Chapter 6

Best Practices for the Prevention and Detection of Insider Threats

This chapter describes 16 practices, based on existing industry-accepted best practices, providing you with defensive measures that could prevent or facilitate early detection of many of the insider incidents other organizations experienced in the hundreds of cases in the CERT insider threat database.[1]

This chapter was written for a diverse audience. Decision makers across your organization will 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 personnel from your management, human resources, information technology, software engineering, legal, and security teams,

[1] This chapter includes portions from "Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition–Version 3.1, " by Dawn Cappelli, Andrew Moore, Randall Trzeciak, and Timothy J. Shimeall.

along with your data owners, understand the overall scope of the problem and communicate it to all employees in your organization.

We briefly describe each practice, explain what you should do, and provide a few actual case examples illustrating what could happen if the practice is not implemented. Finally, we describe how the practice could have prevented an attack or facilitated early detection.

While you read, please remember everything else you have read so far in this book regarding contractors and trusted business partners. Although we usually use the term *employee* in this chapter, much of this chapter also applies to contractors and trusted business partners. Please keep this in mind, and do not overlook those insiders!

Summary of Practices

Each of the 16 practices is summarized here and then expanded on in the following sections.

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

  It is difficult for you to balance trusting your employees, providing them access to achieve your mission, and protecting your assets from potential compromise by those same employees. Insiders' access, combined with their knowledge of your technical vulnerabilities and vulnerabilities introduced by gaps in business processes, gives them the ability and opportunity to carry out malicious activity against you 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 you to take an enterprise-wide view of information security, first determining your critical assets, and then defining a risk management strategy for protecting those assets from both insiders and outsiders.

- ***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, fraud, and IT sabotage, in the CERT database. Specific policies are discussed in this practice. In addition, consistent policy enforcement is important. Some employees in our cases 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.***

  A culture of security awareness must be instilled in your organization so that all employees understand the need for policies, procedures, and technical controls. All employees in your 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 your mission. Each employee needs to understand your security policies and the process for reporting policy violations.

- ***Practice 4: Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.***

  You should attempt to identify suspicious or disruptive behavior by individuals before they are hired, and closely monitor employee behavior 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.

- ***Practice 5: Anticipate and manage negative workplace issues.***

  This practice describes suggestions beginning with preemployment issues, continuing through employment, and including termination issues. For example, you 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 coworkers 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.

- ***Practice 6: Track and secure the physical environment.***

  While employees and contractors obviously must have access to your 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 nonpublic areas of your facilities. This practice details lessons learned from cases in the CERT database in which physical access vulnerabilities allowed an insider to attack.

- ***Practice 7: Implement strict password and account management policies and practices.***

  No matter how vigilant you are in trying to prevent insider attacks, if your 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.

- ***Practice 8: Enforce separation of duties and least privilege.***

  If 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 reduced. 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.

- ***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, such as those involving insiders who took advantage of inadequate separation of duties, have an indirect tie. This practice 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.***

  System administrators and privileged users such as database administrators (DBAs) have the technical ability and access to commit and conceal malicious activity. Technically adept individuals are more likely to resort to technical means to exact revenge for perceived wrongs. Techniques such as separation of duties or the two-person rule for critical system administrator functions, nonrepudiation 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.

- ***Practice 11: Implement system change controls.***

  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, unauthorized hardware, logic bombs, or other malicious programs on the system or network. These types of attacks are stealthy and therefore difficult to detect, but technical controls can be implemented for early detection. Once baseline software and hardware configurations are characterized, comparison to the current configuration can detect discrepancies and alert managers for action.

- ***Practice 12: Log, monitor, and audit employee online actions.***

  If account and password policies and procedures are enforced, you 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 systems, download of confidential or sensitive information such as intellectual property (IP), customer or client information, and Personally Identifiable Information (PII) can be detected via data-leakage tools.

- ***Practice 13: Use layered defense against remote attacks.***

  If employees are trained and vigilant, accounts are protected from compromise, and employees know that their actions are being logged and monitored, 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, you 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 your equipment is particularly important for terminated employees.

- ***Practice 14: Deactivate computer access following termination.***

  When an employee or contractor terminates employment, whether the circumstances were favorable or not, it is important that you have in place a rigorous termination procedure that disables all of the employee's access points to your physical locations, networks, systems, applications, and data. Fast action to disable all access paths 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.***

  No organization can completely eliminate its risk of insider attack; risk is inherent in the operation of all organizations. 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 you 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 practice contains descriptions of insider threat cases in which the organization's lack of attention to incident response and organizational resiliency resulted in serious disruption of service to its customers.

- ***Practice 16: Develop an insider incident response plan.***

  You 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 the insiders who can use their technical skills against you. 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 you have evidence in hand to identify the insider and follow up appropriately. Lessons learned should be used to continually improve the plan.

Practice 1: Consider Threats from Insiders and Business Partners in Enterprise-Wide Risk Assessments

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

What Can You Do?

It is not practical for most organizations to implement 100% protection against every threat to every organizational resource. Therefore, it is important to focus on protecting your critical information and 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 your mission from both external and internal threats.

Risk is the combination of threat, vulnerability, and mission impact. Enterprise-wide risk assessments help identify critical assets, potential threats to those assets, and mission impact if the assets are compromised. You should use the results of the assessment to develop or refine your overall strategy for securing your systems, striking the proper balance between countering the threat and accomplishing your mission.[2]

You need to understand the threat environment under which your systems operate in order to accurately assess enterprise risk. Characterization of the threat environment can proceed in parallel with evaluation of the vulnerability and its impact. However, the sooner the threat environment can be characterized, the better. The purpose of this practice is to assist you in correctly assessing the insider threat environment, your vulnerabilities that enable that 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 you recognize the potential danger posed by the knowledge and access of your employees, contractors, and business partners, and specifically address that threat as part of an enterprise risk assessment.

[2] See www.cert.org/resilience/.

Understanding your vulnerability to a threat is also important, but organizations often focus 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. You 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. Organizations are increasingly outsourcing critical business functions. As a result, people external to your organization sometimes have full access to your policies, processes, information, and systems; access and knowledge previously only provided to your employees. You need to recognize the increased risk; your enterprise boundary includes all people who have an understanding of and privileged access to your organization, information, and information systems.

