Common Sense Guide to Prevention and Detection of Insider Threats

1st Edition – April 2005

Carnegie Mellon University
CyLab

Authors

Dawn Cappelli
Andrew Moore
Timothy Shimeall

A. Introduction

1. **Are insiders really a threat?**
2. **Who needs to read this?**
3. **Can insiders be stopped?**

B. Best Practices for the Prevention and Detection of Insider Threats

1. **Institute periodic employee security awareness training for all employees.**
2. **Enforce separation of duties and least privilege.**
3. **Implement strict password and account management policies and practices.**
4. **Log, monitor, and audit employee online actions.**
5. **Use extra caution with system administrators and privileged users.**
6. **Actively defend against malicious code.**
7. **Use layered defense against remote attacks.**
8. **Monitor and respond to suspicious or disruptive behavior.**
9. **Deactivate computer access following termination.**
10. **Collect and save data for use in investigations.**
11. **Implement secure backup and recovery processes.**
12. **Clearly document insider threat controls.**

C. References/Sources of Best Practices

INTRODUCTION

Are insiders really a threat?

The threat of attack from insiders is real and substantial. The 2004 E-Crime Watch Survey™ conducted by the United States Secret Service, CERT® Coordination Center (CERT/CC), and CSO Magazine,[1] found that in cases where respondents could identify the perpetrator of an electronic crime, 29 percent were committed by insiders. The impact from insider attacks can be devastating. One complex case of financial fraud committed by an insider in a financial institution resulted in losses of over $600 million.[2] Another case involving a logic bomb written by a technical employee working for a defense contractor resulted in $10 million in losses and the layoff of 80 employees.[3]

Over the past several years, Carnegie Mellon University has been conducting a variety of research projects on insider threat. One of the conclusions reached is that insider attacks have occurred across all organizational sectors, causing significant damage to the affected organizations. These acts have ranged from "low-tech" attacks, such as fraud or theft of proprietary information, to technically sophisticated crimes that sabotage the organization. Damages are not only financial but can also include severe damage to the organization's reputation, resulting from widespread public reporting of the event.

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

Partnering with the United States Secret Service, the CERT/CC is conducting the Insider Threat Study to gather extensive insider threat data from more than 150 case files of crimes that involve most of the nation's critical infrastructure sectors.[4] This study is showing that use of the widely accepted best practices for information security could have prevented many of the insider attacks examined. Part of our research of insider threat cases entailed an examination of how each organization could have prevented the attack or at the very least detected it earlier. Rather than requiring new practices or technologies for prevention of insider threats, the research instead identifies existing best practices that are critical to the mitigation of the risks from malicious insiders.

---

1 http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf.

2 http://www.baltimoresun.com/business/bal-te.bz.allfirst06jun06,0,4228032,print.story?coll=bal-business-indepth.

3 http://www.nwfusion.com/research/2000/0626feat.html.

4 The first report in a series documenting the results of the study is published in *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. http://www.cert.org/archive/pdf/bankfin040820.pdf.

The practices outlined in this report are the most important for mitigating insider threats in our case research to date.

Who should read this report?

Decision makers across an organization can benefit from reading this guide. 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 the overall scope of the problem is understood by management, human resources, information technology, and security staff.

This report is written for a diverse audience, outlining practices that should be implemented by organizations to prevent insider threats. Each practice is described briefly in terms of why it should be implemented and one or more case studies illustrate what could happen if it is not implemented, and how the practice could have prevented an attack or facilitated early detection.

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

Can insiders be stopped?

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

Practices for preventing insider attacks

Implementation of the following 12 practices for preventing insider attacks will provide an organization with defensive measures that would have prevented or facilitated early detection of many of the insider attacks that other organizations have experienced.

PRACTICE 1: *Institute periodic employee security awareness training for all employees*. A culture of security awareness must be instilled in the organization so that all employees understand the need for policies, procedures, and technical controls. The first line of

defense from insider threats is the employees themselves. All employees in an organization must understand that security policies and procedures exist, that there is a good reason for why they exist, that they must be enforced, and that there can be serious consequences for infractions.

PRACTICE 2: *Enforce separation of duties and least privilege*.
If all employees are adequately trained in security awareness, and responsibility for critical functions is divided among employees within the organization, the possibility that one individual could commit fraud or sabotage without the cooperation of another individual within the organization is limited. Effective separation of duties requires the implementation of *least privilege*, that is, authorizing people only for the resources they need to do their jobs.

