and is intended to convince the reader that someone in the organization should be given responsibility for reviewing existing organizational policies, processes, and technical controls and for recommending necessary additions or modifications.

Can insiders be stopped?

Insiders can be stopped, but stopping them is a complex problem. Insider attacks can only be prevented through a layered defense strategy consisting of policies, procedures, and technical controls. Therefore, management must pay close attention to many aspects of its organization, including its business policies and procedures, organizational culture, and technical environment. It must look beyond information technology to the organization's overall business processes and the interplay between those processes and the technologies used.

Acknowledgements

In sponsoring the *Insider Threat Study*, the U.S. Secret Service provided more than just funding for CERT's research. The joint study team, composed of CERT information security experts and behavioral psychologists from the Secret Service's National Threat Assessment Center, defined the research methodology and conducted the research that has provided the foundation for all of CERT's subsequent insider threat research. The community as a whole owes a debt of gratitude to the Secret Service for sponsoring and collaborating on the original study, and for permitting CERT to continue to rely on the valuable casefiles from that study for ongoing research. Specifically, CERT would like to thank Dr. Marisa Reddy Randazzo, Dr. Michelle Keeney, Eileen Kowalski, and Matt Doherty from the National Threat Assessment Center, and Cornelius Tate, David Iacovetti, Wayne Peterson, and Tom Dover, our liaisons with the Secret Service during the study.

The authors would also like to thank the CERT members of the *Insider Threat Study* team, who reviewed and coded cases, conducted interviews, and assisted in writing the study reports: Christopher Bateman, Casey Dunlevy, Tom Longstaff, David Mundie, Stephanie Rogers, Timothy Shimeall, Bradford Willke, and Mark Zajicek.

Since the *Insider Threat Study*, the CERT team has been fortunate to work with psychologists who have contributed their vast experience and new ideas to our work: Dr. Eric Shaw, a Visiting Scientist on the CERT Insider Threat team who has contributed to most of the CERT insider threat projects, Dr. Steven Band, former Chief of the FBI Behavioral Sciences Unit, who has provided expertise on psychological issues, and Dr. Lynn Fischer from the Department of Defense Personnel Security Research Center, who sponsored CERT's initial insider threat research and has continued to work with the CERT team on various insider threat projects.

The CERT team is extremely appreciative of the ongoing funding provided by CyLab. The impact of the insider threat research sponsored by CyLab has been enormous, within industry and government, and inside the U.S. as well as globally. CyLab has provided key funding that has enabled the CERT team to perform research for the benefit of all: government and industry, technical staff as well as management. Specifically, we would like to thank Pradeep Khosla, Don McGillen, and Linda Whipkey, who have been advocates for CERT's insider threat research since its inception, as well as Richard Power, Gene Hambrick, Virgil Gligor, and Adrian Perig, who the CERT team has had the pleasure of working with over the past year.

The CERT team has had assistance from various CyLab graduate students over the past few years. These students enthusiastically joined the team and devoted their precious time to the CERT insider threat projects: Akash Desai, Hannah Benjamin-Joseph, Christopher Nguyen, Adam Cummings, and Tom Carron. Special thanks to Tom, who is a current member of the CERT/CyLab insider threat team, and who willingly dropped everything he was doing over and over again to search the database for specific examples we needed to make this report as compelling as possible.

The Secret Service provided the 150 original casefiles for CERT's insider threat research. CyLab's research required identification and collection of additional case materials. The CERT team gratefully acknowledges the hard work and long hours, including many weekends, spent by Sheila Rosenthal, SEI's Manager of Library Services, assisting with this effort. Sheila was instrumental in obtaining the richest source materials available for more than 100 new cases used in the team's CyLab-sponsored research.

Finally, CERT would like to thank all of the organizations, prosecutors, investigators, and convicted insiders who agreed to provide confidential information to the team to enhance the research. It is essential to the community that all of the "good guys" band together and share information so that together we can keep employees happy, correct problems before they escalate, and use our technical resources and business processes to prevent malicious insider activity or detect the precursors to a devastating attack.

Patterns and Trends Observed by Type of Malicious Insider Activity

The CERT insider threat team has collected approximately 250 actual insider threat cases. One hundred ninety of those cases were analyzed in detail for this report. Because the remaining cases did not have sufficient information available or were still in the U.S. court system at the time of this publication, they have not yet been formally analyzed.

This section of the document presents trends and patterns observed in those cases by class of malicious insider activity:

- ***IT sabotage:*** cases in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of harming a specific individual, the organization, or the organization's data, systems, and/or daily business operations.

- ***Theft or modification for financial gain:*** cases in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of stealing or modifying confidential or proprietary information from the organization for financial gain.

- ***Theft or modification for business advantage:*** cases in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of stealing confidential or proprietary information from the organization with the intent to use it for a business advantage.

- ***Miscellaneous:*** cases in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of stealing confidential or proprietary information from the organization, not motivated by financial gain or business advantage.

The breakdown of the cases into those four categories is shown in Figure 1.

Figure 1. Breakdown of Insider Threat Cases[5]

Some cases fell into multiple categories. For example, some insiders committed acts of IT sabotage against their employers' systems, then attempted to extort money from them, offering to assist them in recovery efforts only in exchange for a sum of money. A case like that is categorized as both IT sabotage and theft or modification of information for financial gain. Four of the 190 cases were classified as theft for financial gain and IT sabotage. Another case involved a former vice president of sales copying a customer database and sales brochures from the organization before deleting them and taking another job. This case is classified as theft of information for business advantage and IT sabotage. One case was classified as theft for business advantage and IT sabotage. Finally, three cases where classified as IT Sabotage and Theft for Miscellaneous Reasons.

A breakdown of the cases depicting the overlap between categories is shown in Figure 2.

[5] 190 cases were analyzed for this report; however, some of the cases were classified as more than one type of crime.

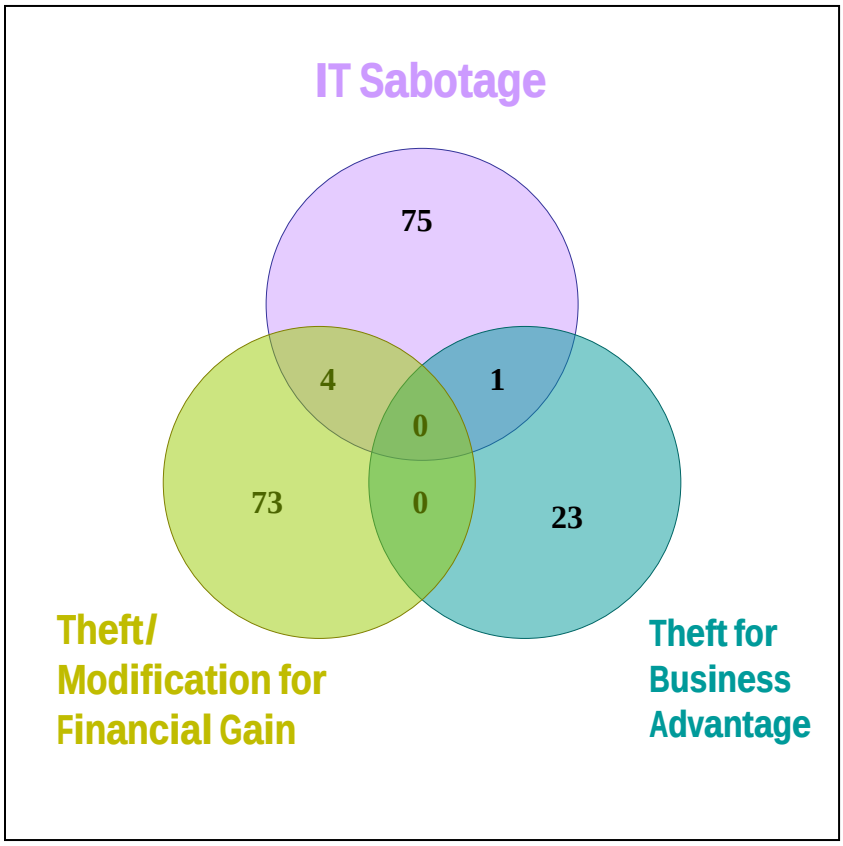

Figure 2. Overlap among the Insider Threat Classes[6]

Figure 3 shows the distribution of each type of case by critical infrastructure sector. It is interesting to note the differences among sectors. For instance, it is not surprising that theft of information for financial gain is most prominent in the Banking and Finance sector. However, it might be a bit unexpected to note that theft for financial gain in the Government sector is a close second, followed by Information Technology and Telecommunications.

Theft of information for business advantage, on the other hand, is highly concentrated in the IT and Telecommunications sector, with cases in the Banking and Finance sector second. Chemical and Hazardous Materials and the Defense Industrial Base were the only other two critical infrastructure sectors that experienced theft of information for business advantage.

The number of cases of insider IT sabotage in the IT sector is quite striking. The government sector was second in number of insider IT sabotage attacks. Note that the only two sectors to have experienced no insider IT sabotage attacks were Chemical and

[6] Seventeen of the cases were classified as "Miscellaneous Theft" cases, in which the motive was not for financial gain or business advantage. This figure does not depict those seventeen crimes.

Hazardous Materials and Emergency Services; every other sector experienced at least one attack.

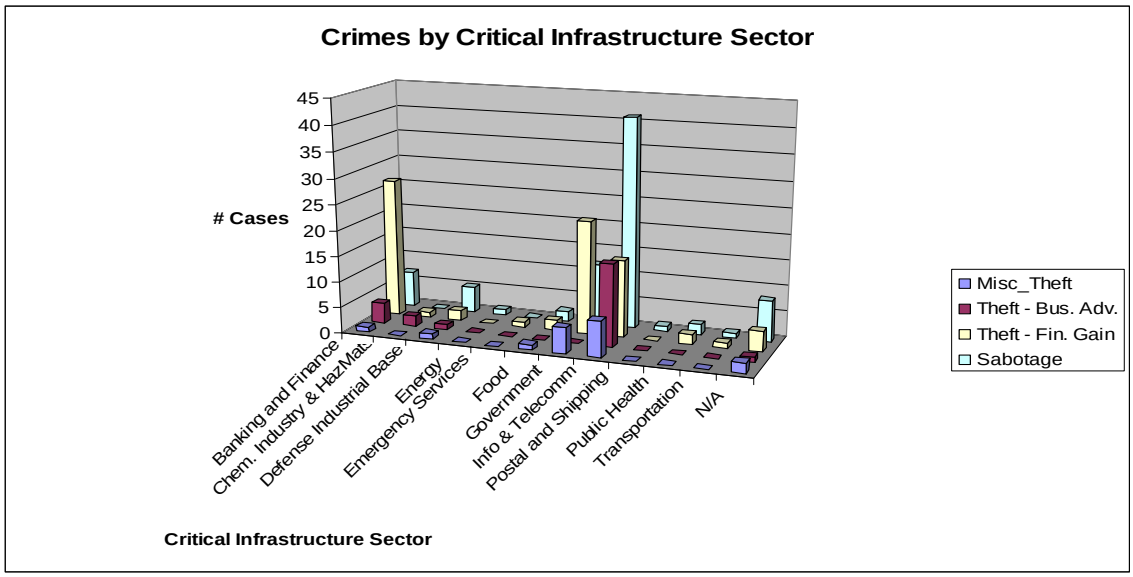

Figure 3. Distribution of Cases by Critical Infrastructure Sector

Insider IT Sabotage

In this report, insider IT sabotage cases are defined as follows: cases in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of harming a specific individual, the organization, or the organization's data, systems, and/or daily business operations.

CERT researchers analyzed 80 cases of IT sabotage that occurred in the United States between 1996 and 2007.

Who were the insiders?

The insiders who committed IT sabotage were primarily male and held highly technical positions, the majority hired with system administrator or privileged access. However, according to the U.S. Department of Labor Bureau of Labor Statistics, in 2007, 74% of all employees in computer and mathematical occupations were male.[7] Therefore, while it is useful to note that sabotage was typically committed by technically sophisticated employees, focusing attention only on male employees is probably not a logical conclusion. In addition, the majority of the insiders who committed IT sabotage were former employees.

Why did they do it?

Over half of the insiders were perceived as disgruntled, and most of them acted out of revenge for some negative precipitating event. Examples of negative events include termination, disputes with the employer, new supervisors, transfers or demotions, and dissatisfaction with salary increases or bonuses.

How did they attack?

The majority of the insiders who committed IT sabotage did not have authorized access at the time of their attack. Only 30% used their own username and password; 43% of them compromised an account. Twenty-four percent used another employee's username and password, and 16% used an unauthorized (backdoor) account they had created previously. They also used shared accounts, including some that had been overlooked in the termination process; 23% used system administrator or database administrator (DBA) accounts and 11% used other types of shared accounts, for instance testing accounts or training accounts.

Thirty-five percent used sophisticated technical means for carrying out their attacks. Commonly used technical methods included writing a script or program, such as a logic bomb, or creating a backdoor account for later use. Other technical mechanisms included planting a virus on customer computers, using password crackers, and installation of remote system administration tools.

[7] http://www.bls.gov/cps/cpsaat9.pdf

Approximately 30% took technical preparatory actions prior to the attack, particularly in cases where they anticipated termination. For example, they wrote, tested, and planted logic bombs, sabotaged backups, and created backdoor accounts. Most logic bombs were designed to delete massive amounts of data; however, at least one was designed to disrupt business operations surreptitiously, six months following the insider's termination. Some backdoor accounts were fairly obvious and could have been detected easily in an account audit, while others were well concealed. Most insiders used remote access, and carried out their attack outside of normal working hours.

How was it detected?

Most of the attacks were detected manually due to system failure or irregularity. Non-security personnel, including customers in almost 25% of the cases, often detected the attacks. Employees detecting the attacks included supervisors, coworkers, and security staff.

Observable concerning behaviors were exhibited by the insiders prior to setting up and carrying out their attack. Common behavioral precursors included conflicts with supervisors and coworkers (which were sometimes quite angry or violent), decline in performance, tardiness, or unexplained absenteeism. In some cases, management did not notice or ignored the problems. In other cases, sanctions imposed by the organization only increased the insider's concerning behaviors, rather than put an end to them.

How was the insider identified?

In most cases, system logs were used to identify the insider, including remote access logs, file access logs, database logs, application logs, and email logs. Most of the insiders took steps to conceal their actions; some insiders, knowing that the logs would be used for identification, attempted to conceal their actions by modifying the logs. In some cases, they modified the logs to implicate someone else for their actions.

What were the impacts?

In 68% of the cases, the organization suffered some type of business impact, such as inability to conduct business due to the system or network being down, loss of customer records, or inability to produce products due to damaged or destroyed software or systems.

Other negative consequences resulted from

- negative media attention
- forwarding management email containing private information, like strategic plans or plans of impending layoffs to customers, competitors, or employees
- exposure of personal information, like Social Security numbers
- web site defacements in which legitimate information was replaced with invalid or embarrassing content
- publication of confidential customer information on a public web site

In 28% of the cases, an individual was harmed. Examples of harm to individuals include threats, modification of evidence to falsely implicate supervisors or coworkers, and exposure of personal or private information.

For a more detailed description of insider IT sabotage, see *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures*, which can be downloaded at http://www.cert.org/archive/pdf/08tr009.pdf.

Theft or Modification for Financial Gain

In this report, insider theft or modification for financial gain cases are defined as follows: cases in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of stealing or modifying their employer's confidential or proprietary information for financial gain.

CERT researchers analyzed 77 cases of theft or modification for financial gain that occurred in the United States between 1996 and 2007. Seventy three cases involved only theft or modification for financial gain and four also involved IT sabotage.

Who were the insiders?

Only five of the insiders who committed crimes in this category were former employees; all others were current employees when they committed their illicit activity. Half of the insiders were male and half were female. The insiders committing this type of crime tended to occupy "lower-level,", non-technical positions in the organization. Their job duties included data entry and management of personally identifiable information (PII) or customer information (CI). For example, many of these insiders held data entry positions or were classified as clerks.

Why did they do it?

The primary motivation for all insiders in this category is financial gain. Insiders stole information to sell it, modified data to achieve financial benefits for themselves, friends, or family, or were paid by outsiders to modify information. Some insiders were motivated to provide additional income for their relatives, and a few insiders had large credit card debts or drug-related financial difficulties.

Most of these attacks were long, ongoing schemes; approximately one third of the incidents continued for more than one year. Of the short, quick compromises, half ended because the insider was caught quickly, and the other half ended because the crime was committed as the employee was leaving the organization or following termination.

The prevalence of collusion between the insiders in these cases and either people external to the organization or with other insiders is extremely high. Some cases involved collusion with both insiders and outsiders. In cases of insider theft for financial gain, the insider colluded with outsiders in two thirds of the cases, and one third of the cases involved collusion between the insider and someone else inside the organization. In those theft cases, an outsider recruited the insider to commit the crime in half of the cases. In less than one third of the cases, the insider acted alone.

A recurring pattern in the theft of information for financial gain cases includes an outsider recruiting an insider in a low-paying, non-technical position who has access to PII or CI. The insider steals the information; the outsider then pays the insider and uses the information to commit fraud or identity theft.