Insider threats may impact the integrity, availability, or confidentiality of information critical to your 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 those types of insider incidents, 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?

> An 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 the organization the passwords for its system administrator accounts. Over a period of three days, the insider modified the systems so that employees could not access them, defaced the company Web site, and deleted files.

It is critical that you consider the risk you assume when you place all system administration power into the hands of a single employee. Even if you are part of a large organization, do not overlook small development teams, stand-alone machines, and other independently maintained systems in your organization that are not a part of your enterprise infrastructure. We know from doing insider threat assessments that even the largest organizations have these types of systems, which can be a part of critical projects and development or even production systems. Worst of all, there likely has been no formal risk assessment performed that accounts for potential insider threats.

> One 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. The manufacturer 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, 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, you should consider provisions in your 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 your facilities or systems. You could require notification a specified amount of time before the action is taken against the contractor, in order to perform your own risk assessment for the potential threat posed to your network, systems, or information.

> A computer help desk attendant employed by a government contractor created fake government email addresses on the government systems for which he was responsible. He then used those email addresses to request replacement parts for 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.

> He received almost 100 shipments with a retail value of almost $5 million and sold the equipment on the Internet.

This incident indicates the need to have transaction verification built into supplier agreements. Even though operations might be outsourced, you still need to include those operations in your enterprise risk assessment so that you can ensure that your trusted business partners implement adequate controls against insider threat in their organizations.

> A system administrator had authorized access to sanitized databases of customer information on an FTP server hosted by one of his organization's business partners. The business partner was contracted by financial institutions and phone companies to perform services using customer data. He located an unsanitized version of these customer databases when looking around on the FTP server. The databases were protected with passwords and encryption. The insider ran a password cracking utility and obtained more than 300 passwords he could use to access the protected information. He found original and complete phone records, billing information, and other PII for millions of Americans. He proceeded to download millions of customer records from the databases, including Social Security numbers, birthdates, and other personal information. The insider bragged in online IRC channels about his access to confidential and personal data, and was asked at one point by another individual in the chat room to provide data on an FBI agent who was actively investigating him. The insider provided the information within minutes. The ongoing FBI investigation of that individual led back to the insider, who was found with dozens of CDs and other media containing millions of customer records in his apartment.

In this case, proprietary information from the original organizations' customers was inadequately protected from access by a third organization that was subcontracted by a second organization, the trusted business partner. Legal controls to ensure contractor compliance with your data-handling policies could be employed to protect against the extended pool of insiders created by working with vendors and other external partners. These measures would allow contractors to perform their work, while protecting your sensitive information.

Practice 2: Clearly Document and Consistently Enforce Policies and Controls

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

What Can You 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.

You should ensure the following with regard to your 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

You should be particularly clear on policies regarding

- Acceptable use of your 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 your organization, they should receive a copy of your policies that clearly lays out what is expected of them, together with the consequences of violations. You should retain evidence that each individual has read and agreed to your policies.

Employee disgruntlement was a recurring factor in insider incidents; particularly in insider IT sabotage cases. As explained in Chapter 2, Insider IT Sabotage, disgruntlement is usually caused by some unmet expectation on the part of 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. You 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?

> Two contractors were formerly employed as software developers for a company that provided news filtering and distribution services to Web sites. In response to their termination, their legal counsel faxed a letter to the company. The letter insisted that the insiders owned the software they had created during their employment, and demanded that the company stop using the software and return all copies to them. On the evening before a holiday, the insiders used a home computer and their own credentials, which were still active, to remotely access the company's network and download the proprietary software and business plans. The insiders were arrested after the company discovered the unauthorized access, and connected them to the theft using their usernames and system logs.

In this case, it is clear that there was confusion regarding who owned the software the contractors had created for the company. Intellectual property ownership should be documented in formal policies that are clearly communicated to all employees and contractually enforced for all contractors and trusted business partners. In addition, you should have your employees re-sign the agreements periodically. We have discussed this with several organizations who instituted IP agreements for all employees more than 20 years ago. All employees signed them at that time, and all new employees now sign them. However, some employees have not signed again since they originally signed more than 20 years ago! It is debatable whether those aged agreements would stand up in a court of law!

You might also consider incorporating a new angle into your IP agreements to protect yourself from being the unknowing recipient of stolen IP from *another* organization. As part of your IP agreement that you make new employees sign, you might want to include a statement attesting to the fact that they have not brought any IP from any previous employer with them to your organization.

> 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 database 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 confidential company information to the media to force the company to deal with the problem.
- An insider, who was upset about his company's practice of canceling 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 these organizations.

Practice 3: Institute Periodic Security Awareness Training for All Employees

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

What Can You 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 in the CERT database 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. There is not one demographic profile for a malicious insider.

Security awareness training should encourage observation of behavior in the workplace to identify employees who may be at higher risk of malicious activity, 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 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)

Your managers and employees need to be trained to recognize recruitment in which an insider engages other employees to join his 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 to gain either physical access or electronic access via accounts and passwords. Some of the CERT database cases reveal social engineering of a different type, however. In one 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 nontechnical 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 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 your organization and include all personnel. For effectiveness and longevity, the measures used to secure your 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 your organization places a high value on customer service quality, you may view customer information as its most critical asset and focus security on protection of your data. Your organization could train your employees 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—for example, 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 policies, and include 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. Your employees need to understand your organization's policies and procedures, and be aware that your managers will respond to security issues in a fair and prompt manner.

Your 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.

As described in Chapter 4, Insider Fraud, in many of the insider fraud incidents 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 PII to her boyfriend, who used it to open and make purchases on fraudulent credit card accounts.

You should educate your 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 many of the fraud cases where insiders modified information for financial gain, the insider recruited at least one other employee in the organization 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 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. Your 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.

In Chapter 3, Insider Theft of Intellectual Property, we indicated that many cases involve technical employees who stole their organization's intellectual property because of dissatisfaction. 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.