PRACTICE 3: *Implement strict password and account management policies and practices*.
No matter how vigilant the employees are in trying to prevent insider attacks, if the organization's computer accounts can be compromised, insiders have an opportunity to circumvent both manual and automated mechanisms that are in place to prevent insider attacks.

PRACTICE 4: *Log, monitor, and audit employee online actions*.
If account and password policies and procedures are in place and enforced, an organization can associate online actions with the employee who performed them. Logging, periodic monitoring, and auditing provide an organization with the opportunity to discover and investigate suspicious insider actions before more serious consequences ensue.

PRACTICE 5: *Use extra caution with system administrators and privileged users*.
Typically, logging and monitoring is performed by a combination of system administrators and privileged users. Therefore, additional vigilance must be devoted to those users.

PRACTICE 6: *Actively defend against malicious code*.
One class of insider attack that can be executed by system administrators or privileged users is the use of logic bombs or installation of other malicious code on the system or network. These types of attacks are stealthy and therefore difficult to detect ahead of time, but practices can be implemented for early detection.

PRACTICE 7: *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, then disgruntled insiders will think twice about attacking systems or networks at work. Insiders tend to feel more confident and less inhibited when they have little fear of scrutiny by coworkers; therefore, remote access policies and procedures must be designed and implemented very carefully.

PRACTICE 8: *Monitor and respond to suspicious or disruptive behavior*.
In addition to monitoring online actions, organizations should closely monitor other suspicious or disruptive behavior by employees in the workplace. Policies and procedures should be in place for employees to report such behavior when they observe it in coworkers, with required follow-up by management.

PRACTICE 9: *Deactivate computer access following termination.*
When an employee terminates employment, whether the circumstances were favorable or not, it is important that the organization have in place a rigorous termination procedure that disables all of the employee's access points to the organization's networks, systems, applications, and data.

PRACTICE 10: *Collect and save data for use in investigations*.
Should an insider attack, it is important that the organization have evidence in hand to identify the insider and follow up appropriately.

PRACTICE 11: *Implement secure backup and recovery processes*.
Despite all of the precautions implemented by an organization, it is still possible that an insider will attack. Therefore, it is important that organizations prepare for that possibility by implementing secure backup and recovery processes that are tested periodically.

PRACTICE 12: *Clearly document insider threat controls*.
As an organization acts to mitigate insider threat, clear documentation will help to ensure fewer gaps for attack, better understanding by employees, and fewer misconceptions that the organization is acting in a discriminatory manner.

Practice 1: Institute periodic employee security awareness training for all employees.

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

What to do?

Employees and managers need to understand that there is no "profile" of a malicious insider. Reported cases have involved both highly technical people and those who have very minimal understanding of the systems they exploited. Ages of perpetrators have ranged from late teens to retirement. Both men and women have been malicious insiders. These people have been introverted "loners," aggressive "get it done" people, and extroverted "star players." Their 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 employees, contractors, and temporary employees. As such, security awareness training needs to encourage employees to identify malicious insiders by behavior, not by stereotypical characteristics. Behaviors that should be a source of concern include making threats against the organization, bragging about the damage one could do to the organization, or discussing plans to work against the organization. Also of concern are attempts to gain other employees' passwords and to fraudulently obtain access through trickery or exploitation of a trusted relationship (often called "social engineering").

Organizations need to provide training programs that create a culture of security that is appropriate for them and that includes both security and non-security personnel. For effectiveness and longevity, the measures used to secure an organization against insider threat need to be tied to the organization's mission, values, and critical assets. For example, if an organization places a high value on customer service quality, it may view security as protection of individual customer information, as well as the ability to serve customers. That organization could train its members about malicious employee actions focusing on a number of key issues, including

- reducing risks to customer information by auditing access to customer records (see Practice 4)
- requiring separation of duties between employees who modify customer accounts and those who approve modifications or issue payments (see Practice 2)
- using secure backup and recovery methods to ensure availability of customer service data (see Practice 11)

Training on reducing risks to customer service processes would focus on

- protecting computer accounts used in these processes (see Practice 3)
- using malicious code detection tools (see Practice 6)
- detecting and reporting disruptive behavior by employees (see Practice 8)

- implementing proper system administration safeguards for critical servers (see practices 5, 7, and 9)

Training content would be based on documented policy (see Practice 12), including a confidential means of reporting security issues with appropriate follow-up to security reports.