Some insiders were paid to modify data, for example credit histories. In some cases they were paid by people with poor credit histories, and in others by someone (like a car dealer) who would benefit from the beneficiaries' loan approvals. Other insiders were paid by external people to create false drivers licenses, to enter fake health care providers, and to generate false claims totaling significant amounts. Still others were paid to counterfeit federal identity documents.

Finally, some insiders were able to design and carry out their own modification scheme due to their familiarity with the organization's systems and business processes. For example, a payroll manager defrauded her employer of more than $300,000 by adding her husband to the payroll every week, generating a paycheck for him, then removing him immediately from the payroll system to avoid detection. Her crime was only discovered approximately one year after she left the company when an accountant noticed the unauthorized checks.

In cases of insider modification of information for financial gain, insiders colluded with an outsider in half of the cases, and almost half of the cases involved collusion between the insider and someone else inside the organization. In modification cases, an outsider recruited the insider to commit the crime in less than one third of the cases. In one third of the cases, the insider acted alone.

How did they attack?

Ninety five percent of the insiders stole or modified the information during normal working hours, and over 75% of the insiders used authorized access. Twenty five percent did not have authorized access when they committed their crime; all others were legitimate users. Five had system administrator or database administrator access and less than 15% had privileged access. Almost all of the insiders used only legitimate user commands to steal or modify the data. Only 16% of the crimes involved sophisticated technical techniques, like use of a script or program, creation of a backdoor account, or account compromise.

Eight-five percent of the insiders used their own usernames and passwords to commit their crimes. Slightly over 10% compromised someone else's account, two insiders used a computer left logged in and unattended by a coworker, one insider used a customer account, and one used a company-wide training account. In nine of the cases, the insider was able to compromise access to an account via social engineering methods. Some insiders used more than one account to carry out their crime.

Only two insiders took technical preparatory actions to set up their illicit activity. One insider enabled fraudulent medical care providers to be added to the database. Another disabled automatic notification of the security staff when a certain highly restricted function was used in the system, then used that function to conduct his fraudulent scheme.

How was it detected?

Only one of the insiders was detected due to network monitoring activities. Half were detected due to data irregularities, including suspicious activities in the form of bills, tickets, or negative indicators on individual's credit histories. The majority of the cases were detected by non-technical means, such as notification of a problem by a customer, law enforcement officer, coworker, informant, auditor, or other external person who became suspicious. In five cases, the insider was detected when the information was offered for sale directly to a competitor via email or posted online. Most of the malicious activity was eventually detected by multiple people. Over 50% of the cases were detected internally by non-IT security personnel, 26% by clients or customers of the organization, approximately 10% by customers, and 5% by competitors.

How was the insider identified?

In most cases, system logs were used to identify the insider, including database logs, system file change logs, file access logs, and others.

What were the impacts?

The theft or modification cases analyzed for this report affected not only the insiders' organizations, but also other innocent victims. For example, a check fraud scheme resulted in innocent people receiving collection letters due to fraudulent checks written against their account. Other cases involved insiders committing credit card fraud by abusing their access to confidential customer data. Other insiders subverted the justice system by modifying court records. Some cases could have very serious consequences – cases in which insiders created false official identification documents or drivers licenses for illegal aliens or others who could not obtain them legally. Similarly, one insider accepted payment to modify a database to overturn decisions denying asylum to illegal aliens, enabling them to remain in the U.S. illegally.

The insiders' organizations also suffered as a result of these crimes. Impacts included negative media attention as well as financial losses. One insider committed fraud against a state insurance fund for a total of almost $850,000, and another insider working for the same company was tied to almost $20 million in fraudulent or suspicious transactions. Another insider committed fraud against a federal agency for over $600,000. In a case involving both sabotage and fraud, an insider set himself up to benefit from the abrupt decline in his company's stock price when he deleted over 10 billion files on the company's servers, costing the organization close to $3 million in recovery costs.

Theft of Information for Business Advantage

In this report, cases involving theft of confidential or proprietary information are defined as follows: cases in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of stealing confidential or proprietary information from the organization with the intent to use it for a business advantage. While an argument can be made that this type of incident may ultimately be about money, these insiders had longer term ambitions, such as using the information to get a new job, to use in a new job with a competing business, or to start a competing business.

CERT researchers analyzed twenty-four cases of theft of confidential or proprietary information for business advantage that occurred in the United States between 1996 and 2007. Twenty-three cases involved only information theft and one also involved IT sabotage.

Who were the insiders?

In all of the cases analyzed, the insiders who stole confidential or proprietary information were male and 71% held technical positions. The remaining 29% occupied sales positions. Twenty-five percent were former employees; the other 75% were current employees when they committed their illicit activity. Interestingly, nearly 80% of the insiders had already accepted positions with another company or had started a competing company at the time of the theft.

Why did they do it?

By definition, all of these insiders committed the crime in order to obtain a business advantage. Some insiders stole the information to give them an immediate advantage at a new job. Others used the information to start a new, competing business. Almost all (95%) of the insiders resigned before or after the theft. Most (almost 70%) took place within three weeks of the insider's resignation.

In 25% of the cases, the insider gave the information to a foreign company or government organization. It is important to note that half of the theft for business advantage cases with the highest financial impact involved foreign organizations.

How did they attack?

Eighty-eight percent of the insiders had authorized access to the information when they committed the theft. The only insiders who did *not* have authorized access to the information they stole were former employees at the time of the crime. None of the insiders had privileged access, such as system administrator or database administrator access, that enabled them to commit the crime, although one former employee was given authorized access to do some additional work; he used that access to commit the theft. In other words, the widespread fear of system administrators using their privileged access to steal information was not evidenced in these cases.

The majority of these theft cases occurred quickly, spanning less than a one-month period. Less than one third of the insiders continued their theft over a longer period, half

of them stealing for a side business, and half to take to a new employer. Although most of the thefts occurred quickly, there often was significant planning by the insider. More than one third of the insiders had already created, or were planning to start, a new business while still working at the victim organization. Some of the insiders were deceptive about their plans when leaving the organization, either lying about future job plans or declining to reveal that they had already accepted another position. One insider created a side business as a vehicle for transferring trade secrets he stole from his current employer to a foreign-state-owned company. He concealed his connection to the side business by removing his name from the business article of incorporation and only using a post office box as the address for the company.

There was slightly less collusion in these theft cases than in the cases of theft or modification for financial gain, but the numbers are still significant. In approximately half of the cases, the insider colluded with at least one other insider to commit the crime. In some cases, the employee stole the information, resigned his position, then recruited other employees still at the original organization to steal additional information. These crimes were usually the insider's own idea; the insider was only recruited by someone outside the organization in less than 25% of the cases.

The majority of these crimes were committed during working hours, although a few insiders acted outside working hours. Very few (roughly 12%) used remote access, accessing their employers' networks from their homes or from another organization. Some insiders stole information using both remote access and access from within the workplace, and some acted both inside and outside normal working hours.

How was it detected?

Many of these incidents were detected by non-technical means, such as

- notification by a customer or informant,
- detection by law enforcement investigating the reports of the theft by victims,
- reporting of suspicious activity by co-workers, and
- sudden emergence of new competing organizations.

In one case, the victim organization became suspicious upon seeing a product strikingly similar to theirs at a competitor's booth at a trade show. In another, customers alerted the victim organization to the theft when the insider attempted to sell identical products and services to theirs on behalf of a new organization.

Twenty-five percent of the cases were detected by system administrators or IT security personnel while monitoring download logs or email logs.

How was the insider identified?

In most cases, system logs were used to identify the insider, including file access, database, and email logs.

What were the impacts?

Impacts on organizations included financial and other losses. It is extremely difficult to quantify the losses resulting from stolen trade secrets. In 38% of the cases, proprietary software or source code was stolen; an equal number of cases involved business plans, proposals, and other strategic plans; and a slightly smaller number involved trade secrets, such as product designs or formulas.

Finally, the insiders themselves sometimes suffered unanticipated consequences. Some insiders were surprised that their actions were criminal in nature, claiming that they created the information once, and could do it again, and therefore it was easier to simply take it with them when they left the organization. In one case, the insider committed suicide before he could be brought to trial.

Summary

Forty-five percent of the 176 cases analyzed for this report involved IT sabotage, 44% involved theft or modification of information for financial gain, and 14% involved theft or modification of information for business advantage.[8] However, although IT sabotage and theft or modification of information for financial gain were the most prevalent types of crime, the potential impacts of all three types of crime are serious. Therefore, organizations should consider whether each of these activities is a potential threat to them, and if so, consider the information in this report regarding those types of crimes carefully.

Furthermore, the authors of this report contend that insider IT sabotage is a threat to any organization that relies on an IT infrastructure for its business, regardless of the size or complexity of the configuration. Likewise, it is unlikely that many organizations can disregard insider theft of proprietary or confidential information as an insider threat. Therefore, it is recommended that all organizations consider the practices detailed in the remainder of this report for prevention of sabotage and information theft.

Table 1 provides a summary of the details surrounding the three types of insider crimes.

High-Level Comparison of Insider Threat Types

Potential threat of insider sabotage is posed by disgruntled technical staff following a negative work-related event. These insiders tend to act alone. While coworkers might also be disgruntled immediately following the negative event, most of them come to accept the situation. The potential for insider IT sabotage should be considered when there are ongoing, observable behavioral precursors preceding technical actions that are taken to set up the crime.

Data pertaining to theft or modification of information for financial gain and information theft for business advantage, on the other hand, suggest that organizations need to exercise some degree of caution with *all* employees. Current employees in practically any position have used legitimate system access to commit those types of crimes. In theft or modification for financial gain, there was also a high degree of collusion with both outsiders (primarily to market the stolen information or to gain benefit from its modification) and other insiders (primarily to facilitate the theft or modification). Collusion was less common, but still significant, in theft for business advantage. Crimes for financial gain were also more likely to be induced by outsiders than crimes for business advantage.

Of special note, however, is the fact that ninety-five percent of the employees who stole information for business advantage resigned before or after the theft. Therefore, extra caution should be exercised once the organization becomes aware of this type of information, either formally or via rumor. A balance of trust and caution should factor into the organization's policies, practices, and technology.

[8] Recall that some crimes fit into multiple categories. Also, cases of Miscellaneous theft were excluded from this calculation.

	Insider IT Sabotage	Insider Theft or Modification of Information for Financial Gain	Insider Theft of Information for Business Advantage
Percentage of crimes in CERT's case database	45%	44%	14%
Current or former employee?	Former	Current	Current
Type of position	Technical (e.g. system administrators or database administrators)	Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)	Technical (71%) - scientists, programmers, engineers Sales (29%)
Gender	Male	Fairly equally split between male and female	Male
Target	Network, systems, or data	Personally Identifiable Information or Customer Information	Intellectual Property (trade secrets) – 71% Customer Information – 33% [9]
Access used	Unauthorized access	Authorized access	Authorized access
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At work
Recruited by outsiders	None	Half recruited for theft; less than one third recruited for modification	Less than one fourth
Collusion	None	Almost half colluded with another insider in modification cases; 2/3 colluded with outsiders in theft cases	Almost half colluded with at least one insider; half acted alone

Table 1. Summary Comparison by Type of Insider Incident

[9] Some insiders stole more than one type of information.

How Can they be Stopped?

The methods of carrying out malicious insider activity varied by type of crime. The IT sabotage cases tended to be more technically sophisticated, while the theft or modification of information for financial gain and information theft for business advantage tended to be technically unsophisticated in comparison.

It is important that organizations carefully consider implementing the practices outlined in the remainder of this report to protect themselves from any of these malicious activities that pose a risk to them. Proactive technical measures need to be instituted and maintained at a constant level in order to prevent or detect technical preparatory actions. Good management practices need to be instituted and maintained in order to prevent insider threats, or recognize and react appropriately when indicators of potential insider threats are exhibited. Legal and contractual implications in the cases examined by CERT need to be understood and accounted for with employees, contractors, and partner organizations.

Too often, organizations allow the quality of their practices to erode over time because they seem to be less important than competing priorities if no malicious insider activity has been detected. One of the vulnerabilities posed by insiders is their knowledge of exactly this: the quality of their organization's defenses.

What if an Insider Attack Succeeds?

One pattern common to all of the cases is the importance of system logs in identifying the insider. Regardless of type of crime, system logs provide the evidence needed to take appropriate action. Since many technical insiders attempted to conceal their actions, sometimes by altering system logs, it is particularly important that organizations architect their systems to ensure the integrity of their logs.

In addition to protecting and defending against insider threats, it is also important that organizations are prepared to respond to an insider incident should one occur. Organizations frequently overlook insider threats when preparing incident response plans. Insider incidents need to be investigated carefully, since it is not always apparent who can be trusted and who cannot. In addition, organizations should make a proactive decision regarding forensics capability: if an insider incident occurs, will forensics be handled internally, or will an external forensics expert be hired? Some insider cases obtained by CERT could not be prosecuted because the organization did not properly handle system logs, and as a result they could not be used as evidence in prosecution.

The remainder of this document is structured around sixteen practices that could have been effective in preventing the insider incidents analyzed for this report, or at the very least, would have enabled early detection of the malicious activity.

Best Practices for the Prevention and Detection of Insider Threats

Summary of practices

The following sixteen practices will provide an organization defensive measures that could prevent or facilitate early detection of many of the insider incidents other organizations experienced in the hundreds of cases examined by CERT. Some of these practices have been updated from the previous version of the Common Sense Guide based on approximately 100 recent cases collected and examined since that version was published. Other practices are new ones added in this version. Each practice listed below is labeled as either *Updated* or *New*.

PRACTICE 1: *Consider threats from insiders and business partners in enterprise-wide risk assessments. (Updated).*

It is difficult for organizations to balance trusting their employees, providing them access to achieve the organization's mission, and protecting its assets from potential compromise by those same employees. Insiders' access, combined with their knowledge of the organization's technical vulnerabilities and vulnerabilities introduced by gaps in business processes, gives them the ability and opportunity to carry out malicious activity against their employer if properly motivated. The problem is becoming even more difficult as the scope of insider threats expands due to organizations' growing reliance on business partners with whom they contract and collaborate. It is important for organizations to take an enterprise-wide view of information security, first determining its critical assets, then defining a risk management strategy for protecting those assets from both insiders and outsiders.

NEW PRACTICE

PRACTICE 2: *Clearly document and consistently enforce policies and controls.*

Clear documentation and communication of technical and organizational policies and controls could have mitigated some of the insider incidents, theft, modification, and IT sabotage, in the CERT case library. Specific policies are discussed in this section of the report. In addition, consistent policy enforcement is important. Some employees in the cases examined by CERT felt they were being treated differently than other employees, and retaliated against this perceived unfairness by attacking their employer's IT systems. Other insiders were able to steal or modify information due to inconsistent or unenforced policies.

PRACTICE 3: *Institute periodic security awareness training for all employees.* (*Updated*)

A culture of security awareness must be instilled in the organization so that all employees understand the need for policies, procedures, and technical controls. All employees in an organization must be aware that security policies and procedures exist, that there is a good reason why they exist, that they must be enforced, and that there can be serious consequences for infractions. They also need to be aware that individuals, either inside or outside the organization, may try to co-opt them into activities counter to the organization's mission. Each employee needs to understand the organization's security

policies and the process for reporting policy violations. This section of the guide has been updated with important new findings relevant to recruitment of insiders by outsiders to commit crimes.

PRACTICE 4: *Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process*. (*Updated*)
Organizations should closely monitor suspicious or disruptive behavior by employees before they are hired, as well as in the workplace, including repeated policy violations that may indicate or escalate into more serious criminal activity. The effect of personal and professional stressors should also be considered. This section has been updated based on findings in 100 recent cases, particularly due to the high degree of internal and external collusion observed in these cases and the high incidence of previous arrests.

NEW PRACTICE
PRACTICE 5: *Anticipate and manage negative workplace issues.*
This section describes suggestions for organizations beginning with pre-employment issues and continuing through employment and with termination issues. For example, employers need to clearly formulate employment agreements and conditions of employment. Responsibilities and constraints of the employee and consequences for violations need to be clearly communicated and consistently enforced. In addition, workplace disputes or inappropriate relationships between co-workers can serve to undermine a healthy and productive working environment. Employees should feel encouraged to discuss work-related issues with a member of management or human resources without fear of reprisal or negative consequences. Managers need to address these issues when discovered or reported, before they escalate out of control. Finally, contentious employee terminations must be handled with utmost care, as most insider IT sabotage attacks occur following termination.

NEW PRACTICE
PRACTICE 6: *Track and secure the physical environment*.
While employees and contractors obviously must have access to organization facilities and equipment, most do not need access to all areas of the workplace. Controlling physical access for each employee is fundamental to insider threat risk management. Access attempts should be logged and regularly audited to identify violations or attempted violations of the physical space and equipment access policies. Of course, terminated employees, contractors, and trusted business partners should not have physical access to non-public areas of the organization facilities. This section details lessons learned from cases in the CERT case library in which physical access vulnerabilities allowed an insider to attack.