Finally, your employees need to be educated about the confidentiality and integrity of your company's information, and that compromises will be dealt with immediately. Some insiders in the CERT database did not understand this, viewing information as being their own property rather than the organization's; for example, customer information developed by a salesperson or software developed by a programmer.

Case Studies: What Could Happen if I Don't Do It?

> A contractor was employed as a programmer by a high-technology company. He requested to work remotely from home, his request was denied, and he informed the organization that he would be resigning. He actually had obtained employment with a competitor. On the evening before his last day of work, he returned to the facility, outside of normal work hours. He entered a building which was not his normal work location and removed the name plate from an engineer's office. He then asked a janitor to let him in, claiming it was his office and he'd been accidentally locked out. The janitor complied with the request; the insider now had physical access to all of the computers in the engineer's office.

You probably think you know the ending to this case, right? He stole the information and left the office. Not quite; read on…

> The engineer who occupied that office happened to walk in—and caught the insider in the act of stealing his proprietary source code from his computer. The insider quickly made up a false explanation as to why he was there, and promptly left. The following day, the insider reported for his last day of work, and was observed leaving with a CD. The organization reported him to law enforcement, thinking he might have stolen

> its intellectual property on the CD. An investigation confirmed the theft, specifically of proprietary source code. The contractor was arrested, convicted, and sentenced to one year of work furlough.

This case demonstrates many interesting security awareness issues. First, would your custodial staff or security guards fall for that scheme? Don't forget them when preparing and delivering your security awareness training! Second, do you educate your employees to report suspicious activity in their offices? Would they fall for this ploy? What would your employees do if they caught someone in their office after hours? Finally, there is good news at the end of this case: The organization was suspicious enough to notify law enforcement of the departing contractor carrying a CD out with him.

> The lead developer of a mission-critical safety-related application had extensive control over the application source code. The only copy of the source code was on his 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.
>
> 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.

This case could have had dire consequences due to the critical nature of the application. How could the problem have been avoided? We could say that management should have had more direct oversight of the development process, but the malicious insider was the lead developer, so you can't necessarily blame management completely. However, the insider's team members were aware of the insider's deliberate inaction; they could have informed management of his statements and actions in time to prevent the attack. This case demonstrates the importance of educating all of your employees that the security and survivability of the system is everyone's responsibility, as well as clear procedures for reporting concerning behavior.

Practice 4: Monitor and Respond to Suspicious or Disruptive Behavior, Beginning with the Hiring Process

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

What Can You Do?

Your approach to reducing the insider threat should start in the hiring process by performing background checks and evaluating prospective employees 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. When creating a preemployment screening policy or other policies recommended in this practice, it is important to keep in mind privacy and legal requirements (e.g., notification of the candidate).

Recall from Chapter 2 that 30% of the insiders who committed IT sabotage in our original study with the Secret Service had a previous arrest history, including arrests for violent offenses (18%), alcohol- or drug-related offenses (11%), and nonfinancial/fraud-related theft offenses (11%).[3] In fact, some of those insiders had been arrested for multiple offenses. 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 it is appropriate to give the new employee access to critical, confidential, or proprietary information or systems.

In addition to screening for potential red flags during the hiring process, you also should invest time and resources in training your 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.

[3] See [Keeney 2005].

It is important that you consistently investigate and respond to all rule violations committed by your employees and contractors.

Given that financial gain is a primary motive for much insider fraud, you 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 financial need. In addition, recall from Chapter 4 that fraud may involve theft or modification of small amounts of data (e.g., Social Security numbers) repeatedly over long periods of time. This suggests that for fraud crimes there is ample time to catch the insider in the act while still employed by you. In addition, 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. These crimes also had a high rate of collusion with both insiders and outsiders. Secretive meetings among employees and obvious attempts to deceive the organization about outside relationships are of concern.

In Chapter 3, Insider Theft of Intellectual Property, we described that these crimes tend to involve larger amounts of data (e.g., proprietary source code) and often occur within one month of the insider's resignation. However, many of the incidents involve 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 some of those incidents, 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. As with insider fraud, suspicious interactions among employees and obvious attempts to deceive the organization about outside business relationships are of concern.

As we described in Chapter 2, Insider IT Sabotage, insiders have also become disgruntled due to professional stressors, including financial compensation issues, problems with a supervisor, hostile working environments, and layoffs. Often, the first sign of disgruntlement is the onset of concerning behaviors in the workplace. Unfortunately in many of our cases, the concerning behaviors were not recognized by management prior to the incidents, or the organization failed to take action to address the behaviors.

Policies and procedures should exist for your employees to report concerning or disruptive behavior by coworkers. While frivolous reports need to be screened, all reports should be investigated. If one of your employees exhibits suspicious behavior, you should respond with due care. Disruptive employees should not be allowed to migrate from one position to another within your organization, evading documentation of disruptive or concerning activity. Threats, boasting about malicious acts or abilities ("You wouldn't believe how easily I could trash this net!"), and other negative sentiments should also be treated as concerning behaviors. 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 should be aided in the resolution of those difficulties.

Once concerning behavior is identified, several steps may assist you 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 examine recent online activity by the employee or contractor. While this is done, you should provide options to the individual for coping with the behavior, perhaps including access to a confidential employee-assistance program.

Suspicious behaviors, if detected, provide you an opportunity to recognize a higher risk of insider threat and act accordingly. Often, coworkers are aware of issues; anonymous means for reporting coworker suspicions should be in place and communicated to your employees.

Keep in mind that legal and employee privacy issues must be considered when implementing this practice. It is very important that you work with your legal department in developing these types of policies and procedures!

Case Studies: What Could Happen if I Don't Do It?

> A subcontractor worked 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 coconspirator's name and address. He 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.

Background checks should be required for all potential employees, including contractors and subcontractors.

> A former system administrator at a university's cancer institute deleted 18 months of cancer research after quitting because of personality and work ethic differences between himself, his supervisor, and his coworkers. He had been the sole system administrator on the cancer research project team. On numerous occasions he had displayed aggressive and malicious (nontechnical) behaviors before quitting his job. He was not liked by his coworkers, but was seen as a "necessary evil" for his skills. He was described as very lazy—slacking on the job—but they didn't know how to get rid of him. A few days after quitting, he returned to the lab. His badge had been disabled, so he could not enter on his own; therefore, he asked an employee who recognized him to let him in. Once inside the building, he used a key that had not been confiscated to enter the office and delete the cancer research.