PRACTICE 7: *Implement strict password and account management policies and practices*. (*Updated*)
No matter how vigilant an organization is in trying to prevent insider attacks, if their computer accounts can be compromised, insiders have an opportunity to circumvent both manual and automated controls. Password and account management policies and practices should apply to employees, contractors, and business partners. They should

ensure that all activity from any account is attributable to the person who performed it. An anonymous reporting mechanism should be available and used by employees to report attempts at unauthorized account access, including potential attempts at social engineering. Audits should be performed regularly to identify and disable unnecessary or expired accounts. This section has been updated to reflect new account issues identified in 100 recent cases added to the CERT case library, many of them involving unauthorized access by trusted business partners.

PRACTICE 8: *Enforce separation of duties and least privilege*. (*Updated*)
If all employees are adequately trained in security awareness, and responsibility for critical functions is divided among employees, the possibility that one individual could commit fraud or sabotage without the cooperation of another individual within the organization is limited. Effective separation of duties requires the implementation of *least privilege*; that is, authorizing insiders only for the resources they need to do their jobs, particularly when they take on different positions or responsibilities within the organization. This section has been updated to reflect findings from recent cases involving collusion among multiple insiders.

NEW PRACTICE
PRACTICE 9: Consider insider threats in the software development life cycle.
Many insider incidents can be tied either directly or indirectly to defects introduced during the software development life cycle (SDLC). Some cases, such as those involving malicious code inserted into source code, have an obvious tie to the SDLC. Others, like those involving insiders who took advantage of inadequate separation of duties, have an indirect tie. This section of the report details the types of oversights throughout the SDLC that enabled insiders to carry out their attacks.

PRACTICE 10: *Use extra caution with system administrators and technical or privileged users*. (*Updated*)
System administrators and privileged users like database administrators have the technical ability and access to commit and conceal malicious activity. Technically adept individuals are more likely resort to technical means to exact revenge for perceived wrongs. Techniques like separation of duties or two-man rule for critical system administrator functions, non-repudiation of technical actions, encryption, and disabling accounts upon termination can limit the damage and promote the detection of malicious system administrator and privileged user actions. This section has been updated to include recent findings regarding technical employees who stole information for business advantage–to start their own business, take with them to a new job, or give to a foreign government or organization.

PRACTICE 11: *Implement system change controls*. (*Updated*)
A wide variety of insider compromises relied on unauthorized modifications to the organization's systems, which argues for stronger change controls as a mitigation strategy. System administrators or privileged users can deploy backdoor accounts, keystroke loggers, logic bombs, or other malicious programs on the system or network. These types of attacks are stealthy and therefore difficult to detect ahead of time, but

technical controls can be implemented for early detection. Once baseline software and hardware configurations are characterized, comparison of current configuration can detect discrepancies and alert managers for action. This section has been updated to reflect recent techniques used by insiders that could have been detected via change controls.

PRACTICE 12: *Log, monitor, and audit employee online actions*. (*Updated*)
If account and password policies and procedures are enforced, an organization can associate online actions with the employee who performed them. Logging, periodic monitoring, and auditing provide an organization the opportunity to discover and investigate suspicious insider actions before more serious consequences ensue. In addition to unauthorized changes to the system, download of confidential or sensitive information such as intellectual property, customer or client information, and personally identifiable information can be detected via data leakage tools. New findings detailed in this section can assist organizations in refining their data leakage prevention strategy, for example, in the weeks surrounding employee termination.

PRACTICE 13: *Use layered defense against remote attacks*. (*Updated*)
If employees are trained and vigilant, accounts are protected from compromise, and employees know that their actions are being logged and monitored, then disgruntled insiders will think twice about attacking systems or networks at work. Insiders tend to feel more confident and less inhibited when they have little fear of scrutiny by coworkers; therefore, remote access policies and procedures must be designed and implemented very carefully. When remote access to critical systems is deemed necessary, organizations should consider offsetting the added risk with requiring connections only via organization-owned machines and closer logging and frequent auditing of remote transactions. Disabling remote access and collection of organization equipment is particularly important for terminated employees. This section has been updated to include new remote attack methods employed by insiders in recent cases.

PRACTICE 14: *Deactivate computer access following termination*. (*Updated*)
When an employee terminates employment, whether the circumstances were favorable or not, it is important that the organization have in place a rigorous termination procedure that disables all of the employee's access points to the organization's physical locations, networks, systems, applications, and data. Fast action to disable all access points available to a terminated employee requires ongoing and strict tracking and management practices for all employee avenues of access including computer system accounts, shared passwords, and card control systems.

PRACTICE 15: *Implement secure backup and recovery processes*. (*Updated*)
No organization can completely eliminate its risk of insider attack; risk is inherent in the operation of any profitable enterprise. However, with a goal of organizational resiliency, risks must be acceptable to the stakeholders, and as such, impacts of potential insider attacks must be minimized. Therefore, it is important for organizations to prepare for the possibility of insider attack and minimize response time by implementing secure backup and recovery processes that avoid single points of failure and are tested periodically. This

section contains descriptions of recent insider threat cases in which the organization's lack of attention to incident response and organizational resiliency resulted in serious disruption of service to their customers.

NEW PRACTICE
PRACTICE 16: *Develop an insider incident response plan.*
Organizations need to develop an insider incident response plan to control the damage due to malicious insiders. This is challenging because the same people assigned to a response team may be among the most likely to think about using their technical skills against the organization. Only those responsible for carrying out the plan need to understand and be trained on its execution. Should an insider attack, it is important that the organization have evidence in hand to identify the insider and follow up appropriately. Lessons learned should used to continually improve the plan.

Practice 1: Consider threats from insiders and business partners in enterprise-wide risk assessments. (UPDATED)

Organizations need to develop a comprehensive risk-based security strategy to protect critical assets against threats from inside and outside, as well as trusted business partners who are given authorized insider access.

What to do?

It is not practical for most organizations to implement 100% protection against every threat to every organizational resource. Therefore, it is important to adequately protect critical information and other resources and not direct significant effort toward protecting relatively unimportant data and resources. A realistic and achievable security goal is to protect those assets deemed critical to the organization's mission from both external and internal threats. Unfortunately, organizations often fail to recognize the increased risk posed when they provide insider access to their networks, systems, or information to other organizations and individuals with whom they collaborate, partner, contract, or otherwise associate. The boundary of the organization's enterprise needs to be drawn broadly enough to include as insiders all people who have a privileged understanding of and access to the organization, its information, and information systems.

Risk is the combination of threat, vulnerability, and mission impact. Enterprise-wide risk assessments help organizations identify critical assets, potential threats to those assets, and mission impact if the assets are compromised. Organizations should use the results of the assessment to develop or refine the overall strategy for securing their networked systems, striking the proper balance between countering the threat and accomplishing the organizational mission.[10]

The threat environment under which the system operates needs to be understood in order to accurately assess enterprise risk. Characterizing the threat environment can proceed in parallel with the evaluation of vulnerability and impact. However, the sooner the threat environment can be characterized the better. The purpose of this guide is to assist organizations in correctly assessing the insider threat environment, organizational vulnerabilities that enable the threat, and potential impacts that could result from insider incidents, including financial, operational, and reputational.

Unfortunately, many organizations focus on protecting information from access or sabotage by those external to the organization and overlook insiders. Moreover, an information technology and security solution designed without consciously acknowledging and accounting for potential insider threats often leaves the role of protection in the hands of some of the potential threats—the insiders themselves. It is imperative that organizations recognize the potential danger posed by the knowledge and access of their employees, contractors, and business partners, and specifically address that threat as part of an enterprise risk assessment.

[10] See http://www.cert.org/nav/index_green.html for CERT research in Enterprise Security Management.

Understanding the vulnerability of an organization to a threat is also important, but organizations often focus too much on low-level technical vulnerabilities, for example, by relying on automated computer and network vulnerability scanners. While such techniques are important, our studies of insider threat have indicated that vulnerabilities in an organization's business processes are at least as important as technical vulnerabilities. Organizations need to manage the impact of threats rather than chase individual technical vulnerabilities. In addition, new areas of concern have become apparent in recent cases, including legal and contracting issues, as detailed in the "Recent Findings" section below.

Insider threats impact the integrity, availability, or confidentiality of information critical to an organization's mission. Insiders have affected the integrity of their organizations' information in various ways, for example by manipulating customer financial information or defacing their employers' web sites. They have also violated confidentiality of information by stealing trade secrets or customer information. Still others have inappropriately disseminated confidential information, including private customer information as well as sensitive email messages between the organization's management. Finally, insiders have affected the availability of their organization's information by deleting data, sabotaging entire systems and networks, destroying backups, and committing other types of denial-of-service attacks.

In the types of insider incidents mentioned above, current or former employees, contractors, or business partners were able to compromise their organizations' critical assets. It is important that protection strategies are designed focusing on those assets: financial data, confidential or proprietary information, and other mission critical systems and data.

Case Studies: What could happen if I don't do it?

One organization failed to protect extremely critical systems and data from internal employees. It was responsible for running the 911 phone-number-to-address lookup system for emergency services. An insider deleted the entire database and software from three servers in the organization's network operations center (NOC) by gaining physical access using a contractor's badge. The NOC, which was left unattended, was solely protected via physical security; all machines in the room were left logged in with system administrator access.

Although the NOC system administrators were immediately notified of the system failure via an automatic paging system, there were no automated failover mechanisms. The organization's recovery plan relied solely on backup tapes, which were also stored in the NOC. Unfortunately, the insider, realizing that the systems could be easily recovered, took all of the backup tapes with him when he left the facility. In addition, the same contractor's badge was authorized for access to the offsite backup storage facility, from which he next stole over fifty backup tapes.

Had an enterprise risk assessment been performed for this system prior to the incident, the organization would have recognized the criticality of the systems, assessed the threats and vulnerabilities, and developed a risk mitigation strategy accordingly.

Another insider was the sole system administrator for his organization. One day, he quit with no prior notice. His organization refused to pay him for his last two days of work, and he subsequently refused to give them the passwords for the administrator accounts for its systems. Over a period of three days, the insider modified the systems so that they could not be accessed by the employees, defaced the company web site, and deleted files. It is critical that organizations consider the risk they assume when they place all system administration power into the hands of a single employee.

Recent Findings:

Organizations are increasingly outsourcing critical business functions. As a result, people external to the organization sometimes have full access to the organization's policies, processes, information, and systems, access and knowledge previously only provided to employees of the organization. CERT's definition of insider, which originally encompassed current and former employees and contractors, had to be extended to include partners, collaborators, and even students associated with the organization.

One recent case involved an employee of a company that obtained a contract to set up a new wireless network for a major manufacturer. The insider was on the installation team and therefore had detailed knowledge of the manufacturer's systems. He was removed from the team by his employer, apparently under negative circumstances. However, he was able to enter the manufacturing plant and access a computer kiosk in the visitors' lobby. Based on his familiarity with the manufacturer's computer system and security, he was able to use the kiosk to delete files and passwords from wireless devices used by the manufacturer across the country. It was forced to remove and repair the devices, causing wide-scale shutdown of facilities and disruption of its processes.

This case highlights several new insider threat issues. First of all, an enterprise-wide risk assessment should have identified the ability to override security and obtain privileged access to the manufacturer's network from a publicly accessible kiosk. Second, the manufacturer's contract with the insider's organization should have instituted strict controls over employees added to or removed from the project. Specifically, organizations should consider provisions in their contracts that require advance notification by the contracted organization of any negative employment actions being planned against any employees who have physical and/or electronic access to the contracting organization's systems. The contracting organization could require a specified amount of time before the action occurs, in order to perform its own risk assessment for the potential threat posed to its own network, systems, or information.

Another recent incident indicates the need to have transaction verification built into supplier agreements. A computer help desk attendant employed by a military contractor created fake military email addresses on the military systems for which he was responsible. He then used those email addresses to request replacement parts for military equipment recalled by a major supplier. The supplier sent the replacement parts to the address specified in the emails, with the expectation that the original recalled products would be returned after the replacements had been received. The insider provided his

home address for the shipments, and never intended to return the original equipment. The insider received almost 100 shipments with a retail value of almost five million dollars and sold the equipment on eBay.

Another case reflects the complexity of defining the organizational perimeter and the scope of insider threats. The outside legal counsel for a high tech company was preparing to represent the company in civil litigation. The outside counsel was provided with documents containing company trade secrets, which were necessary to prepare the legal case. The legal firm had a contract with a document-imaging company for copying documents for its cases. An employee of the document-imaging company brought in his nephew to help him copy the trade secret documents due to the amount of work required. The nephew, a university student not officially on payroll, scanned the confidential documents using his uncle's work computer, then sent them to a hacker web site for posting. His goal was to help the hacker community crack the high tech company's premier product. Organizations need to carefully consider their enterprise information boundaries when assessing the risk of insider compromise, and use legal means for protecting their information once it leaves their control.

Practice 2: Clearly document and consistently enforce policies and controls. (NEW)

A consistent, clear message on organizational policies and controls will help reduce the chance that employees will inadvertently commit a crime or lash out at the organization for a perceived injustice.

What to do?

Policies or controls that are misunderstood, not communicated, or inconsistently enforced can breed resentment among employees and can potentially result in harmful insider actions. For example, multiple insiders in cases in the CERT database took intellectual property they had created to a new job, not realizing that they did not own it. They were quite surprised when they were arrested for a crime they did not realize they had committed.

Organizations should ensure the following with regard to their policies and controls:

- concise and coherent documentation, including reasoning behind the policy, where applicable
- fairness for all employees
- consistent enforcement
- periodic employee training on the policies, justification, implementation, and enforcement

Organizations should be particularly clear on policies regarding

- acceptable use of organization's systems, information, and resources
- ownership of information created as a paid employee or contractor
- evaluation of employee performance, including requirements for promotion and financial bonuses
- processes and procedures for addressing employee grievances

As individuals join the organization, they should receive a copy of organizational policies that clearly lays out what is expected of them, together with the consequences of violations. Evidence that each individual has read and agreed to the organization's policies should be maintained.

Employee disgruntlement was a recurring factor in insider compromises, particularly in the insider IT sabotage cases. The disgruntlement was caused by some unmet expectation by the insider. Examples of unmet expectations observed in cases include

- insufficient salary increase or bonus
- limitations on use of company resources
- diminished authority or responsibilities
- perception of unfair work requirements
- poor coworker relations

Clear documentation of policies and controls can help prevent employee misunderstandings that can lead to unmet expectations. Consistent enforcement can ensure that employees don't feel they are being treated differently from or worse than other employees. In one case, employees had become accustomed to lax policy enforcement over a long period of time. New management dictated immediate strict policy enforcement, which caused one employee to become embittered and strike out against the organization. In other words, policies should be enforced consistently across all employees, as well as consistently enforced over time.

Of course, organizations are not static entities; change in organizational policies and controls is inevitable. Employee constraints, privileges, and responsibilities change as well. Organizations need to recognize times of change as particularly stressful times for employees, recognize the increased risk that comes along with these stress points, and mitigate it with clear communication regarding what employees can expect in the future.

Case Studies: What could happen if I don't do it?

An insider accepted a promotion, leaving a system administrator position in one department for a position as a systems analyst in another department of the same organization. In his new position, he was responsible for information sharing and collaboration between his old department and the new one. The following events ensued:

- The original department terminated his system administrator account and issued him an ordinary user account to support the access required in his new position.
- Shortly thereafter, the system security manager at the original department noticed that the former employee's new account had been granted unauthorized system administration rights.
- The security manager reset the account back to ordinary access rights, but a day later found that administrative rights had been granted to it once again.
- The security manager closed the account, but over the next few weeks other accounts exhibited unauthorized access and usage patterns.

An investigation of these events led to charges against the analyst for misuse of the organization's computing systems. These charges were eventually dropped, in part because there was no clear policy regarding account sharing or exploitation of vulnerabilities to elevate account privileges. This case illustrates the importance of clearly established policies that are consistent across departments, groups, and subsidiaries of the organization.

There are many cases in the CERT library where an employee compromised an organization's information or system in order to address some perceived injustice:

- An insider planted a logic bomb in an organization's system because he felt that he was required to follow stricter work standards than his fellow employees.

- In reaction to a lower bonus than expected, an insider planted a logic bomb that would, he expected, cause the organization's stock value to go down, thus causing stock options he owned to increase in value.
- A network administrator who designed and controlled an organization's manufacturing support systems detonated a logic bomb to destroy his creation because of his perceived loss of status and control.
- A quality control inspector, who believed his employer insufficiently addressed the quality requirements of its product, supplied company confidential information to the media to force the company to deal with the problem.
- An insider, who was upset about his company's practice of cancelling insurance policies for policy holders who paid late, provided sensitive company information to the opposing lawyers engaged in a lawsuit against the company.

What these insiders did is wrong and against the law. Nevertheless, more clearly defined policies and grievance procedures for perceived policy violations might have avoided the serious insider attacks experienced by those organizations.

Practice 3: Institute periodic security awareness training for all employees. (UPDATED)

Without broad understanding and buy-in from the organization, technical or managerial controls will be short lived.

What to do?

All employees need to understand that insider crimes do occur, and there are severe consequences. In addition, it is important for them to understand that malicious insiders can be highly technical people or those with minimal technical ability. Ages of perpetrators range from late teens to retirement. Both men and women have been malicious insiders, including introverted "loners," aggressive "get it done" people, and extroverted "star players." Positions have included low-wage data entry clerks, cashiers, programmers, artists, system and network administrators, salespersons, managers, and executives. They have been new hires, long-term employees, currently employed, recently terminated, contractors, temporary employees, and employees of trusted business partners.

Security awareness training should encourage identification of malicious insiders by behavior, not by stereotypical characteristics. Behaviors of concern include

- threats against the organization or bragging about the damage one could do to the organization,
- association with known criminals or suspicious people outside of the workplace,
- large downloads close to resignation,
- use of organization resources for a side business, or discussions regarding starting a competing business with coworkers,
- attempts to gain employees' passwords or to obtain access through trickery or exploitation of a trusted relationship (often called "social engineering")

Managers and employees need to be trained to recognize social networking in which an insider engages other employees to join their schemes, particularly to steal or modify information for financial gain. Warning employees of this possibility and the consequences may help to keep them on the watch for such manipulation and to report it to management.

Social engineering is often associated with attempts either to gain physical access or electronic access via accounts and passwords. Some of the CERT cases reveal social engineering of a different type, however. In one recent case, a disgruntled employee placed a hardware keystroke logger on a computer at work to capture confidential company information. After being fired unexpectedly, the now former employee tried to co-opt a non-technical employee still at the company to recover the device for him. Although the employee had no idea the device was a keystroke logger, she was smart enough to recognize the risk of providing it to him and notified management instead. Forensics revealed that he had removed the device and transferred the keystrokes file to his computer at work at least once before being fired.

Training programs should create a culture of security appropriate for the organization and include all personnel. For effectiveness and longevity, the measures used to secure an organization against insider threat need to be tied to the organization's mission, values, and critical assets, as determined by an enterprise-wide risk assessment. For example, if an organization places a high value on customer service quality, it may view customer information as its most critical asset and focus security on protection of that data. The organization could train its members to be vigilant against malicious employee actions, focusing on a number of key issues, including

- detecting and reporting disruptive behavior by employees (see Practice 4)
- monitoring adherence to organizational policies and controls (see Practices 2 and 11)
- monitoring and controlling changes to organizational systems (e.g., to prevent the installation of malicious code) (see practices 9 and 11)
- requiring separation of duties between employees who modify customer accounts and those who approve modifications or issue payments (see Practice 8)
- detecting and reporting violations of the security of the organization's facilities and physical assets (see Practice 6)
- planning for potential incident response proactively (see Practice 16)

Training on reducing risks to customer service processes would focus on

- protecting computer accounts used in these processes (see Practice 7)
- auditing access to customer records (see Practice 12)
- ensuring consistent enforcement of defined security policies and controls (see practice 2)
- implementing proper system administration safeguards for critical servers (see practices 10, 11, 12, and 13)
- using secure backup and recovery methods to ensure availability of customer service data (see Practice 15)

Training content should be based on documented policy, including a confidential means of reporting security issues. Confidential reporting allows reporting of suspicious events without fear of repercussions, thereby overcoming the cultural barrier of whistle blowing. Employees need to understand that the organization has policies and procedures, and that managers will respond to security issues in a fair and prompt manner.

Employees should be notified that system activity is monitored, especially system administration and privileged activity. All employees should be trained in their personal responsibility, such as protection of their own passwords and work products. Finally, the training should communicate IT acceptable use policies.

Case Studies: What could happen if I don't do it?

The lead developer of a critical production application had extensive control over the application source code. The only copy of the source code was on his company-provided laptop; there were no backups performed, and very little documentation existed, even

though management had repeatedly requested it. The insider told coworkers he had no intention of documenting the source code and any documentation he did write would be obscure. He also stated that he thought poorly of his managers because they had not instructed him to make backup copies of the source code.

A month after learning of a pending demotion, he erased the hard drive of his laptop, deleting the only copy of the source code the organization possessed, and quit his job. It took more than two months to recover the source code after it was located by law enforcement in encrypted form at the insider's home. Another four months elapsed before the insider provided the password to decrypt the source code. During this time the organization had to rely on the executable version of the application, with no ability to make any modifications. If the insider's team members had been informed that the security and survivability of the system was their responsibility, and if they had been presented with a clear procedure for reporting concerning behavior, they might have notified management of the insider's statements and actions in time to prevent the attack.

Another insider case involved a less technically sophisticated attack, but one that could have been avoided or successfully prosecuted if proper policies and training had been in place. Four executives left their firm to form a competing company. A few days before they left, one of them ordered a backup copy of the hard drive on his work computer, which contained customer lists and other sensitive information, from the external company that backed up the data. The company also alleged that its consulting services agreement and price list were sent by email from the insider's work computer to an external email account registered under his name. The insiders, two of whom had signed confidentiality agreements with the original employer, disagreed that the information they took was proprietary, saying that it had been published previously. Clear policies regarding definition of proprietary information and rules of use could have prevented the attack or provided a clearer avenue for prosecution.

Recent Findings

A striking finding in recent cases is that in over two thirds of the 31 cases of theft for financial gain, the insider was recruited to steal by someone outside the organization. In many of these cases, the insider was taking most of the risk while receiving relatively small financial compensation. The outsider was often a relative of the insider or an acquaintance who realized the value of exploiting the insider's access to information. One manager of a hospital's billing records gave patients' credit card information to her brother, who used it for online purchases shipped to his home address. Another insider in the human resources department for a federal government organization gave employee personally identifiable information (PII) to her boyfriend who used it to open and make purchases on fraudulent credit card accounts. As in CERT's previous research, outsiders (e.g., car salesmen) continue to convince insiders to "improve" the credit histories of individuals trying to obtain loans.

Organizations should educate employees on their responsibilities for protecting the information with which they are entrusted and the possibility that unscrupulous individuals could try to take advantage of their access to that information. Such

individuals may be inside or outside, the organization. In almost half of the cases of modification of information for financial gain, the insider recruited at least one other employee in the company to participate in the scheme, possibly as a means to bypass separation of duty restrictions, or to ensure that coworkers wouldn't report suspicious behavior. In one recent case, several bank janitorial employees stole customer information while working, changed the customer addresses online, opened credit cards in their names, purchased expensive items using the cards, and drained their bank accounts. Employees should be regularly reminded about procedures the company has in place for anonymously reporting suspicious coworker behavior, or attempts of recruitment by individuals inside or outside the organization.

Employees need to be educated about the confidentiality and integrity of the company's information, and that compromises will be dealt with harshly. Insiders sometimes did not understand this, viewing information as being their own property rather than the company's; for example, customer information developed by a sales person or software developed by a programmer.

There are also recent cases in which technical employees sold their organization's intellectual property because of dissatisfaction with their pay, and others who gave the information to reporters and lawyers over dissatisfaction with the organization's practices. Signs of disgruntlement in cases like those often appear well before the actual compromise. Such attacks can be prevented if managers and coworkers are educated to recognize and report behavioral precursors indicating potential attacks.

Practice 4: Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process. (UPDATED)

One method of reducing the threat of malicious insiders is to proactively deal with suspicious or disruptive employees.

What to do?

An organization's approach to reducing the insider threat should start in the hiring process by performing background checks and evaluating individuals based on the information received. Background checks should investigate previous criminal convictions, include a credit check, verify credentials and past employment, and include discussions with prior employers regarding the individual's competence and approach to dealing with workplace issues. Thirty percent of the insiders who committed IT sabotage had a previous arrest history, including arrests for violent offenses (18%), alcohol or drug related offenses (11%), and non-financial/fraud-related theft offenses (11%).[11] The relatively high frequency of previous criminal arrests underscores the need for background checks. These proactive measures should not be punitive in nature; rather, the individual should be indoctrinated into the organization with appropriate care. In addition, this information should be used as part of a risk-based decision process in determining whether or not it is appropriate to give the new employee access to critical, confidential, or proprietary information or systems.

Background checks should be required for all potential employees, including contractors and subcontractors. In one recent case, an organization employed a contractor to perform system administration duties. The hiring organization was told by the contractor's company that a background check had been performed on him. The contractor later compromised the organization's systems and obtained confidential data on millions of their customers. During the investigation it was discovered that the contractor had a criminal history for illegally accessing protected computers.

Organizations should invest time and resources in training supervisors to recognize and respond to inappropriate or concerning behavior in employees. In some cases, less serious but inappropriate behavior was noticed in the workplace but not acted on because it did not rise to the level of a policy violation. However, failure to define or enforce security policies in some cases emboldened the employees to commit repeated violations that escalated in severity, with increasing risk of significant harm to the organization. It is important that organizations consistently investigate and respond to all rule violations committed by employees.

Given that financial gain is a primary motive for much insider theft or modification of information for financial gain, organizations should monitor indications by employees of possible financial problems or unexplained financial gain. Sudden changes in an employee's financial situation, including increasing debt or expensive purchases, may be indicators of potential insider threat.

---

[11] See "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," http://www.cert.org/archive/pdf/insidercross051105.pdf

Policies and procedures should exist for employees to report concerning or disruptive behavior by coworkers. While frivolous reports need to be screened, all reports should be investigated. If an employee exhibits suspicious behavior, the organization should respond with due care. Disruptive employees should not be allowed to migrate from one position to another within the enterprise, evading documentation of disruptive or concerning activity. Threats, boasting about malicious acts or capabilities ("You wouldn't believe how easily I could trash this net!"), and other negative sentiments should also be treated as concerning behavior. Many employees will have concerns and grievances from time to time, and a formal and accountable process for addressing those grievances may satisfy those who might otherwise resort to malicious activity. In general, any employee experiencing difficulties in the workplace who has access to critical information assets should be aided in the resolution of those difficulties.

Once concerning behavior is identified, several steps may aid an organization in managing risks of malicious activity. First, the employee's access to critical information assets should be evaluated. His or her level of network access should also be considered. Logs should be reviewed to carefully review recent online activity by the employee. While this is done, the organization should provide options to the individual for coping with the behavior, perhaps including access to a confidential employee assistance program.

Case Studies: What could happen if I don't do it?

A system administrator was hired to run the engineering department for an organization and three months later was named as the lead for a major new project. He then began to bully his coworkers and was taken off the project a month after it started. Less than two months after that, he was terminated for poor performance and conduct. Customers had complained that he was rude and coworkers said that he thought he was better than everyone else. His superiors realized that he was not as good technically as they had originally believed and suspected that he was attempting to hide that fact by criticizing others. The company did provide counseling, but he resented it.

Almost two months after his termination, the insider obtained a system administrator account password from a female employee, still with the company, with whom he'd had a relationship. Using this password, the insider was able to hide the project folder on the server that was needed the next day for an important customer demonstration. Although the company did employ standard recommendations in handling this insider, he still managed to sabotage the company's system. This case highlights the potential danger presented by some social relationships between terminated insiders and employees still working for the company.

Another insider, working as a vice president for engineering and responsible for oversight of all software development in the company, was engaged in a long-running dispute with higher management. This dispute was characterized by verbal attacks by the insider and statements to colleagues about the degree of upset he had caused to management. The insider engaged in personal attacks once or twice a week and on one occasion, in a

restaurant, screamed personal attacks at the CEO of the company. A final explosive disagreement prompted the insider to quit.

When no severance package was offered, he copied a portion of a product under development to removable media, deleted it from the company's server, and removed the recent backup tapes. He then offered to restore the software in exchange for $50,000. He was charged and convicted of extortion, misappropriation of trade secrets, and grand theft. However, the most recent version of the software was never recovered. If the organization had recognized the warning of the earlier disruptive behavior and acted to secure assets from his access, substantial losses could have been avoided.

Recent Findings

CERT's analysis of insider information theft and modification cases revealed significant differences depending on whether the information was sold to or modified for outsiders, or used for the insider's own personal business advantage.

When financial gain was the motive, crimes tended to involve theft or modification of small amounts of data (e.g., social security numbers) repeatedly over long periods of time. Out of the 52 cases of modification for financial gain analyzed, almost half of the incidents continued for more than one year, and almost 90% continued for more than one month. This suggests that for most such crimes there is ample time to catch the insider in the act while still employed by the company. Some of the insiders had personal stressors that may have influenced their actions, including family medical problems, substance abuse, financial difficulties, and physical threats by outsiders, but further analysis is required to determine the prevalence of these types of stressors across all of these types of cases.

Insiders may have also been influenced by professional stressors, including financial compensation issues, problems with supervisor, hostile working environment, and layoffs. One system administrator planted a logic bomb designed to wipe out data on seventy company servers after finding out about planned layoffs due to reorganization. Even after surviving the downsizing, the insider refined the logic bomb and set it to go off over a year later. Fortunately, other IT personnel discovered the logic bomb while investigating a system problem and neutralized the destructive code.

When business advantage is the motive, crimes tend to involve much larger amounts of data (e.g., proprietary source code) and often occur within three weeks of the insider's resignation. However, theft for business advantage often involves significant planning well before the theft in which the insider becomes more curious about aspects of the information (e.g., software modules) outside of his area of responsibility. In over one third of the 24 cases analyzed, the insider had already created or was planning to start his own business while still working for the victim organization. Many were deceptive about their reasons for leaving the organization, even while working out the details with competing organizations for the transfer of stolen information. Two scientists formed a competing business for stealing their company's trade secrets and selling them to a Chinese state-owned company. They used their company as the vehicle for the transfer of

the information, and concealed their association with the company by removing their names from the business's articles of incorporation.

Both types of theft and modification of information had a high rate of collusion with both insiders and outsiders. This behavior, if detected, provides an opportunity for an organization to recognize a higher risk of insider threat and act accordingly. Secretive meetings among employees and obvious attempts to deceive the organization about outside business relationships are of concern. Anonymous means for reporting coworker suspicions should be in place and communicated to employees. Since over two thirds of the 24 cases of theft for business advantage took place within three weeks of the insider's resignation, the organization should review the logs for and confront the terminating employee regarding any recent large downloads, making clear the individual's legal responsibilities and constraints regarding the organization's intellectual property.

Practice 5: Anticipate and manage negative workplace issues (NEW)

Clearly defined and communicated organizational policies for dealing with employee issues will ensure consistent enforcement and reduce risk when negative workplace issues arise.

What to do?

Beginning with the first day of employment, an employee needs to be made aware of organizational practices and policies for acceptable workplace behavior, dress code, acceptable usage policies, working hours, career development, conflict resolution, and myriad other workplace issues. The existence of such policies alone is not enough. New employees and veteran employees alike all need to be aware of the existence of such policies and the consequences for violations. Consistent enforcement of the policies is essential to maintain the harmonious environment of the organization. When employees see inconsistent enforcement of polices, it quickly leads to animosity within the workplace. In many of the cases analyzed, inconsistent enforcement or perceived injustices within organizations led to insider disgruntlement. Coworkers often felt that "star-performers" were above the rules and received special treatment. Many times that disgruntlement led the insiders to commit IT sabotage or theft of information.

When employees have issues, whether justified or not, they need an avenue within the organization to seek assistance. Employees need to be able to openly discuss work-related issues with a member of management or human resources without the fear of reprisal or negative consequences. When employee issues arise because of outside issues, including financial and personal stressors, it can be helpful to use a service such as an employee assistance program. These programs offer confidential counseling to assist employees, allowing them to restore their work performance, health, or general well being. If insiders who committed theft or modification of information for financial gain had access to employee assistance programs, they may have found an alternative way to deal with the financial and personal stressors that appear to be a motivating factor in the crimes.

It is imperative that employees are aware of and formally sign off on intellectual property agreements and non-compete agreements with the organization. It is important that they are reminded of those agreements at the time of termination. There should be no ambiguity over who owns intellectual property developed as an employee of the organization. Many of the insiders who committed theft of information claimed to not know it was a violation of company policy when they took customer lists, pricing sheets, and even source code with them upon termination.

Finally, the termination process should include a step to retrieve all organization property from the terminating employee. Employees should be required to return all property, including computers and accessories, software and hardware, organizational confidential information, source code and compiled code, PDAs, removable media, and any other items that contain sensitive, confidential, or intellectual property owned by the organization. Organizations should consider showing employees the signed copy of the

intellectual property agreement and non-compete agreement and explaining the consequences for violating those policies.

Case Studies: What could happen if I don't do it?

In one case, an insider was a subcontractor working for an organization that handled state government employee health insurance claims. Using the medical identity number of an unsuspecting psychologist, the insider changed the name and address associated with the psychologist to a co-conspirators name and address. The insider proceeded to file fake claims and send the payments to the bogus addresses. Auditors discovered the scheme when they began questioning why a psychologist was submitting payment claims for treating broken bones and open wounds, and administering chemotherapy. They also noticed that the name associated with the psychologist was the name of one of their subcontractors. During the investigation it was determined that the insider had a criminal history for fraud and that the subcontracting organization probably did not perform a background check prior to hiring.

In a second case, a female employee who was a database administrator and project manager became increasingly disgruntled when her male coworkers began to override her technical decisions where she was the expert. She filed complaints with HR over what she considered a hostile work environment, but nothing was done about it. After she filed a complaint against her supervisor, her performance reviews, which had been stellar, went downhill. Her supervisor then demoted her by removing her project management responsibilities. Again she complained, but her supervisor started filing complaints against her for failure to follow instructions.