In this case, the employee obviously exhibited concerning behaviors in the workplace. As stated earlier, it is important to have established policies and procedures for dealing with concerning behaviors in the workplace.

Practice 5: Anticipate and Manage Negative Workplace Issues

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

What Can You 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, work 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 policies, it may lead to animosity within the workplace. In many of our cases, 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 your employees have issues, whether they are justified or not, they need an avenue 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 fraud 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 your employees are aware of and sign intellectual property agreements and noncompete agreements. 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 your 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, your termination process should include a step to retrieve all organization property from terminating employees. They should be required to return all property, including computers and accessories, software and hardware, confidential information, source code and compiled code, mobile devices, removable media, and any other items that contain sensitive, confidential, or intellectual property owned by you. You should consider showing employees the signed copy of the intellectual property agreement and noncompete agreement and explaining the consequences for violating those policies as part of the employee termination process.

Case Studies: What Could Happen if I Don't Do It?

> A female employee who was a DBA 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, and disability claims, and caused the system to crash.

In this case, the organization did attempt to manage the negative workplace issues. Obviously, the human resources department was involved and progressive disciplinary actions were taken. Unfortunately, the problems were not resolved when she left the organization. In some cases, it is worth considering alternatives to sanctions in dealing with employee issues. This particular insider had been a stellar employee, but unfortunately her performance was affected by the team with which she worked. A transfer to another part of the organization might have been considered, in order to improve a negative situation for a historically excellent employee.

> A vice president for engineering who was responsible for oversight of all software development in the company was engaged in a long-running dispute with upper management. This dispute was characterized as verbal attacks by the insider and statements to colleagues about how much he had upset management. He 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 him to quit. When no severance package was offered, he copied a portion of the company's 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 company in this case had recognized that the warning signs—the disruptive behavior—could signal a potential insider attack, it could have secured its assets and substantial losses could have been avoided. It is critical that managers recognize, manage, and realize the potential consequences of negative workplace issues.

Practice 6: Track and Secure the Physical Environment

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

What Can You Do?

First and foremost, you must protect your most critical asset: your employees. This process begins by ensuring your office environment is free from occupational hazards and threats to employees from outsiders. While planning for the security of the physical environment, you 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 you can keep unauthorized people out of your facility, you 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 organization's physical security measures. Employee privacy and related laws should be considered when developing a secure physical environment. Commonly used physical security mechanisms, some that were effective and others that were inadequate, in our cases include the following.

- Maintaining a physical security presence on the facilities at all times. Some of the former employees in the CERT database 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 an organization-issued badge and requiring the use of that badge to navigate throughout the facility. One employee in the CERT database 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, and then sabotaged the computers in the network operations center. Another former employee "piggybacked" 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 your facility.
- Using closed-circuit cameras to record entry, exit, and critical operations at the facility. Some of the insiders in the CERT database were successfully identified and convicted through use of closed-circuit cameras or video surveillance.

Once the physical perimeter is as secure as possible, you 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 your 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 that they were unusable, slowing down or crippling the organization when it attempted to recover from the insider attack.

In addition to securing the critical assets housed in your computer facility, careful attention should be paid to the computers, workstations, laptops, printers, and fax machines located in all areas, both secured and not secured. 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.

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 smartphones) by requiring encryption and/or a multifactor authentication method.

To the greatest extent possible, attempts to access your 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 you to detect a security violation before major damage is inflicted.

Finally, you need to implement a strategy for tracking and disposing of documents that contain controlled information. In addition, precautions against insider threats must be applied to all employees, even if they apparently have no access to your computing resources. Several 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, and 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.

Case Studies: What Could Happen if I Don't Do It?

> An employee 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. Because he was suspended late Friday afternoon, his employer decided to wait until Monday morning to notify the energy management facility of his suspension. Late Sunday night he went to the energy production facility; he still had authorized access since facility personnel had not been notified of his suspension. He used a hammer to break the glass case enclosing the "Emergency power off button" and hit the button, shutting down some of the computer systems, including computers that regulated the exchange of electricity between power grids. 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.

This case raises important physical security and legal/contracting issues regarding contractors. These types of contracting issues were already discussed in Practice 1. This case serves as another example of why you should alter your contracting practices to require advance notification of pending employee sanctions by your subcontractors, and requiring immediate notification if one of the contractors is terminated or resigns. It also illustrates the potential damage that could be caused by the cascading effects from a disgruntled insider using physical sabotage to impact mission-critical systems.

Practice 7: Implement Strict Password- and Account-Management Policies and Practices

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

What Can You Do?

No matter how vigilant you are about mitigating the threats posed by insiders, if your 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 your systems for illicit purposes. Fine-grained access control combined with proper computer account management will ensure that access to all of your critical electronic assets is

- Controlled to make unauthorized access difficult
- Logged and monitored so that suspicious access can be detected and investigated
- Traceable 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
- Employees openly sharing passwords
- Employees storing passwords in clear-text files on their computers or in email
- Using unattended computers left logged in

Password policies and procedures should ensure that all passwords are strong,[4] 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.

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

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 the following:

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

The need for every account in your organization should be evaluated regularly. Limiting accounts to those that are 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 your organization's password- and account-management policies are also applied to all contractors, subcontractors, vendors, and other trusted business partners that have access to your information systems or networks. These policies should be written into your contracting agreements, requiring the same level of accountability in tracking who has access to your organization's systems. Contractors, subcontractors, 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, you should be notified in advance so that account passwords can be changed. Finally, be sure to include all shared accounts, including contractor, subcontractor, and vendor accounts, in the regularly scheduled password-change process.

The prevalence of outsourcing, supply-chain management, and the globalization of the marketplace has blurred the line between your boundary and the external world. It is increasingly difficult to tell the difference between insiders and outsiders when it comes to managing access to your 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 your contractor, subcontractor, and vendor relationships, you must recognize that insiders are no longer just employees within your four walls. Careful attention must be paid to ensure that the insiders employed by trusted business partners are managed diligently, only allowing them access to the information they need to fulfill their contractual obligations, and terminating their access when it is no longer needed.