She next filed a complaint with the EEOC for discrimination based on her national origin (India), race (Asian, Indian), and gender (female). She eventually resigned because she was frustrated by the organization's lack of responsiveness to her complaints. After resignation, she found out her grievance against the organization had been denied. The last straw was when she found out that the organization only forwarded her negative performance reviews to the new organization where she was now employed.

She connected from her computer at home to her previous organization. She used another employee's username and password to log in to the system. Next she entered a critical system using a DBA account, which had not been changed since she resigned, and deleted critical data from the system. She deleted two weeks' worth of data used to determine promotions, transfers, disability claims, and caused the system to crash.

Practice 6: Track and secure the physical environment (NEW)

Although organizations are becoming more reliant on electronic communication and online transactions to do business, it is still essential that they track and secure the physical environment against internal and external threats.

What to do?

First and foremost, an organization must protect its most critical asset: its employees. This process begins by ensuring the office environment is free from occupational hazards and threats to employees from outsiders. While planning for the security of the physical environment, the organization should take into consideration the space inside the office walls as well as the perimeter of the building, including lobbies, elevators, stairwells, and parking areas. If an organization can keep unauthorized people out of the facility, they will add an extra layer to the desired security in-depth model.

Likewise, physical security can lend another layer of defense against terminated insiders who wish to regain physical access to attack. Just as with electronic security, however, former employees have been successful in working around their organizations' physical security measures. Commonly used physical security mechanisms, some that were effective and others that were inadequate in some of the cases examined by CERT, were as follows:

- Maintaining a physical security presence on the facilities at all times. Some of the former employees in the cases examined by CERT had to go to extra lengths to carry out their crime due to security guards on duty around the clock. For example, at least one terminated insider lied to the night shift security guard, who had not been told of the termination, about forgetting his badge. However, it is likely that other former insiders were deterred from malicious actions by those same guards.
- Requiring all employees, contractors, customers, and vendors to have a company issued badge and requiring the use of that badge to navigate throughout the facility. One employee in the CERT case library had to obtain a badge from a former contractor, used that badge to obtain physical access to an area of the facility for which he was not authorized after hours, then sabotaged the computers in the network operations center. Another former employee "piggy backed" behind another employee who had a badge to obtain after hours access to the facility. However, once again, these measures probably would deter a less motivated insider from carrying out a crime.
- Using alarms to deter and alert when unauthorized individuals enter an organization's facility. The CERT library contains no cases in which insiders circumvented alarms.
- Using closed circuit cameras to record the entry, exit, and critical operations at the facility. Some of the insiders in the CERT case library were successfully identified and convicted through use of closed circuit cameras or video surveillance.

Once the physical perimeter is as secure as possible, the organization should devote adequate resources to protecting the critical infrastructure, ensuring resiliency of operation. An infrastructure security strategy should begin by defining which assets are critical to the operation of the organization. These assets should be consolidated into a central computing facility with limited access to the physical space. Access control to the facility should be clearly defined and changes made as employees are hired and terminated. Access to the facility should be tracked via an automated logging mechanism or, at a minimum, signing in and out of the facility using a sign-in sheet.

Physical protection of the backup media is also of critical importance. In some cases, malicious insiders were able to steal or sabotage the backups so they were unusable, slowing down or crippling the organization when they attempted to recover from the insider attack.

In addition to securing the critical assets housed in the computer facility, careful attention should be paid to the computers, workstations, laptops, printers, and fax machines located in all areas, both secured and non-secured, of the organization. The security of the computing infrastructure begins with the protection of the perimeter of the organization and moves down to the protection of office space, by locking doors and windows. One employee in a case in the CERT database waited until after hours, removed his co-worker's name plate from outside his office door, and replaced it with his own. He then told the janitor he had forgotten something in his office but didn't have his office key. Since the name on his badge matched the name plate on the office door, the janitor helpfully unlocked the door. The employee then proceeded to download proprietary source code from his coworker's computer, which he stole from the organization.

The next layer of physical defense entails securing computing resources, for example, using password protected screen savers, and securing mobile devices and removable media (such as laptops, memory sticks, and PDAs) by requiring encryption of the removable media and/or a multi-factor authentication method.

To the greatest extent possible, attempts to access organization facilities should be logged. A regular audit of the access logs should be performed to identify violations or attempted violations of the access policy. Automated alerting of those violations could enable an organization to detect a security violation before major damage is inflicted.

Case Studies: What could happen if I don't do it?

The following example raises important physical security and legal/contracting issues regarding contractors. An employee's security access was suspended by his employer, "based on an employee dispute." The employee had been subcontracted by his employer as an IT consultant at an energy management facility. After being told of his suspension, he gained access to the energy production facility late Sunday night and hit an "emergency power off" button, shutting down some of the computer systems, including computers that regulated the exchange of electricity between power grids. He used a hammer to break the glass case enclosing the emergency power button. For a period of

two hours, the shutdown denied the organization access to the energy trading market, but fortunately didn't affect the transmission grid directly.

These types of contracting issues were already discussed in the “Recent Findings” section of Practice 1. This case serves as another example of why organizations should alter their contracting practices to require advance notification of pending employee sanctions by subcontractors. It also illustrates the potential damage that could be caused by the cascading effects from a disgruntled insider using inadequate physical controls to impact mission-critical systems.

An organization also needs to implement a strategy for tracking and disposal of documents containing controlled information. In addition, precautions against insider threats must be applied to all employees, even if they apparently have no access to the organization’s computing resources. Several recent cases involved the compromise of sensitive, proprietary, confidential, or secret information due to lax controls involving disposal of materials containing that information. In one case, a night-shift janitor obtained personal information for bank customers by searching through office trash, then used the information to commit identity theft. In another case, an employee was able to obtain documents containing trade secrets from a hopper containing confidential material to be destroyed, and sold the documents to a foreign competitor.

Practice 7: Implement strict password and account management policies and practices. (UPDATED)

If the organization's computer accounts can be compromised, insiders can circumvent manual and automated control mechanisms.

What to do?

No matter how vigilant organizations are about mitigating the threats posed by insiders, if the organization's computer accounts can be compromised, insiders have an opportunity to circumvent mechanisms in place to prevent insider attacks. Therefore, computer account and password management policies and practices are critical to impede an insider's ability to use the organization's systems for illicit purposes. Fine-grained access control combined with proper computer account management will ensure that access to all of the organization's critical electronic assets

- is controlled to make unauthorized access difficult
- is logged and monitored so that suspicious access can be detected and investigated
- can be traced from the computer account to the individual associated with that account

Some methods used by malicious insiders to compromise accounts included using password crackers, obtaining passwords through social engineering or because employees openly shared passwords, obtaining passwords because employees stored passwords in clear-text files on their computer or in email, and using unattended computers left logged in. Password policies and procedures should ensure that all passwords are strong,[12] employees do not share their passwords with anyone, employees change their passwords regularly, and all computers automatically execute password-protected screen savers after a fixed period of inactivity. As a result, all activity from any account should be attributable to its owner. In addition, an anonymous reporting mechanism should be available and its use encouraged for employees to report all attempts at unauthorized account access.

Some insiders created backdoor accounts that provided them with system administrator or privileged access following termination. Other insiders found that shared accounts were overlooked in the termination process and were still available to them. System administrator accounts were commonly used. Other shared accounts included DBA accounts. Some insiders used other types of shared accounts, such as those set up for access by external partners like contractors and vendors. One insider also used training accounts that were repeatedly reused over time without ever changing the password.

Periodic account audits combined with technical controls enable identification of

- backdoor accounts that could be used later for malicious actions by an insider, whether those accounts were specifically set up by the insider or were left over from a previous employee

[12] See *Choosing and Protecting Passwords*: http://www.us-cert.gov/cas/tips/ST04-002.html.

- shared accounts whose password was known by the insider and not changed after termination
- accounts created for access by external partners like contractors and vendors whose passwords were known by multiple employees, and were not changed when one of those employees were terminated

The need for every account should be re-evaluated periodically. Limiting accounts to those that are absolutely necessary, with strict procedures and technical controls that enable auditors or investigators to trace all online activity on those accounts to an individual user, diminishes an insider's ability to conduct malicious activity without being identified. Account management policies that include strict documentation of all access privileges for all users enable a straightforward termination procedure that reduces the risk of attack by terminated employees.

It is important that an organization's password and account management policies are also applied to all contractors, subcontractors, and vendors that have access to the organization's information systems or networks. These policies should be written into contracting agreements, requiring the same level of accountability in tracking who has access to your organization's systems. Contractors, subcontracts, and vendors should not be granted group accounts for access to your information systems. They should not be permitted to share passwords, and when employees are terminated at the external organization, your organization should be notified in advance so that account passwords can be changed. Finally, be sure to include contractor, subcontractor, and vendor accounts in the regularly scheduled password change process.

Case Studies: What could happen if I don't do it?

A disgruntled software developer downloaded the password file from his organization's UNIX server to his desktop. Next, he downloaded a password cracker from the Internet and proceeded to "break" approximately forty passwords, including the root password. Fortunately, he did no damage, but he did access parts of the organization's network for which he was not authorized. The insider was discovered when he bragged to the system administrator that he knew the root password. As a result, his organization modified its policies and procedures to implement countermeasures to prevent such attacks in the future. System administrators were permitted to run password crackers and notify users with weak passwords, and it improved security training for employees on how and why to choose strong passwords.

A second case also illustrates the importance of employee awareness of password security. Two temporary data entry clerks and one permanent employee were able to embezzle almost $70,000 from their company by fraudulently using other employees' computer accounts. The employees within their group openly shared their passwords to enhance productivity. The system's role-based access provided the other employees' accounts with access to privileged system functions. The clerks used those accounts without authorization to subvert the business process governing vendor payment. First, they entered valid data into the database using

their own accounts. Then they used the other, privileged employee's accounts to modify the vendor's name and address to that of a friend or relative, issued the check from the system, and then modified the data back to the original, valid vendor information. The fraud was discovered only after almost five months when an accountant in the general ledger department noticed that the number of checks issued was larger than normal and further investigation revealed the irregularities in the handling of the checks.

Recent Findings

The prevalence of outsourcing, supply chain management, and the globalization of the marketplace has blurred the line between an organization's boundaries and the external world. It is increasingly difficult to tell the difference between insiders and outsiders when it comes to managing access to an organization's data and information systems. Contractors, subcontractors, and vendors are now critical components to an organization that is trying to compete in a global marketplace. When dealing with contractor, subcontractor, and vendor relationships, the organization must recognize that insiders are no longer just employees within their four walls. Careful attention must be paid to ensure that the insiders employed by business partners are managed diligently, allowing them access to only information they need to fulfill their contractual obligations, and terminating their access when it is no longer needed.

In a recent case, the insider was employed by a marketing firm as a system administrator. The marketing firm was contracted by another organization, one of the world's largest processors of consumer data. As a result of the contractual relationship, the insider was given access to the contracting organization's FTP server so that he could periodically download sanitized, aggregated information from the consumer data organization's customers, which included banks, credit card companies, and phone companies. The system administrator found several unprotected files on the FTP server containing encrypted passwords for the original customer databases. He easily cracked the passwords to the customer databases belonging to ten percent of the consumer data organization's customers (approximately 200 large companies). He proceeded to copy the personal data for millions of Americans to dozens of compact disks. The disks were found in a search of his residence after his theft was accidentally discovered during an investigation of a hacker to whom he provided some sensitive customer information.

This case emphasizes the importance for organizations to take appropriate legal steps to secure their information once it leaves the organizational boundaries. It also illustrates the importance of requiring strong controls for any third party that maintains an organization's information.

Practice 8: Enforce separation of duties and least privilege. (UPDATED)

Separation of duties and least privilege must be implemented in business processes and for technical modifications to critical systems or information to limit the damage that malicious insiders can inflict.

What to do?

Separation of duties requires dividing functions among people to limit the possibility that one employee could steal information or commit fraud or sabotage without the cooperation of another. One type of separation of duties, called *two-person rule*, is often used. It requires two people to participate in a task for it to be executed successfully. The separation of duties may be enforced via technical or non-technical controls. Examples include requiring two bank officials to sign large cashier's checks, or requiring verification and validation of source code before the code is released operationally. In general, employees are less likely to engage in malicious acts if they must collaborate with another employee.

Effective separation of duties requires implementation of *least privilege*, authorizing people only for the resources needed to do their job. Least privilege also reduces an organization's risk of theft of confidential or proprietary information by its employees, since access is limited to only those employees who need access to do their jobs. Some cases of theft of information for business advantage involved sales people, for instance, who had unnecessary access to strategic products under development.

It is important that management of least privilege be an ongoing process, particularly when employees move throughout the organization, including promotions, transfers, relocations, and demotions. As employees change jobs, organizations tend to neglect to review their required access to information and information systems. All too often, employees are given access to new systems and/or information required for their new job without revoking their access to information and systems required to perform their previous job duties. Unless an employee maintains responsibility for tasks from their previous job that require access to information and information systems, their access should be disabled when they assume the new position.

Typically, organizations define roles that characterize the responsibilities of each job, as well as the access to organizational resources required to fulfill those responsibilities. Insider risk can be mitigated by defining and separating roles responsible for key business processes and functions. For example,

- requiring online management authorization for critical data entry transactions
- instituting code reviews for the software development and maintenance process
- using configuration management processes and technology to control software distributions and system modification
- designing auditing procedures to protect against collusion among auditors

Physical, administrative, and technical controls can be used to restrict employees' access to only those resources needed to accomplish their jobs. Access control gaps often facilitated insider crimes. For example, employees circumvented separation of duties enforced via policy rather than through technical controls. Ideally organizations should include separation of duties in the design of their business processes and enforce them via technical and non-technical means.

Access control based on separation of duties and least privilege is crucial to mitigating the risk of insider attack. These principles have implications in both the physical and the virtual worlds. In the physical world, organizations need to prevent employees from gaining physical access to resources not required by their work roles. Researchers need to have access to their laboratory space but do not need access to human resources file cabinets. Likewise, human resources personnel need access to personnel records but do not need access to laboratory facilities. There is a direct analogy in the virtual world in which organizations must prevent employees from gaining online access to information or services that are not required for their job. This kind of control is often called *role-based access control*. Prohibiting access by personnel in one role from the functions permitted for another role limits the damage they can inflict if they become disgruntled or otherwise decide to exploit the organization for their own purposes.

Case Studies: What could happen if I don't do it?

In one case, a currency trader (who also happened to have a college minor in computer science) developed much of the software used by his organization to record, manage, confirm, and audit trades. He implemented obscure functionality in the software that enabled him to conceal illegal trades totaling $691 million over a period of five years. In this case, it was nearly impossible for auditors to detect his activities.

The insider, who consented to be interviewed for the *Insider Threat Study*, told the study researchers that problems can arise when "the fox is guarding the henhouse."[13] Specifically, the insider's supervisor managed both the insider and the auditing department responsible for ensuring his trades were legal or compliant. When auditing department personnel raised concern about the insider's activities, they were doing so to the insider's supervisor (who happened to be their supervisor as well). The supervisor directed auditing department personnel not to worry about the insider's activities and to cease raising concern, for fear the insider would become frustrated and quit.

This case illustrates two ways in which separation of duties can prevent an insider attack or detect it earlier:

- end users of an organization's critical systems should not be authorized to modify the system functionality or access the underlying data directly
- responsibility for maintaining critical data and responsibility for auditing that same data should never be assigned to the same person

[13] *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. http://www.cert.org/archive/pdf/bankfin040820.pdf.

In another case, a supervisor fraudulently altered U.S. immigration asylum decisions using his organization's computer system in return for payments of up to several thousand dollars per case, accumulating $50,000 over a two-year period. The insider would approve an asylum decision himself, request that one of his subordinates approve the decision, or overturn someone else's denial of an asylum application. Several foreign nationals either admitted in an interview or pleaded guilty in a court of law to lying on their asylum applications and bribing public officials to approve their applications. The organization had implemented separation of duties via role-based access control by limiting authorization for approving or modifying asylum decisions to supervisors' computer accounts. However, supervisors were able to alter any decisions in the entire database, not just those assigned to their subordinates. An additional layer of defense, least privilege, also could have been implemented to prevent supervisors from approving asylum applications or overturning asylum decisions with which they or their teams were not involved.

Recent Findings

Analysis of recent cases revealed that almost one third of the theft of information for financial gain cases and half of the modification of information for financial gain cases involved collaboration with at least one other insider. A number of reasons could explain the high degree of collusion. For example, internal collusion could be necessary to overcome controls that enforce separation of duties. Given that the enforcement of separation of duties alone will not prevent insider attacks, it is essential that the organization implement a layered defense to decrease the likelihood of such an attack.

A recent case involved an insider who worked at a consumer credit report agency. The insider's job was to maintain the information stored in the consumer credit database. In exchange for money from an external collaborator, the insider conspired with coworkers to artificially inflate the credit scores of specific consumers to enable them to secure loans from credit institutions and lenders. The insider and internal conspirators modified or deleted credit-history data for 178 consumers. The purpose was to strengthen their creditworthiness and cause lenders to issue loans to these consumers. The insider received advanced payment for the modification and passed the payment on to her co-workers to make the alterations in the database. Over $4 million dollars of risky loans resulted in this case.

One pattern the CERT team observed in multiple recent cases involved insiders who changed the mailing address and/or email address of customers so that they did not receive automated notifications, bills, and other company correspondences regarding fraudulent credit card accounts that the insiders then opened using the customer's identity. Some banks and other organizations have instituted practices for verifying customer address and email address changes before actually making the change in customer databases. This practice provides an additional control on top of the separation of duties that used to be sufficient for protection of such information.

These cases in this section show the importance of designing auditing procedures to detect potential collusion among employees, with the assumption that collusion to override separation of duties controls is quite possible.

Practice 9: Consider insider threats in the software development life cycle (NEW)

Technical employees have taken advantage of defects introduced in the software development life cycle (SDLC) to deliberately perform malicious technical actions; likewise non-technical employees have recognized vulnerabilities and used them to carry out their fraudulent activities.

What to do?

Impacts from insiders that exploited defects in the SDLC include

- a company went out of business
- fraud losses up to $691 Million
- drivers licenses created for individuals who could not get a legitimate license
- disruption of telecommunications services
- court records, credit records, and other critical data modified
- a virus planted on customers' systems

Clearly the impacts in these cases were significant. It is important that organizations recognize these threats, and consider potential threats and mitigation strategies when developing and maintaining software internally, and also when implementing systems acquired elsewhere.

Insiders exploited defects in all phases of the SDLC in the cases examined. Each phase of the SDLC is analyzed in more detail below.

Requirements Definition: Many systems automate business and workflow processes. When defining the requirements for such systems, the processes to be automated must be carefully defined. In the cases examined, many of the insiders were able to carry out their illicit activities because they recognized instances in which protection from insider threats was not considered. For example, in some cases, there was no separation of duties required in automated processes. In others, authentication and role-based access controls were not required for system access. System requirements should also include specification of data integrity and consistency checks that should be implemented for all changes made to production data by system end users, as well as automated checks which must be run periodically to detect suspicious modifications, additions, or deletions. In other words, requirements should consider periodic auditing functions, which can be implemented and run automatically on a more frequent basis than manual system audits.

Note that all of the recommendations detailed here for system requirements definition apply to both systems built by the organization and those acquired. When evaluating new systems for acquisition, the types of requirements detailed here should also be considered. Once requirements have been defined and potential systems are evaluated for purchase, the ability of each system to meet those requirements is an important part of the evaluation process.

System Design: In some cases, the organization did address protection from insiders in their system requirements definition process. However, inadequate design of those functions in automated workflow processes enabled some insiders to commit malicious activity. For example, improperly designed separation of duties facilitated some insider crimes. In some cases, separation of duties was not designed into the system at all. In others, although separation of duties was implemented, there was no design to "check the checker." Unfortunately, due to the high degree of collusion observed in insider theft or modification cases, it is necessary for system designers to consider how they might implement yet another layer of defense on top of separation of duties, to discover cases in which two employees are working together to commit a crime. Most of these types of crimes continue over a prolonged period, so although detection might not be immediate, patterns of suspicious activity can be discovered to catch the activity sooner rather than later.

Another key finding related to system design vulnerabilities involved authorized system overrides. Several insiders used special system functions created for exception handling to carry out their crimes. They realized that these functions were created for exceptional situations in which changes had to be made quickly, thus bypassing the usual mandated security checks. This type of functionality provided an easy way for insiders to" get around the rules." It is important to design special data integrity checks for any data modified, added, or deleted using these exception handling functions.

Implementation: Very few insiders actually introduced intentional vulnerabilities or malicious code into source code during the initial development process; that type of activity was more often carried out during the maintenance phase of the SDLC. However, one eighteen-year-old web developer did use backdoors he had inserted into his source code during system development to access his former company's network, spam its customers, alter its applications, and ultimately put it out of business. Code reviews and strict change control, a part of any solid software development process, could have detected the backdoor and perhaps saved the company.

During the software development process, organizations are vulnerable to the same types of insider attacks that can occur on production systems. One software development project manager, recognizing there was no way to attribute actions to a single user in the development environment, repeatedly sabotaged his own team's project. The motivation in this case is unique: his team was falling behind in the project schedule, and he used the repeated sabotage as a convenient excuse for missed deadlines. It is important that organizations consider resiliency during the development process just as on production systems.

Installation: A variety of oversights in the process of moving a system from development to production provided avenues for attack by insiders. Examples from several different cases follow.

- A system was put into production at a large government agency without instituting backups of the source code. The manager of the development project encrypted the only copy of the source code for the project after the system was

put into production, then attempted to extort money to decrypt the code.

- The same password file was used for the operational system when it was moved into production as had been used in the development environment, enabling one of the developers to access and steal sensitive data after it had been entered into the operational system.
- Unrestricted access to all customers' systems enabled a computer technician to plant a virus directly on customer networks.
- An organization implemented a web content management system that managed all changes to its public website. Although they used a change control system to track changes, they had no process for approval of changes before they were released to the website. As a result, a college intern, before leaving for the summer, published material intended to be a joke on the organization's website, causing quite a scandal and damage to the reputation of the government agency.

It is important that organizations carefully consider these types of issues as they move a system from development to production because employees using those systems on a daily basis will likely notice the vulnerabilities.

System Maintenance: More insider incidents occurred during the maintenance phase of the SDLC than during initial system implementation. It appears that organizations impose more stringent controls during the initial development process, but once a system has been in production and stabilized following initial release, those controls tend to become more lax. Insiders in the cases took advantage of those relaxed controls in a variety of ways.

While many organizations institute mandatory code reviews for development of new systems or significant new modules for existing systems, several insiders were able to inject malicious code into stable, fairly static systems without detection. Ineffective configuration or change control processes contributed to their ability to do so. A few organizations in the cases examined implemented configuration management systems that recorded a detailed log of the malicious insider activity. However, there was no proactive process for actually controlling system releases using those systems or reviewing the logs to detect malicious activity after the fact.

Insiders were also able to sabotage backup systems that were left unprotected to amplify their attack. Also, known system vulnerabilities were exploited on unpatched systems by a few knowledgeable insiders. Risk management of critical systems needs to extend beyond the system itself to surrounding support systems, such as the operating system and backups.

User authorization is another area that tends to become more lax over time. When a system is initially released, system authorizations and access methods tend to be carefully implemented. Once the system is in production, user access controls tend to slip. Access to the system and to the source code itself must be carefully managed over time.

Case Studies: What could happen if I don't do it?

A programmer at a telecommunications company was angry when it was announced that there would be no bonuses. He used the computer of the project leader, who sat in a cubicle and often left his computer logged in and unattended, to modify his company's premier product, an inter-network communication interface. His modification, consisting of two lines of code, inserted the character "i" at random places in the supported transmission stream and during protocol initialization. The malicious code was inserted as a logic bomb, recorded in the company's configuration management system, and attributed to the project leader. Six months later, the insider left the company to take another job. Six months after that, the logic bomb finally detonated, causing immense confusion and disruption to the company's services to their customers. This case exemplifies many of the issues discussed in this section.

Another case illustrates a more low-tech incident that was enabled by oversights in the SDLC. The primary responsibility of a police communications operator was to communicate information regarding drivers' licenses to police officers in the field. This case began when the operator was approached by an acquaintance and asked if she would be willing to look up information for three people for him, and she agreed. Over time, she proceeded to look up information on people in return for payment by her acquaintance. At some point she discovered that she not only could read information from the database, but she also had the ability to use other system functions. At that point, at the request of her accomplice, she began to generate illegal drivers' licenses for people who were unable to gain legitimate licenses in return for payment. Fortunately, a confidential informant led to her arrest for fraudulently creating approximately 195 illegal drivers licenses. This case shows the dangers of overlooking role-based access control requirements when defining system requirements, designing the system, and during implementation.

Practice 10: Use extra caution with system administrators and technical or privileged users. (UPDATED)

System administrators and technical or privileged users have the technical ability, access, and oversight responsibility to commit and conceal malicious activity.

What to do?

Recall that the majority of the insiders who committed sabotage, and over half of those who stole confidential or proprietary information, held technical positions. Technically sophisticated methods of carrying out and concealing malicious activity included writing or download of scripts or programs (including logic bombs), creation of backdoor accounts, installation of remote system administration tools, modification of system logs, planting of viruses, and use of password crackers.

System administrators and privileged users[14] by definition have a higher system, network, or application access level than other users. This higher access level comes with higher risk due to the following:

- They have the technical ability and access to perform actions that ordinary users cannot.
- They can usually conceal their actions, since their privileged access typically provides them the ability to log in as other users, to modify system log files, or to falsify audit logs and monitoring reports.
- Even if an organization enforces technical separation of duties, system administrators are typically the individuals with oversight and approval responsibility when application or system changes are requested.

Techniques that promote non-repudiation of action ensure that online actions taken by users, including system administrators and privileged users, can be attributed to the person that performed them. Therefore, should malicious insider activity occur, non-repudiation techniques allow each and every activity to be attributed to a single employee. Policies, practices, and technologies exist for configuring systems and networks to facilitate non-repudiation. However, keep in mind that system administrators and other privileged users will be the ones responsible for designing, creating, and implementing those policies, practices, and technologies. Therefore, separation of duties is also very important: network, system, and application security designs should be created, implemented, and enforced by multiple privileged users.

Even if online actions can be traced to the person who engaged in the action, it is unreasonable to expect that all user actions can be monitored proactively. Therefore, while the practices discussed above ensure identification of users following detection of suspicious activity, additional steps must be taken by organizations to defend against

[14] For the purposes of this report, the term “privileged users” refers to users who have an elevated level of access to a network, computer system, or application that is short of full system administrator access. For example, database administrators (DBAs) are privileged users as they have the ability to create new user accounts and control the access rights of users within their domain.

malicious actions before they occur. For instance, system administrators and privileged users have access to all computer files within their domains. Technologies such as encryption can be implemented to prevent such users from reading or modifying sensitive files to which they should not have access.

Policies, procedures, and technical controls should enforce separation of duties and require actions by multiple users for releasing all modifications to critical systems, networks, applications, and data. In other words, no single user should be permitted or be technically able to release changes to the production environment without online action by a second user. These controls would prevent an insider from releasing a logic bomb without detection by another employee. They would also have been effective against a foreign investment trader, who manipulated source code to carry out his crime. He happened to have a degree in computer science, and was therefore given access to the source code for the trading system. He used that access to build in backdoor functionality which enabled him to hide trading losses without detection totaling $691 million over a five year period.

Note that in order to enforce separation of duties for system administration functions, at least two system administrators must be employed by the organization. There are several case examples throughout this report in which the organization was victimized by the organization's sole system administrator. Although many small organizations cannot afford to hire more than one system administrator, it is important that they recognize the increased risk that accompanies that situation.

Finally, many of the insiders studied, especially those engaged in IT sabotage, were former employees. Organizations must be particularly careful in disabling access, particularly for former system administrators and technical or privileged users. Thoroughly documented procedures for disabling access can help ensure that stray access points are not overlooked. In addition, the two-person rule should be considered for the critical functions performed by these users to reduce the risk of extortion after they leave the organization.

Case Studies: What could happen if I don't do it?

A system administrator at an international financial organization heard rumors that the annual bonuses were going to be lower than expected. He began constructing a logic bomb at home and used authorized remote access to move the logic bomb to the company's servers as part of the typical server upgrade procedure over a period of two and a half months. When he was informed by his supervisor that his bonus would be significantly lower than he had expected, he terminated his employment immediately. Less than two weeks later, the logic bomb went off at 9:30 a.m., deleting 10 billion files on approximately 1,000 servers throughout the United States. The victim organization estimated that it would cost more than $3 million to repair its network, and the loss affected 1.24 billion shares of its stock.

In another case, an insider was promoted from one position to another within the same organization. Both positions used the same application for entering, approving, and authorizing payments for medical and disability claims. The application used role-based access to enforce separation of duties for each system function. However, when this particular insider was promoted, she was authorized for her new access level, but administrators neglected to rescind her prior access level (separation of duties was inadequately enforced). As a result, she ended up having full access to the application, with no one else required to authorize transactions (payments) from the system. She entered and approved claims and authorized monthly payments for her fiancé, resulting in payments of over $615,000 over almost two years.

Recent Findings

Seventy-one percent of the theft of information for business advantage cases were committed by individuals with a technical background. In many cases, technical employees, including programmers, took customer information and intellectual property, including source code and or system architecture / security documents, with them when they left the organization. Those employees used the information for a number of reasons: obtaining a new job, giving the individual a competitive advantage at the new organization, and assisting them in competing against the victim organization.

In addition, recent cases continue to demonstrate that organizational failures in dealing with disgruntled system administrators and other privileged users eventually resulted in IT sabotage. In one case, the subject was a developer of e-commerce software for an organization. He decided to move his family to a different state, and therefore could no longer work for the organization. The organization hired him as a consultant and he traveled across state lines to work two days a week and telecommuted three days a week from home. He was disgruntled because the organization would not provide the benefits he felt he deserved once he became a contractor, and the relationship continued to deteriorate. Finally, the organization told him his employment would be terminated in approximately one month.

After a week and a half, the insider logged in remotely from home, deleted the software he was developing, as well as software being developed by others, modified the system logs to conceal his actions, and then changed the root password. He then joined a telephone conference, never mentioning what he had done. After the telephone conference ended he reported that he was having problems logging in, again to conceal his actions. At the end of the day he announced his resignation. This action cost the organization over $25,000, including 230 staff hours and associated costs.

Practice 11: Implement system change controls. (UPDATED)

Changes to systems and applications must be controlled to prevent insertion of backdoors, keystroke loggers, logic bombs, and other malicious code or programs.

What to do?

Controls are processes that provide assurance for information and information services, and help mitigate risks associated with technology use. *Change controls* are controls that ensure the accuracy, integrity, authorization, and documentation of all changes made to computer and network systems.[15] The wide variety of insider compromises that relied on unauthorized modifications to the organization systems suggests the need for stronger change controls. To support this, organizations should identify baseline software and hardware configurations. An organization may have several baseline configurations, given the different computing and information needs of different users (e.g., accountant, manager, programmer, and receptionist). But as configurations are identified, the organization should characterize the hardware and software that makes up those configurations.

Characterization can be a basic catalog of information, tracking information like versions of installed software, hardware devices, and disk utilization. However, such basic characterizations can be easily defeated, so more comprehensive characterizations are often required. These characterizations include

- cryptographic checksums (using SHA-1 or MD5, for example)
- interface characterization (such as memory mappings, device options, and serial numbers)
- recorded configuration files

Once this information is captured, computers implementing each configuration can be validated by comparing it against the baseline copy. Discrepancies can then be investigated to determine whether they are benign or malicious. Using these techniques, changes to system files or the addition of malicious code will be flagged for investigation. There are tools called *file integrity checkers* that partially automate this process and provide for scheduled sweeps through computer systems.[16]

Computer configurations do not remain unchanged for long. Therefore, characterization and validation should be part of an organization's change management process. Different roles should be defined within this process and conducted by different individuals so that no one person can make a change unnoticed by others within the organization. For example, validation of a configuration should be done by a person other than the one who

[15] See Information Technology Controls, the Institute of Internal Auditors, http://www.theiia.org/download.cfm?file=70284.
[16] See http://www.sans.org/resources/idfaq/integrity_checker.php for a discussion of file integrity checkers.

made changes so that there is an opportunity to detect and correct malicious changes (including planting of logic bombs).

Change logs and backups need to be protected so that unauthorized changes can be detected and, if necessary, the system rolled back to a previous valid state. In addition, some insiders in cases in the CERT database modified change logs to conceal their activity or frame someone else for their actions. Other insiders sabotaged backups to further amplify the impact of their attack.

Many organizations defend against malicious code using antivirus software and host or network firewalls. While these defenses are useful against external compromises, their value is limited in preventing attacks by malicious insiders in two important respects: they do not work against new or novel malicious code (including logic bombs planted by insiders) and they are concerned primarily with material spread through networking interfaces rather than installed directly on a machine. Change controls help address the limitations of these perimeter defenses.

Just as tools can be implemented for detecting and controlling system changes, configuration management tools should be implemented for detecting and controlling changes to source code and other application files. As described in Practice 9, some insiders modified source code in order to carry out their attack. Note that these modifications were done during the maintenance phase of the software development life cycle, not during initial implementation. It appears that some organizations institute much more stringent configuration management controls during initial development of a new system, including code reviews and use of a configuration management system. However, once the system is in production and development stabilizes, those controls do not seem to be as strictly enforced. It appears that organizations tend to relax the controls, leaving open a vulnerability for exploit by technical insiders with the proper motivation and lack of ethics.

Case Studies: What could happen if I don't do it?