Case Studies: What Could Happen if I Don't Do It?

> A computer administrator for an Internet service provider (ISP) quit his job after becoming dissatisfied, and began to write threatening emails to the ISP. He was able to retain partial access to the organization as a paying customer, and then exploited his knowledge of a company tool to elevate his privileges on the system to that of an employee. The ISP detected his unauthorized access in the log files, and disabled the insider's customer account. The insider, however, was able to continue attacking the organization using two other backdoor accounts he had created. He changed all administrative passwords, altered the billing system, and deleted two internal billing databases. It took an entire weekend to recover from the attack.

This case might not seem applicable to you if you are not an ISP, but take a moment to really think about whether you have any accounts for accessing your systems from outside by customers, vendors, partners, and so on. Remember that your insiders know your vulnerabilities and technical gaps!

> 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 the organization improved security training for employees on how and why to choose strong passwords.

This case ends up being a "good-news" case when you consider how the organization responded to the incident!

Practice 8: Enforce Separation of Duties and Least Privilege

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 Can You Do?

Separation of duties requires dividing functions among people to limit the possibility that one employee could steal information, commit fraud, or commit sabotage without the cooperation of another. One type of separation of duties, called the 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 nontechnical 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 reduces your risk of theft of confidential or proprietary information by your employees, since access is limited to only those employees who need access to do their jobs. Some cases of theft of intellectual property involved salespeople, 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 for reasons including promotions, transfers, relocations, and demotions. As employees change jobs, organizations often fail to review the employees' 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 his or her previous job that require access to information and information systems, the employee's access should be disabled when he or she assumes 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. Here are some examples:

- 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, you should include separation of duties in the design of your business processes and enforce them via a combination of technical and nontechnical means.

These principles have implications in both the physical and the virtual worlds. In the physical world, you 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 you 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.

It is important to understand that separation of duties alone is not always sufficient to protect against insider threats; it is one layer in a multitiered defense. Many of the insiders who committed fraud in the CERT database collaborated with at least one other insider to carry out the crime. 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 you implement a layered defense to decrease the likelihood of such an attack.

One pattern observed in multiple fraud 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.

Finally, it is important to design auditing procedures to detect potential collusion among employees, with the assumption that collusion to override separation of duties controls is quite possible.

Case Studies: What Could Happen if I Don't Do It?

> 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 approximately $700 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 CERT Program/Secret Service Insider Threat Study, told the study researchers that problems can arise when "the fox is guarding the henhouse" [Randazzo 2004]. Specifically, his 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 his 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 his activities and to cease raising concern, for fear he 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 your 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.

> 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. He 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.

Practice 9: Consider Insider Threats in the Software Development Life Cycle

Technical employees have taken advantage of defects introduced in the Software Development Life Cycle (SDLC) to deliberately perform malicious technical actions; likewise, nontechnical employees have recognized vulnerabilities and used them to carry out their fraudulent activities.

This best practice is described in detail in Chapter 5, Insider Threat Issues in the Software Development Life Cycle. A summary was intentionally left in this chapter to keep all 16 best practices in one location for easy reference.

What Can You Do?

Impacts from insiders that exploited defects in the SDLC include

- Closing of a business
- Fraud losses of up to $700 million
- Driver′s licenses created for individuals who could not get a legitimate license
- Disruption of telecommunications services
- Modification of court records, credit records, and other critical data
- A virus planted on customers′ systems

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

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

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 that 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 systems you build in-house and to those you acquire. 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 capability 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 its 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 fraud 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 18-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 backdoors and perhaps saved the company.

During the software development process, you 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 was 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 you 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.

- 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 Web site. Although it used a change-control system to track changes, it had no process for approval of changes before they were released to the Web site. As a result, a college intern, before leaving for the summer, published material intended to be a joke on the organization's Web site, causing quite a scandal and damage to the reputation of the government agency.

It is important that you carefully consider these types of issues as you 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. We know from our assessments and workshops 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 our 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 used by his project leader, who sat in a cubicle and often left the 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 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 thereafter, the logic bomb finally detonated, causing immense confusion and disruption to the company's services to its customers.

This case exemplifies many of the issues discussed in this section. The next case illustrates a more low-tech incident that was enabled by oversights in the SDLC, with serious consequences.

> The primary responsibility of a police communications operator was to communicate information regarding driver's 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 also could use other system functions. At that point, at the request of her accomplice, she began to generate, in return for payment, illegal driver's licenses for people who were unable to gain legitimate licenses. Fortunately, a confidential informant led to her arrest for fraudulently creating approximately 195 illegal driver's 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

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

What Can You Do?

Recall that the majority of the insiders who committed IT sabotage held technical positions such as system administrator, DBA, or programmer. Technically sophisticated methods of carrying out and concealing malicious activity included writing or downloading 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**[5] 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 you enforce 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 nonrepudiation of action ensure that online actions taken by users, including system administrators and privileged users, can be attributed to the person who performed them. Therefore, should malicious insider activity occur, nonrepudiation 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 nonrepudiation. However, keep in mind that system administrators and

[5] *Privileged users:* 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 because they have the ability to create new user accounts and control the access rights of users within their domain.

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 here ensure identification of users following detection of suspicious activity, additional steps must be taken to defend against 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.

As we described in Practice 6, 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 approximately $700 million over a five-year period.

Note that in order to enforce separation of duties for system administration functions, you must employ at least two system administrators. There are a few cases in this book in which the organization was victimized by its sole system administrator. Although many small organizations may not be able 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. You 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 paths 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 this case, the disgruntled insider planted his logic bomb in the script that propagated software to all of the company's servers nightly as part of its configuration-management process. This is an example of a file that should be carefully monitored for changes, as the repercussions of illicit modifications will impact every server in the organization.

> An employee 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 employee 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 more than $615,000 over almost two years.