A manufacturing firm's system administrator began employment as a machinist. Over a ten-year period, the insider created the company's network supporting the critical manufacturing processes and had sole authority for system administration over that network. The company eventually expanded, opening additional offices and plants nationally and internationally. The insider

- began to feel disgruntled at his diminishing importance to the company
- launched verbal and physical assaults on coworkers
- sabotaged projects of which he was not in charge
- loaded faulty programs to make coworkers look bad

He received a verbal warning, two written reprimands, was demoted, and finally fired as a result of his actions. A few weeks later, a logic bomb executed on the company's network, deleting one thousand critical manufacturing programs from the company's servers. The estimated cost of the damage exceeded $10 million, leading to the layoff of

approximately 80 employees. The investigation revealed that the insider had actually tested the logic bomb three times on the company's network after hours prior to his termination.

Practices for detection of malicious code would have detected that a new program had been released with timed execution. Change control procedures with a two-person rule for release of system-level programs, and characterization procedures, could have detected the release of a new system file that was not part of the original system baseline.

In another case, an organization built automated monitoring into its software that sent automatic notification to the security officer any time a highly restricted screen was used to modify information stored in the database. Role-based access control restricted access to this screen to a few privileged users; the automated notification provided a second layer of defense against illegal data modification using that function. However, a developer of the application who happened to have access to that function modified the code so that the automated notification was no longer sent. He then proceeded to use the function to steal a large sum of money from his employer.

Interestingly, the organization had a configuration management system in place for software changes. When a program was compiled, a report was produced listing which files were compiled, by which computer account, and when. It also listed modules added, modified, or deleted. Unfortunately, this report was not monitored, and therefore the application changes were not detected during the year and a half over which the fraud was committed. Had it been monitored, or had the configuration control system enforced, a two-person rule for releasing new versions of software, the removal of the security notification would have been detected and the insider could not have committed the fraud.

Recent Findings

Some recent cases involved theft of information using a keystroke logger – a hardware or software device that records the exact keystrokes entered into a computer system. Keystroke loggers can be used maliciously to obtain an organization's confidential information, an individual's private information, and in the worst case, can be used to obtain passwords or encryption keys.

In one case, a claims manager at an insurance company, who was upset with the company's practice of cancelling policies after late payment, installed a hardware keystroke logging device on the computer of the secretary to a chief executive. Although he did not have access to the executive's office, he realized that an abundance of confidential information passed from the secretary to and from the executive. Furthermore, her desk was not physically secured like the executive's office. The insider used the keystroke logger to gather confidential information from the secretary's computer, which he then sent to the legal team assembling the case against the organization.

Other cases involved software keystroke loggers. In one case, two insiders colluded with an external person to collect their company's intellectual property and relay it to a competitor. The external collaborator sent an email message containing an attachment infected with a virus to one of the insiders. The insider deliberately double clicked on the infected attachment, and it proceeded to install a keystroke logger on machines on the company's network. The keystroke logger periodically sent confidential information to a competitor, who used it to lure customers away from the victim organization.

Use of logic bombs by employees to vent dissatisfaction with their organization continues in recent cases. Logic bombs were used to delete financial records for over 50,000 accounts in a credit union, and to wipe out a patient-specific drug interaction conflict database for a health care solutions organization. In another case, a logic bomb was detonated simply to make the insider's successor in the organization look bad.

A contract system adminsitrator lost his contract to oversee the daily operation of a computer system used to track and plot the location of ships, submarines, and underwater obstructions. The insider planted logic bombs on five servers and set them to detonate long after he left the organization. Three of the five went off and caused major damage; the other two were located and neutralized.

Some insiders opted for a simpler way to disrupt systems, simply deleting software on which their organization relied. The individual responsible for unauthorized changes to system configurations or programs can be identified if an organization audits such actions and protects the system logs. Unfortunately, unptotected logs are often targeted by the sophisticated insider.

Practice 12: Log, monitor, and audit employee online actions. (UPDATED)

Logging, monitoring, and auditing can lead to early discovery and investigation of suspicious insider actions.

What to do?

If account and password policies and procedures are in place and enforced, an organization has a good chance of clearly associating online actions with the employee who performed them. Logging, monitoring, and auditing provide an organization with the opportunity to discover and investigate suspicious insider actions before more serious consequences ensue.

Auditing in the financial community refers to examination and verification of financial information. In the technical security domain it refers to examination and verification of various network, system, and application logs or data. To prevent or detect insider threats, it is important that auditing involve the review and verification of changes to *any* of the organization's critical assets.[17] Furthermore, auditing must examine and verify the integrity as well as the legitimacy of logged access.

Automated integrity checking should be considered for flagging a required manual review of suspicious transactions that do not adhere to predefined business rules. Insider threats are most often detected by a combination of automated logging and manual monitoring or auditing. For example, integrity checking of computer account creation logs involves automated logging combined with manual verification that every new account has been associated with a legitimate system user and that the user is aware of the account's existence.

Automated tools could detect creation of the typical backdoor account–a system administrator account not associated with a current employee. Unfortunately, detection of backdoor accounts cannot be totally automated. For example, one insider created VPN accounts for three legitimate, current employees, and simply did not tell them the accounts had been created. After being fired, he used those backdoor accounts to obtain remote access at night for two weeks. He setup his attack during those two weeks right under the nose of a contractor, who was hired specifically to monitor the network for remote access by him.

Likewise, data audits typically involve manual processes, such as comparing electronic data modification history to paper records or examining electronic records for suspicious discrepancies.

[17] Many risk management methodologies are based on protection of critical assets. For example, see the OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation℠) risk-based strategic assessment and planning technique for security: http://www.cert.org/octave/.

Auditing should be both ongoing and random. If employees are aware that monitoring and auditing is a regular, ongoing process and that it is a high priority for the individuals who are responsible for it, it can serve as a deterrent to insider threats. For example, if a disgruntled system administrator is aware that all new computer accounts are reviewed frequently, then it is less likely that he or she will create backdoor accounts for later malicious use.

On the other hand, it probably is not practical to institute daily monitoring of every financial transaction in a financial institution. Monthly and quarterly auditing provides one layer of defense against insiders, but it also provides a predictable cycle on which insiders could design a fraud scheme that could go undetected over a long period of time. Random auditing of all transactions for a given employee, for example, could add just enough unpredictability to the process to deter an insider from launching a contemplated attack.

Finally, it is worth mentioning that two insiders in cases in the CERT library attacked *other external* organizations from their computer at work. The forensics and investigation activities that the employees' organizations had to endure as a result were very disruptive to their staff and operations.

Case Studies: What could happen if I don't do it?

A large international company, while performing remote access monitoring, noticed that a former consultant had obtained unauthorized access to its network and created an administrator account. This prompted an investigation of the former insider's previous online activity, revealing he had run several different password-cracking programs on the company's network five different times over a ten-month period. Initially, he stored the cracked passwords in a file on the company's server. Later he installed a more sophisticated password-cracking program on the company's system. This program enabled him to automatically transfer all accounts and passwords that could be cracked to a remote computer on a periodic basis. Five thousand passwords for company employees were successfully transferred. This case illustrates the importance of logging and proactive monitoring. Because of those practices, this insider's actions were detected before any malicious activity was committed using the accounts and passwords or the backdoor account.

Another insider attack provides a contrasting example—one in which lack of auditing permitted the insider to conduct an attack that was less technically sophisticated but that enabled him to steal almost $260,000 from his employer over a two-year period. The insider was the manager of a warehouse. The attack proceeded as follows:

- The insider convinced his supervisor that he needed privileged access to the entire purchasing system for the warehouse.
- Next, he added a fake vendor to the list of authorized suppliers for the warehouse.
- Over the next two years, he entered 78 purchase orders for the fake vendor, and,

although no supplies were ever received, he also authorized payment to the vendor.

The insider was aware of approval procedures, and all of his fraudulent purchases fell beneath the threshold for independent approval. The bank account for the vendor happened to be owned by the insider's wife. The fraud was accidentally detected by a finance clerk who noticed irregularities in the paperwork accompanying one of the purchase orders. This fraud could have been detected earlier by closer monitoring of online activities by privileged users, particularly since this particular user possessed unusually extensive privileged access. In addition, normal auditing procedures could have validated the new vendor, and automated integrity checking could have detected discrepancies between the warehouse inventory and purchasing records.

Recent Findings

In almost all of the 24 cases of insider theft for business advantage, the insider resigned before or after the theft. About two-thirds of the thefts took place within three weeks of the insider's resignation and over half stole all of the information at once. In one case the insider accepted a position with a competing organization, resigned his position, and proceeded to download proprietary information to take with him to the new company before his last day of work. He stole the information despite admonitions by the hirer not to bring any proprietary information with him to his new position. When questioned about the theft, the insider admitted to downloading the information, saying that he hoped to use it if he ever started his own business.

In a similar case, the insider accepted a position with a competitor and started downloading documents containing trade secrets the very next day. A few weeks later, after several sessions of high-volume downloading, the insider left the organization and started working for the competitor. Just two days after starting his new job, the insider loaded the stolen files onto his newly assigned laptop, and within a month had emailed the trade secrets to his new co-workers. This lack of any technical effort to conceal the theft was also apparent in other cases of this type. This suggests that monitoring of online actions, particularly downloads within one month before and after resignation, could be particularly beneficial for preventing or detecting early the theft of proprietary information.

A wide variety of technical means were used in the theft cases to transfer information, including email, phone, fax, downloading to or from home over the Internet, malicious code collection and transmission, and printing out material on the organizations' printers. One particularly vengeful insider acted out of anger at his employer's rewarding executives with exorbitant bonuses while lower-level employees were receiving meager raises or being laid off. He began downloading confidential corporate documents to his home computer, carrying physical copies out of the offices, and emailing them to two competitors. Neither of the two competitors sought the trade secret information and both sent the information they received back to the organization. This insider made no attempt to conceal or deny his illicit activity. Other recent cases similarly involved current employees who emailed large files to their home machines or to competing organizations.

Organizations monitoring for theft of confidential information need to consider the wide variety of ways that information is purloined and customize their detection strategy accordingly. Data leakage tools may help with this task. Many tools are available that enable the organization to perform functions like

- alerting administrators to emails with unusually large attachments
- tagging documents that should not be permitted to leave the network
- tracking or preventing printing, copying, or downloading of certain information, such as personally identifiable information or documents containing certain words like new product codenames
- tracking of all documents copied to removable media
- preventing or detecting emails to competitors, outside the U.S., to gmail or hotmail accounts, and so on

Many theft cases involved insiders downloading information outside their area of expertise or responsibility. This may provide a means for an organization to detect suspicious activity, provided the organization tracks what information each employee needs in order to accomplish their job. Role-based access control may provide a basis for such tracking.

Finally, organizations must be aware of the possibility that insiders will attack another organization, possibly a previous employer, using the organization's systems. While not common, such crimes can and do happen–there are a few such cases in the CERT library. Organizations need to consider the liability and disruption that such a case could cause.

One such attack by an insider against his former employer from his current employer's systems may have been a major factor in the current employer's downfall. The insider claimed that the attack was payback for misdeeds against him and his current company. Although the current employer disavows having anything to do with the attack, it too suffered as a result of the insider's action. The FBI investigators surrounded its offices and told workers not to tamper with any company data or files, putting its work on temporary hold. In a panic, the insider started massive erasure of potential evidence. The insider received 5 years for computer hacking and 20 years for obstruction of justice.

Practice 13: Use layered defense against remote attacks. (UPDATED)

Remote access provides a tempting opportunity for insiders to attack with less risk.

What to do?

Insiders often attack organizations remotely using legitimate access provided by the organization or following termination. While remote access can greatly enhance employee productivity, caution is advised when remote access is provided to critical data, processes, or information systems. Insiders have admitted that it is easier to conduct malicious activities from home because it eliminates the concern that someone could be physically observing the malicious acts.

The vulnerabilities inherent in allowing remote access suggest that multiple layers of defense should be built against remote attack. Organizations may provide remote access to email and non-critical data but should strongly consider limiting remote access to the most critical data and functions and only from machines that are administered by the organization. Access to data or functions that could inflict major damage to the company should be limited to employees physically located inside the workplace as much as possible. Remote system administrator access should be limited to the smallest group practicable, if not prohibited altogether.

When remote access to critical data, processes, and information systems is deemed necessary, the organization should offset the added risk with closer logging and frequent auditing of remote transactions. Allowing remote access only from company machines will enhance the organization's ability to control access to their information and networks and monitor the activity of remote employees. Information such as login account, date/time connected and disconnected, and IP address should be logged for all remote logins. It also is useful to monitor failed remote logins, including the reason the login failed. If authorization for remote access to critical data is kept to a minimum, monitoring can become more manageable and effective.

Disabling remote access is an often overlooked but critical part of the employee termination process. It is critical that employee termination procedures include

- retrieving any company-owned equipment
- disabling remote access accounts (such as VPN and dial-in accounts)
- disabling firewall access
- changing the passwords of all shared accounts (including system administrator, database administrator [DBA], and other privileged shared accounts)
- closing all open connections

A combination of remote access logs, source IP addresses, and phone records usually helps to identify insiders who launch remote attacks. Identification can be straightforward because the user name of the intruder points directly to the insider. Of course, corroboration of this information is required, because the intruders might have been

trying to frame other users, cast attention away from their own misdeeds by using other users' accounts, or otherwise manipulate the monitoring process.

Case Studies: What could happen if I don't do it?

For a period of five years, a foreign currency trader with an investment bank "fixed" the bank's records to make his trading losses look like major gains for the bank. His actions made it appear that he was one of the bank's star producers, resulting in lucrative bonuses for his perceived high performance. In actuality, the bank lost hundreds of millions of dollars and drew a large amount of negative media attention as a result of his actions. While initially most of the insider's fraud occurred at work, he increasingly found it easier to conduct his illicit activities from home in the middle of the night because he did not have to worry about anyone in the office or at home looking over his shoulder. Therefore, the risk that other traders would find out about his fraudulent activities was reduced significantly.

In an interview for the *Insider Threat Study*, the insider said that group trading (trading by a team of traders), rather than individual trading, can help mitigate an organization's risks, because it is easier to detect illegal or suspicious trading practices when there are multiple team members trading from the same account.[18] In this case, isolated trading, along with the anonymous nature of remote access, emboldened the insider to continue a fraud in which he otherwise might not have engaged.

In another case, a government organization notified one of its contract programmers that his access to a system under development was being eliminated and that his further responsibilities would be limited to testing activities. After his protests were denied, the programmer quit the organization. Then, three times over a two-week period, the insider used a backdoor into the system with administrator privilege (which he presumably installed before leaving) to download source code and password files from the developmental system. The unusually large size of the remote downloads raised red flags in the organization, which resulted in an investigation that traced the downloads to the insider's residence and led to his arrest, prosecution, and imprisonment. This case demonstrates the value of vigilant monitoring of remote access logs and reaction to suspicious behavior in limiting damage to the organization's interests.

Recent Findings

Cases of compromise from remote locations continue in recent cases as they did in CERT's previous study. Some of these cases involved compromises from the insider's home machine. Several recent compromises, however, occurred not from the insider's home, but from other remote machines not under the administrative control of the organization, such as from a competing organization using access that should have been disabled upon the insider's termination. In one of these cases, the insider used PC Anywhere–a remote system administration tool–to get back into the organization's systems and delete all of their data—email, sales records, correspondence, non-disclosure

[18] *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. http://www.cert.org/archive/pdf/bankfin040820.pdf.

agreements, proprietary technical information, and backup data. He had set up PC Anywhere at his previous job where he had been a system administrator. This particular attack was considered to be a significant contributing factor in the organization's downfall. Disabling of remote access using remote administration tools should be part of the employment termination process.

As in the previous study, some of the recent cases involving remote access were IT sabotage crimes committed following termination and intended to cause harm to a specific person. In one such case, a fired employee got back into his previous employer's system and deleted approximately 1000 files related to employee compensation. He tried to frame a female employee who had spurned his romantic advances while at the organization by changing her records to reflect a $40,000 increase in salary and $100,000 bonus. To further frame the woman, he sent an email to senior organization managers from an account that contained the female employee's last name. The email contained an attachment containing an excerpt of the deleted files.

Practice 14: Deactivate computer access following termination. (UPDATED)

It is important to follow rigorous procedures that disable all access paths into the organization's networks and systems for terminated employees.

What to do?

While employed, insiders have legitimate, authorized access to the organization's network, system, applications, and data. Once employment is terminated, it is important that the organization have in place and execute rigorous termination procedures that disable all access points available to the terminated employee. Otherwise, the organization's network is vulnerable to access by a now-illegitimate, unauthorized user. Some organizations choose to permit continued access by former employees for some time period under favorable termination circumstances; it is important that organizations have a formal policy in place for these circumstances and carefully consider the potential consequences. In addition, it is important to manage the access of employees who change their status with the organization (e.g. change from an employee to a contractor; change from a full-time to part-time employee; or take a leave of absence).