This case illustrates what we mean by "privileged user." The "erosion of access controls" when employees move around within an organization presents a definite vulnerability. We know from our assessments and workshops that this is a very difficult problem that most organizations have not solved. Here is a control that one organization we work with has implemented: When an employee transfers within the organization, the organization sets the transfer date in a database. It has an automated script that sends an email to the manager of the team that the employee transferred *from* three months after the transfer. The script reminds the manager that the employee left, and lists all of the email aliases the employee is still on, all internal Web sites the employee still has access to, all shared folders the employee still has access to, and so on. The organization has found that a three-month transition period is typically the right amount of time in which employees need legitimate access to both their new and old team's information. After three months, the organization has found that most managers are ready to rescind access for their team's former employee.

The following case demonstrates how organizational failures in dealing with disgruntled system administrators and other privileged users can eventually result in IT sabotage.

> A developer of e-commerce software for an organization decided to move his family to a different state, and therefore he 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 him 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, he 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 more than $25,000, including 230 staff hours and associated costs.

In much of the text in this book we use the word *employees* when we really mean *employees and contractors.* This case points out that you cannot overlook contractors who have system administrator or privileged access to your systems, networks, and information.

Practice 11: Implement System Change Controls

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

What Can You Do?

Change controls are formal processes used to ensure that changes to a product or system are introduced in a controlled and coordinated manner.[6] 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, you should identify baseline software and hardware configurations. You 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, you should characterize the hardware and software that make up those configurations.

Characterization can be a basic catalog of information, tracking information such as 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 the information 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**[7] that partially automate this process and provide for scheduled sweeps through computer systems.

Computer configurations do not remain unchanged for long. Therefore, characterization and validation should be part of your change-management

[6] Wikipedia

[7] **File integrity checker:** a tool that partially automates the process of identifying changes to system files or the addition of malicious code and flagging them for investigation. See www.sans.org/resources/idfaq/integrity_checker.php for a discussion of file integrity checkers.

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 your organization. For example, validation of a configuration should be done by a person other than the one who 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 anti-virus 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 typically done during the maintenance phase of the SDLC, 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 did the following.
>
> - He began to feel disgruntled at his diminishing importance to the company.
> - He launched verbal and physical assaults on coworkers.
> - He sabotaged projects of which he was not in charge.
> - He loaded faulty programs to make coworkers look bad.
>
> He received a verbal warning and two written reprimands, was demoted, and finally was fired as a result of his actions. A few weeks later, a logic bomb executed on the company's network, deleting 1,000 critical manufacturing programs from the company's servers. The estimated cost of the damage exceeded $10 million, leading to the layoff of approximately eighty 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.

In this case, 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.

> An organization built automated monitoring into its software that sent automatic notification to the security officer anytime 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, an IT manager who had access to the source code modified it so that the automated notification was no longer sent; he simply commented out a single line of code. He then proceeded to use the function to steal a large sum of money from his employer.

Interestingly, this 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.

Although this insider committed fraud, stop to ask yourself if you have any mission-critical systems that could be modified in this way. What if this had been a safety system, or a security system? What potential damage could one of your employees or contractors inflict by commenting out a few lines of source code?

Some cases in the CERT database 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 or an individual's private information, and in the worst case can be used to obtain passwords or encryption keys.

> A claims manager at an insurance company, who was upset with the company's practice of canceling policies after late payment, installed a hardware keystroke logger 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 was. 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.

> 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.

The software keystroke logger could have been detected by a change-control process as described in this section.

Practice 12: Log, Monitor, and Audit Employee Online Actions

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

What Can You Do?

If account and password policies and procedures are in place and enforced, your organization has a good chance of clearly associating online actions with the employee who performed them. Logging, monitoring, and auditing provide you 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 your critical assets.[8] 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 virtual private network (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 set up his attack during those two weeks right under the nose

[8] Many risk management methodologies are based on protection of critical assets—for example, the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) risk-based strategic assessment and planning technique for security [Alberts 2003]. See also www.cert.org/octave/.

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.

A common reaction to our suggestions for monitoring and auditing for potential insider threats is this: There is an abundance of monitoring tools on the market, and they produce so much information overload that it is impossible to review the data; it's like trying to find a needle in a haystack. The good news is that if you design monitoring strategies based on the patterns in insider threat cases we describe in this book, you will minimize information overload by using a risk-based approach to prioritizing alerts.

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, 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.

It is also worth mentioning that multiple insiders in cases in the CERT database attacked other external organizations from their computers 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.

As we described in Chapter 3, in almost all of the insider theft of IP cases the insider resigned before or after the theft. The majority of the thefts took place within one month of the insider's resignation, and most stole all of the information at once. Most of those insiders made no effort to conceal their technical actions. This suggests that monitoring of online actions, particularly downloads within one month before and after resignation, could be particularly beneficial for preventing or detecting 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, collection and transmission by malicious code, and printing out material on the organizations' printers. If you are monitoring for theft of information, you need to consider the wide variety of ways that information is purloined and customize your detection strategy accordingly. Data leakage tools may help with this task. Many tools are available that enable you to perform functions such as the following:

- 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 PII or documents containing certain words like new-product codenames
- Tracking of all documents copied to removable media
- Preventing or detecting emails to competitors, to governments and organizations outside the United States, to Gmail or Hotmail accounts, and so on

Central logging appliances and event correlation engines may help craft automated queries that reduce an analyst's workload for routinely inspecting this type of data.

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

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

The bottom line is that you need to have clearly defined employee-monitoring policies, and they must be consistently enforced. Policies must define very clear thresholds for when a specific employee will be audited and monitored. In addition, you cannot monitor some employees who exceed those thresholds and not others. Employee privacy laws must be considered when developing a monitoring policy; employee monitoring policies and procedures should be developed in conjunction with your legal staff.

Case Studies: What Could Happen if I Don't Do It?