If formal termination policies and procedures are not in place, the termination process tends to be ad hoc, posing significant risk that one or more access points will be overlooked. The *Insider Threat Study* shows that insiders can be quite resourceful in exploiting obscure access mechanisms neglected in the termination process. If a formal process exists, it must be strictly followed. It is also critical that organizations remain alert to new insider threat research and periodically review and update these processes. If at the time of termination the organization has not been diligently following strict account management practices, it may be too late to perform an account audit for the terminating employee. A backdoor account could have been created months before, and verification of the legitimacy of all accounts of all types–system login accounts, VPN accounts, database or application accounts, email accounts, and so on—can be a very time-consuming process, depending on the size of the organization. When an employee leaves, the organization should be able to confidently say it disabled all access paths available to that employee

Some aspects of the termination process are quite obvious, such as disabling the terminated employee's computer account. However, organizations that have been victims of insider attacks were often vulnerable because of poor, non-existent, or non-comprehensive account management procedures. Many employees have access to multiple accounts; *all* account creations should be tracked and periodically reviewed to ensure that all access can be quickly disabled when an employee is terminated.

Accounts sometimes overlooked in the termination process are shared accounts, such as system administrator accounts, database administrator (DBA) accounts, and testing, training, and external organizational accounts, such as vendor accounts. In addition, some applications require administrative accounts that are frequently shared among multiple users. It is important that the organization meticulously maintain a record of every shared

account and every user authorized to have the password to each and change those accounts when employees are terminated.

Remote access is frequently exploited by former insiders. Remote access or virtual private network (VPN) accounts must be disabled, as well as firewall access, in order to prevent future remote access by the terminated employee. In addition, any remote connections already open by that employee at the time of termination must be closed immediately.

If an employee is terminated under adverse circumstances, the organization might consider reviewing the employee's desktop computer and system logs to ensure no software or applications have been installed that may permit the employee back into the organization's systems. In one case, a terminated employee left software on his desktop that allowed him to access it, control it remotely, and use it to attack his next employer. In addition, a few insiders who stole intellectual property immediately before leaving the organization were caught when their desktop computer activity logs were analyzed.

In summary, a layered defense that accounts for all access methods should be implemented. Remote access should be disabled, but if an obscure remote access method is overlooked, the next layer of defense is accounts. All accounts should be disabled for use by the former employee, so that even if remote access is established, the insider is prevented from proceeding further. Therefore, it is important that intranet accounts, application-specific accounts, and all other accounts for which the user was authorized be disabled or the passwords changed. Also, keep in mind that if the terminated insider was responsible for establishing accounts for others, such as employees, customers, or external web site users, then those accounts could also be accessible to the terminated insider.

Finally, termination procedures must include steps to prevent physical access. Insiders have exploited physical access to gain access to their former employer's systems. Careful attention should be paid to disable access by collecting keys, badges, parking permits, and disabling access to facilities in card control systems. When employees are fired, it is important that other employees are aware that the person was terminated. Multiple insider attacks were facilitated when terminated employees were able to obtain physical access to the organization by piggy backing through doors, using the excuse that they forgot their badge.

Case Studies: What could happen if I don't do it?

A credit union's system administrator was terminated suddenly with no notice that his employer was dissatisfied with his work. That night he suspected that his replacement, who he felt was technically inferior, had not disabled his access. He attempted to access the system from home and found that his replacement had failed to disable his access through the company firewall. Although his account had been disabled, she had failed to change the password of the system administrator account. The insider used that account to shut down the organization's primary server, one that had been having problems and had in fact crashed the previous weekend (and had taken him an entire weekend to bring

up again). It took the credit union three days to bring the server back into service; during that time none of its customers were able to access any of their accounts in any way. This case illustrates the necessity of thoroughly disabling access, as well as the consequences when an organization has no competent backup for a single system administrator.

In another case, a system administrator logged in one morning and was notified by her custom-written login software that her last login was one hour earlier. This set off immediate alarms, as she had in fact not logged in for several days. She had previously taken steps to redirect logging of actions by her account to a unique file rather than the standard shell history file. Therefore, she was able to trace the intruder's steps and saw that the intruder had read another employee's email using her account, then deleted the standard history file for her account so that there would be no log of his actions.

The login was traced to a computer at a subsidiary of the company. Further investigation showed that the same computer had logged into the company's system periodically for the past month. Monitoring revealed that a former employee had accessed up to sixteen of his former employer's systems on a daily basis during working hours. The insider

- gained access to at least 24 user accounts
- read electronic mail
- reviewed source code for his previous project
- deleted two software modification notices for the project

The former employee had been terminated for non-performance and then went to work for the subsidiary. This case illustrates the importance of terminating access completely for former employees, careful monitoring for post-termination access, and paying particular attention to terminated technical employees.

Recent Findings

Recent cases reveal that organizations are still finding it difficult to completely disable access for terminated employees. Many commonly accepted best practices are still not being followed, as illustrated in the case below. In addition to IT sabotage, employers need to be concerned about reach back into the organization's intellectual property by previous employees wishing to use or sell that information, or just out of simple curiosity.

In one recent case, the Vice President of Technology at a finance market information publisher was dismissed after five years due to a disagreement with the organization. He oversaw the company's computer network and internal email system. Three years after termination, he went back into his former company's email system to eavesdrop on top executive's emails about employees' job status.

The insider spied on email traffic from his home over a five-month period, curious about which employees were being terminated. He intercepted the emails of the human resources director and high-level executives that discussed employees' termination. The insider notified those employees of their possible terminations. The employees who received the email warning notified their supervisors, who initiated an investigation.

During the investigation it was determined that the organization's usernames/passwords virtually did not change for the entire three-year period.

Practice 15: Implement secure backup and recovery processes. (UPDATED)

Despite all of the precautions implemented by an organization, it is still possible that an insider will successfully attack. Therefore, it is important that organizations prepare for that possibility and enhance organizational resiliency by implementing secure backup and recovery processes that are tested periodically.

What to do?

Prevention of insider attacks is the first line of defense. However, experience has taught that there will always be avenues for determined insiders to successfully compromise a system. Effective backup and recovery processes need to be in place and operational so that if compromises do occur business operations can be sustained with minimal interruption. Our research has shown that effective backup and recovery mechanisms can make the difference between

- several hours of downtime to restore systems from backups
- weeks of manual data entry when current backups are not available
- months or years to reconstruct information for which no backup copies existed

Backup and recovery strategies should consider the following:

- controlled access to the facility where the backups are stored
- controlled access to the physical media (e.g., no one individual should have access to both online data and the physical backup media)
- separation of duties and two-person rule when changes are made to the backup process

In addition, accountability and full disclosure should be legally and contractually required of any third-party vendors responsible for providing backup services, including offsite storage of backup media. It should be clearly stated in service level agreements the required recovery period, who has access to physical media while it is being transported offsite, as well as who has access to the media in storage. Furthermore, case examples throughout this report have demonstrated the threat presented by employees of trusted partner organizations; the mitigation strategies presented for those threats should also be applied to backup service providers.

When possible, multiple copies of backups should exist, with redundant copies stored offsite in a secure facility. Different people should be responsible for the safekeeping of each copy so that it would require the cooperation of multiple individuals to compromise the means to recovery. An additional level of protection for the backups can include encryption, particularly when the redundant copies are managed by a third party vendor at the offsite secure facility. Encryption provides an additional level of protection, but it does come with additional risk. The two-person rule should always be followed when managing the encryption keys, so that you are always in control of the decryption process in the event the employees responsible for backing up your information leave the organization.

System administrators should ensure that the physical media on which backups are stored are also protected from insider corruption or destruction. Insider cases in our research have involved attackers who

- deleted backups
- stole backup media (including offsite backups in one case)
- performed actions that could not be undone due to faulty backup systems

Some system administrators neglected to perform backups in the first place, while others sabotaged established backup mechanisms. Such actions can amplify the negative impact of an attack on an organization by eliminating the only means of recovery. To guard against insider attack, organizations should

- perform and periodically test backups
- protect media and content from modification, theft, or destruction
- apply separation of duties and configuration management procedures to backup systems just as they do for other system modifications
- apply the two-person rule for protecting the backup process and physical media, so that one person can not take action without the knowledge and approval of another employee

Unfortunately, some attacks against networks may interfere with common methods of communication, thereby increasing uncertainty and disruption in organizational activities, including recovery from the attack. This is especially true of insider attacks, since insiders are quite familiar with organizational communication methods and, during attack, may interfere with communications essential to the organization's data recovery process. Organizations can mitigate this effect by maintaining trusted communication paths outside of the network with sufficient capacity to ensure critical operations in the event of a network outage. This kind of protection would have two benefits: the cost of strikes against the network would be mitigated, and insiders would be less likely to strike against connectivity because of the reduced impact.

Case Studies: What could happen if I don't do it?

Centralization of critical assets and sabotage of backups has enabled some insiders to amplify the impact of their attacks by eliminating redundant copies and avenues for recovery. One insider, the sole system administrator, centralized the only copy of all of the company's critical production programs on a single server and convinced management to institute policies mandating this practice. That server was later the target of a logic bomb written by the same insider. No other current copy of the software was available to recover from the attack, since he had also requested and received, through intimidation, the only backup tape, violating company policy. The logic bomb, which deleted all of the company's programs, cost the company millions of dollars and caused company-wide layoffs. While centralization can contribute to the efficiency of an organization, care must be taken that backups are performed regularly and are protected to ensure business continuity in the event of damage to or loss of centralized data.

In another case, an insider was terminated because of his employer's reorganization. The company followed proper procedure by escorting the insider to his office to collect his belongings and then out of the building. The IT staff also followed the company's security policy by disabling the insider's remote access and changing passwords. However, they overlooked one password that was known to three people in the organization. The terminated insider used that account to gain access to the system the night of his termination and to delete the programs he had created while working there. Some of these programs supported the company's critical applications.

Restoration of the deleted files from backup failed. Although the insider had been responsible for backups, company personnel believe that the backups were not maliciously corrupted. The backups had simply not been tested to ensure that they were properly recording the critical data. As a result, the organization's operations in North and South America were shut down for two days, causing more than $80,000 in losses. This case illustrates the delay that can be caused in recovery following an insider attack if backups are not tested periodically.

Recent Findings

Organizations continue to have non-existent or faulty backup and recovery programs in place, leading to devastating losses from insider attack. In one recent case, an insider left his employer, an Internet service provider (ISP), abruptly and without explanation but apparently due to disagreement about financial compensation. Shortly after quitting, the insider demanded back salary, but the company declined to pay. While suing the company, the insider remotely deleted critical software that supported customer Internet service. The systems were down for three days while the company rewrote the deleted software–no backups were available for restoration. The company's losses totaled about $120,000.

In another recent case, an insider worked for an (ISP) that provided wired and wireless Internet service to residential and business customers. As part of its service, the organization provided communication services in interstate and foreign commerce and communication. The ISP's technology used wireless radio (Wi-Fi) signals between radio towers and its customers' wireless access points. Radio towers and access points were operated by computers at the organization's facilities.

The insider left the ISP over business and financial disputes and went to work for a direct competitor. In his attack on his ex-employer's network, the insider used administrator accounts to take control of ISP's network. He reprogrammed 110 of the ISP's customers' wireless access points to cut off their Internet service. He executed his written programs/commands on the radio-tower computers. The execution caused the radio-tower computer to send commands to customers' access points, which prevented customers from accessing the Internet. The disconnected services included the service of one customer who was relying on electronic mail for news of an organ donor.

Unfortunately, no recovery plan for remote access to customer configurations had ever been conceived. Unable to remotely repair the network, the ISP dispatched technicians to the premises of the subscribers who lost Internet access. Servicing all customers took the ISP three weeks, leaving some customers without Internet access for that entire time period. The insider's action also caused the ISP's access points to repeatedly broadcast radio signals that interfered with the signals of another ISP.

In total, more than 170 customers (including individuals, families, and businesses) lost Internet service, some of them for as long as three weeks, and collectively caused more than $65,000 in losses.

Practice 16: Develop an Insider Incident Response Plan. (NEW)

Procedures for investigating and dealing with malicious insiders present unique challenges; response must be planned, clearly documented, and agreed to by organization managers and attorneys.

What to do?

An incident response plan for insider incidents differs from a response plan for incidents caused by an external attacker. The organization needs to minimize the chances that the insider perpetrator is assigned to the response team or is aware of its progress. This is challenging since the technical people assigned to the response team may be among the employees with the most knowledge and ability to use their technical skills against the organization. Another challenge of insider incident response is the hesitation or resistance that managers may have to participating in an investigation. This hesitation could have several causes: it could divert their team's resources from business-critical activities, expose a team member to investigation, or expose shortcomings by management or oversights in system security, opening them up to embarrassment or liability for losses.

The organization needs to develop an insider incident response plan with the rights of everyone involved in mind. Specific actions to control damage by malicious insiders should be identified, together with the circumstances under which those efforts are appropriate. The plan should describe the general process to be followed and the responsibilities of the members of the response team. A mediator for communication between the departments of the organization needs to be assigned that is trusted by all department heads. The department heads need to understand the plan and what information can and cannot be shared in the investigation of the incident.

The details of the insider incident response plan probably would not be shared with all organization employees. Only those responsible for carrying out the plan need to understand it and be trained on its content and execution. Employees may know of its existence and should be trained on how to (anonymously) report suspicious behavior, as well as specific types of suspicious behaviors that should be reported. Managers need to understand how to handle personal and professional problems and when they might indicate increased risk of insider compromise. If the organization experiences damage due to a malicious insider or if other risks evolve, such as new forms of internal or external attack, the employee training should be updated. Lessons learned from insider incidents should be fed back into the insider incident response plan to ensure its continual improvement.

Case Studies: What could happen if I don't do it?

One insider of a lottery agency turned losing lottery tickets into winners to steal nearly $63,000 over a year and a half. To carry out the scam, he purchased a ticket as usual, then modified it to be a winner in the lottery agency's database. When the lottery agency discovered the fraudulent tickets, they started an investigation. Fortunately, the insider was on vacation or he would have been chosen to investigate the incident. Upon his return, when confronted with the fraudulent tickets, the insider behaved suspiciously, and therefore was put on administrative leave and his physical access was disabled.

While the organization took the right actions to remove the suspect from the organization, they neglected to inform coworkers of the action, so the insider still had managerial control of organization personnel. Before he left on administrative leave, the insider deleted a history log that may have proven his criminal act. He also asked one of his colleagues to delete four weeks of backup tapes, claiming that they wouldn't be useful under a new backup data format that was being implemented. The colleague complied with this request and the organization lost much of the evidence of the insider's tampering with system security controls. The insider also asked a different colleague to retrieve some additional backup tapes for him that would help him prove his innocence. The colleague complied, and the organization never recovered those tapes. If the organization had a coherent insider incident response plan in place and employees educated on their responsibilities for responding to the insider's requests, the organization may have been better able to respond to the insider's fraud.

In another case, an assembly inspector at a manufacturing plant complained to management about the lack of support given to inspectors to do their job, saying that inspectors are pressured to approve work regardless of quality. Despite the fact that an independent evaluator determined that his claims were unfounded, the insider threatened to sue the company and offered his silence for a cash settlement. This extortion attempt was declined by the company and no further action was taken until years later when newspaper articles began appearing divulging some of the company's proprietary information. After receiving an anonymous tip that the insider was responsible for the leaks, the organization started an investigation.

Working with law enforcement, the organization found evidence that the insider had been downloading the organization's confidential information, which was outside his area of responsibility, for over two years. The insider had downloaded massive amounts of information using a USB removable storage drive and stored it at his residence. The investigation also found evidence of the insider's email correspondence with reporters discussing the proprietary documents, articles, and meetings. While hindsight is 20/20, if the organization had executed an incident response plan at the time of the attempted extortion, it may have prevented the insider's follow-on actions and have been able to prevent the flow of its confidential information to the media.

References/Sources of Best Practices

Alberts, Christopher; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; and Zajicek, Mark. *Defining Incident Management Processes for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html.

British Standards Institute. http://www.bsigroup.com/.

CERT. Survivability and Information Assurance Curriculum (SIA). http://www.cert.org/sia.

CERT. Virtual Training Environment (VTE). https://www.vte.cert.org/.

Corporate Information Security Working Group (CISWG). Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. "Report of the Best Practices and Metrics Teams," 2005. http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661.

Department of Homeland Security, National Cyber Security Division. *Build Security In*. https://buildsecurityin.us-cert.gov/daisy/bsi/home.html.

Federal Financial Institutions Examination Council. *FFIEC Information Technology Examination Handbook.* http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

Information Security Forum. *The Standard of Good Practice*. http://www.isfsecuritystandard.com/.

Information Systems Audit and Control Association. http://www.isaca.org.

International Standards Organization. "Information technology -- Security techniques -- Code of practice for information security management," (ISO/IEC 17799:2005/Cor 1:2007), 2007. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46381 .

International Standards Organization. "Information technology -- Security techniques -- Information security management systems – Requirements," (ISO/IEC 27001:2005), 2005. http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=4210.

MasterCard Worldwide. *The MasterCard SDP Program (Site Data Protection)*. https://sdp.mastercardintl.com/pdf/pcd_manual.pdf.

National Institute of Standards and Technology. Special Publications (800 Series). http://csrc.nist.gov/publications/PubsSPs.html.

United Kingdom Office of Government Commerce, Information Technology Infrastructure Library. http://www.ogc.gov.uk/index.asp?docid=1000368.

Visa. *Cardholder Information Security Program.* http://usa.visa.com/merchants/risk_management/cisp_tools_faq.html.