> A research chemist was responsible for various research and development projects. His organization offered him a position in a foreign country, but his family did not want to move to that location. Consequently, he sought employment with a competitor; the competing company offered him a position, but the start date was not for a few months. The insider did not notify his current organization of his plan to resign until two weeks prior to starting his new job with the competitor. Over that four-month period, from when he received the job offer to when he left the victim organization, he downloaded nearly 17,000 PDF files and 22,000 abstracts containing trade secrets from his employer's server. The downloads took place on-site, during work hours, over several 15- to 20-hour periods. The amount of data he downloaded was 15 times higher than that of the next highest user and the data was not related to his research. His activities went unnoticed until he left, and the victim organization detected his substantial number of downloads.
>
> After starting his job at the competitor, he transferred the information to a company-assigned laptop. The victim organization notified the competitor that it had discovered the high-volume downloads. The competitor seized the insider's laptop and turned it over to the victim organization, which turned it over to the FBI. Agents discovered documents from the victim organization marked "Confidential," shredded technical documents, and numerous other documents in the insider's apartment and in a storage unit. When the search was conducted, the insider was attempting to erase an external hard drive. He was arrested, convicted, sentenced to 18 months of imprisonment, and ordered to pay $14,500 in restitution and a $30,000 fine.

Consider whether this could happen to you. If so, you should consider use of technical detection methods for alerting when an employee or contractor downloads a significant amount of information. This should not result in "information overload" as one would think this should not happen very often!

> 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. The next case 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, who was the manager of a warehouse, convinced his supervisor that he needed privileged access to the entire purchasing system for the warehouse. He then 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. He 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 his 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 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.

Practice 13: Use Layered Defense against Remote Attacks

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

What Can You Do?

Insiders often attack organizations remotely, either using legitimate access 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 to us in interviews 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. You may provide remote access to email and noncritical data but should consider limiting remote access to the most critical data and functions and only from machines that are administered by your organization. Access to data or functions that could inflict major damage to you 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, you should offset the added risk with closer logging and frequent auditing of remote transactions. Allowing remote access only from organization-owned machines will enhance your ability to control access to 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 a sometimes overlooked but critical part of the employee termination process. It is critical that employee termination procedures include

- Retrieving any organization-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, DBA, and other privileged shared accounts)
- Closing all open connections

A combination of remote access logs and source IP addresses usually helps to identify insiders who launch remote attacks. Identification can be straightforward because the username 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?

> The chief technology officer (CTO) announced his resignation following a salary dispute with the CEO. He left one month later, and went to work as a temporary employee for an unrelated organization. Three weeks after he left, his former company's voice-mail service started sending some customers to a pornographic telephone service. One week after that incident, unusual traffic on the company's network caused the network to fail. A short time later, its email servers were flooded with thousands of messages containing pornographic images, and auto-reply messages were sent from its email server disparaging the company and its services. The CEO began to receive strange and threatening email messages, some claiming to be from a cremation society. Threatening emails, phone calls, and forum postings continued until law enforcement was able to identify the source of the threatening messages: a computer associated with the former CTO's new employer.

This case highlights an important issue for you to consider: Who has the access and credentials to modify your voice-mail system? This is not an access path one ordinarily thinks of in the employee termination process, but one that could cause you severe embarrassment if modified as in this 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 his job. Then, three times over a two-week period, he 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 his 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 your interests.

Practice 14: Deactivate Computer Access Following Termination

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

What Can You Do?

While employed, insiders have legitimate, authorized access to your network, system, applications, and data. Once employment is terminated, it is important that you have in place and execute rigorous termination procedures that disable all access points available to the terminated employee. Otherwise, your 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 those 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 your organization (e.g., change from an employee to a contractor; change from a full-time to a 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 paths will be overlooked. Our research 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 consistently followed. It is also critical that you remain alert to new insider threat research and periodically review and update these processes. If at the time of termination you have 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 your organization. When an employee leaves, you should be able to confidently say all access paths available to that employee have been disabled.

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, nonexistent, or noncomprehensive 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, DBA accounts, and testing, training, development, and external organizational accounts, such as vendor or customer accounts. In addition, some applications require administrative accounts that are frequently shared among multiple users. It is important that you meticulously maintain a record of every shared account and every user authorized to have the password to each, and change the passwords for those accounts when employees are terminated.

Remote access is frequently exploited by former insiders. Remote access or 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, you might consider reviewing the employee's desktop computer, laptop, and system logs to ensure no software or applications have been installed that may permit the employee back into your 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, 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, and 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 piggybacking through doors, using the excuse that they forgot their badge.

Case Studies: What Could Happen if I Don't Do It?

> A software engineer at a high-technology company that developed and manufactured computer chips was terminated due to poor performance. He was responsible for managing an automated manufacturing system, and during the work week he maintained a constant remote access connection from his home to the company's network. Prior to informing him of his termination, the company terminated his network access, but failed to detect his remote access connection that was active from home. The day after his termination, outside of work hours and under the influence of alcohol, he used the open remote access connection to completely shut down the company's manufacturing system by deleting critical files. Due to his actions, the company lost four hours of manufacturing time and had to load backup data to restart the manufacturing process. The incident cost the company $20,000 to remedy. Connection and activity logs connected the insider to the incident. He was arrested and convicted, but sentencing details were unavailable.

This case points out one easy step that you should add to your employee termination process, if it's not in there already: Check for any active remote connections by the employee.

> A financial organization's system administrator was terminated suddenly with no advanced 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 he was right—his replacement had failed to disable his access through the company firewall. In addition, 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 company's primary server, one that had been having problems and had in fact crashed the previous weekend (and had taken the organization an entire weekend to bring up again). It took the financial institution 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 you have no competent backup for a single system administrator.

> 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 he had read another employee's email using her account, and 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 in to the company's system periodically for the past month, and that a former employee had accessed up to 16 of his former employer's systems on a daily basis during work hours. The insider had done the following:
>
> - Gained access to at least 24 user accounts
> - Read email
> - Reviewed source code for his previous project
> - Deleted two software modification notices for the project
>
> The former employee had been terminated for nonperformance 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.

Practice 15: Implement Secure Backup and Recovery Processes

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

What Can You Do?

Prevention of insider attacks is the first line of defense. However, experience has taught us 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 affected the outcomes in actual cases, and can mean 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 the 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 off-site 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 off-site, as well as who has access to the media in storage. Furthermore, case examples throughout this book have demonstrated the threat presented by employees of trusted partners; 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 off-site 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 fully 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 off-site 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 your organization.

You 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 did the following:

- Deleted backups
- Stole backup media (including off-site 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, you 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 you do for other system modifications
- Apply the two-person rule for protecting the backup process and physical media so that one person cannot take action without the knowledge and approval of another employee

Make sure you account for pockets of development systems, or production systems that are maintained independently instead of being managed as part of your IT enterprise. These systems can be just as critical to you as your enterprise systems are, and they are not necessarily managed using the same rigor as your centrally maintained IT systems.

Unfortunately, some attacks against networks could 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 your communication methods and, during an attack, may interfere with communications essential to your data-recovery process. You 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?

> An organization 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 off-site backup storage facility, from which he next stole more than 50 off-site backup tapes.

This case illustrates the risk of storing your backups in the same physical location as your critical systems. In addition, there was no layered defense to protect the backups—they were accessible by anyone who had physical access to the NOC. As a result, this very critical system and its backups were totally vulnerable to an insider IT sabotage attack.

> An insider was terminated because of his employer's reorganization. The company followed proper procedure by escorting him 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, resulting in 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.

Practice 16: Develop an Insider Incident Response Plan

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

What Can You Do?

An incident response plan for insider incidents differs from a response plan for incidents caused by an external attacker. You need to minimize the chances that the internal 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 the team's resources from mission-critical activities, expose a team member to investigation, or expose shortcomings by management or oversights in system security, opening the managers up to embarrassment or liability for losses.

You need 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 your organization needs to be assigned that is trusted by all department heads. Your 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 of your employees. Only those responsible for carrying out the plan need to understand it and be trained on its content and execution. Your 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. Your managers need to understand how to handle personal and professional problems and when they might indicate increased risk of insider compromise. If your organization experiences damage due to a malicious insider or as your risks evolve—for instance, due to new internal or external attack vectors—your employee training should be updated. Lessons learned from insider incidents should be fed back into your insider incident response plan to ensure its continual improvement.

Case Studies: What Could Happen if I Don't Do It?

> The IT manager in 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, and then modified it to be a winner in the lottery agency's database. When the agency discovered the fraudulent tickets, it 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, he behaved suspiciously, and therefore was put on administrative leave and his physical access was disabled. Management neglected to inform his subordinates of the action, so he still had managerial control of his personnel. Before he left on administrative leave, he deleted a history log that may have proven his criminal acts. He also instructed one of his subordinates to erase four weeks of backup tapes, claiming that they wouldn't be useful under a new backup data format that was being implemented. She complied with this request, and the organization lost much of the evidence of his tampering with system security controls. Once his alleged crime did come to light, he asked a different subordinate to retrieve some additional backup tapes for him that would help him prove his innocence. He complied, and the organization never recovered those tapes.

While the organization took the right actions to remove the suspect from the organization, it neglected to inform his subordinates of the action, so he still had managerial control of organization personnel. If the organization had a formal insider incident response plan in place, and its employees were 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.

> 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 he 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 that divulged some of the company's proprietary information. After receiving an anonymous tip that the insider was responsible for the leaks, the company started an investigation. Working with law enforcement, the organization found evidence that he had been downloading the organization's confidential information, which was outside his area of responsibility, for more than two years. He had downloaded massive amounts of information using a USB 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.

Summary

The best practices presented in this chapter provide a framework for establishing an insider threat program in your organization. Start by including insider threats in your enterprise-wide risk assessment. Next, conduct a security awareness campaign to ensure that insider threat is understood across your organization so that responsibility for the identification of and response to insiders who pose an elevated risk can be distributed enterprise-wide. Develop clearly defined policies, as described throughout this chapter, and enforce them consistently and fairly. Management needs to understand how to recognize and respond to concerning behavior in the workplace, and needs to understand the potential ramifications of negative workplace events. A well-defined employee termination process is essential in preventing attacks following termination. You need to secure both the physical and electronic environment, including account and password management, separation of duties, controls for your software development process, change controls, and extra vigilance for system administrators, other privileged users, and remote access.

You need to apply a consistent monitoring strategy for online actions; your employee monitoring practices should be developed in conjunction with your legal counsel to ensure that they are compliant with employee privacy laws. If monitoring identifies suspicious activity, a well-defined response plan should be enacted to minimize the impact to your organization.

Despite all of the precautions you implement, it is still possible that an insider will successfully attack. Therefore, it is important that your last step in preparing for an insider threat is to prepare for that possibility and enhance your organizational resiliency by implementing secure backup and recovery processes that are tested periodically.

Remember: It is very important not to overlook contractors and trusted business partners that have access to your information systems, information, or networks. Much of what you read in this chapter applies equally well to those types of insider threats!

This chapter presented a framework that you can use across your organization. The "Common Sense Guide" (referenced at the beginning of this chapter) has been one of the most popular documents we have created, so we stand behind its usefulness and strongly encourage you to measure your organization's practices against it to identify gaps that should be addressed.

When we were writing this book, the National Institute of Standards and Technology (NIST) was working on the next version of *Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations.*[9] The special publication is aimed at providing federal agencies, state and local governments, and private-sector organizations a set of security and privacy controls to safeguard their critical assets. This new version will include new guidance in the form of controls to address privacy, mobility, cloud computing, industrial controls, application security, Web applications, and insider threats. The CERT Insider Threat Center contributed input on insider threat controls to the Joint Task Force, a group of civilian-, defense-, and intelligence-agency information security experts working to produce a unified, federal IT security framework. Please refer to that publication[10] for more information on specific controls.

References/Sources of Best Practices

This chapter described 16 practices, based on existing industry-accepted best practices, providing you with defensive measures that could prevent or facilitate early detection of many of the insider incidents other organizations experienced in the hundreds of cases in the CERT insider threat database. If you would like more detail on implementing any of the practices we described, you should consult the following resources:

- CERT RMM (www.cert.org/resilience/)
- ISO 27002 (www.27000.org/iso-27002.htm)
- NIST 800-53 (http://csrc.nist.gov/publications/PubsSPs.html)
- SANS Top 20 Security Controls (www.sans.org/critical-security-controls/)

[9] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

[10] NIST 800-53: http://csrc.nist.gov/publications/PubsSPs.html