Employees need to understand that the organization has policies and procedures in place and will respond to detected security issues in a fair and prompt manner. Separation of duties and remote access monitoring should be explained. While employee alertness is key to detecting many insider attacks, several cases have been detected because of abnormal system activity (including download of sensitive material to home computers, unusual system load, changes in system configuration, and illicitly escalated user privilege). 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.

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

The lead developer of a critical application used by his organization had extensive control over the source code for that application. He made sure that the only copy of the source code was on his company-provided laptop; there were no backups performed, and very little documentation existed, even though management had repeatedly requested documentation for the system. The insider told his coworkers he had no intention of documenting the source code and any documentation he did write would be encrypted. He also stated that he thought poorly of his management because they had not instructed him to make back-up copies of the source code.

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

Another insider case illustrates a much less technically sophisticated attack, but one that could have been avoided or successfully prosecuted if proper policies and training had been in place. Four executives of a national computer and network support services

consulting firm left that firm to form a competing company. A few days before they left, one of the insiders ordered a backup copy of the hard drive on his work computer from the Internet service the company used to back up its data. The hard drive contained customer lists and other sensitive information. The company alleged that its consulting services agreement and price list were sent by email from the insider's work computer to an external email account registered under his name. The insiders, two of whom had signed confidentiality agreements with the original employer, disputed the fact that the information they took was proprietary, saying that it had been published previously. Clear policies regarding definition of proprietary information and rules of use could have prevented the attack or provided a clearer avenue for prosecution.

PRACTICE 2: Enforce separation of duties and least privilege.

While security awareness training is an excellent start, basic controls for separation of duties and least privilege must be in place to limit the damage that malicious insiders can inflict.

What to do?

Separation of duties requires dividing of functions among people within an organization to limit the possibility that one individual could commit fraud or sabotage without the cooperation of another employee. A particular type of separation of duties called *two-person rule* is often used in cases where two people must participate in a task for it to be executed successfully. 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 the implementation of *least privilege*, that is, authorizing people only for the resources they need to do their job. Typically, organizations define a work role for each employee that characterizes the responsibilities of his or her job and the access to organizational resources that is needed to fulfill those responsibilities. Insider risk can be greatly mitigated by defining and separating the roles responsible for key business processes and functions. For example,

- online management authorization can be required for critical data entry transactions
- code reviews can be instituted for the software development and maintenance process
- configuration management processes and technology can be used to control software distributions and system modification
- auditing procedures can be designed to ensure that collusion involving the auditors themselves is avoided

Physical, administrative, or technical controls can be used to restrict employees' access to only those resources needed to accomplish their jobs.

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

permitted by another role limits the damage they can inflict if they become disgruntled or otherwise decide to exploit the organization for their own purposes.

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

In one case, a currency trader (who also happened to have a college minor in computer science) developed much of the software used by his organization to record, manage, confirm, and audit trades. He implemented obscure functionality in the software that enabled him to conceal his illegal trades, evolving the software over time to facilitate different methods of hiding his activities to reduce the risk of detection. In this case, it was nearly impossible for auditors to detect his activities.

The insider, who consented to be interviewed for the Insider Threat Study, told the study researchers that problems can arise when "the fox is guarding the henhouse."[5] Specifically, the insider's supervisor managed both the insider and the auditing department responsible for ensuring his trades were legal or compliant. When auditing department personnel raised concern about the insider's activities, they were doing so to the insider's supervisor (who happened to be their supervisor as well). The supervisor directed auditing department personnel not to worry about the insider's activities and to cease raising concern, for fear the insider would become frustrated and quit.

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

- end users of an organization's critical systems should not be authorized to modify the system functionality or access the underlying data directly
- responsibility for critical data and responsibility for auditing that critical 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. The insider would approve an asylum decision himself, request that one of his subordinates approve the decision, or overturn someone else's denial of an asylum application. Several foreign nationals either admitted in an interview or pleaded guilty in a court of law to lying on their asylum applications and bribing public officials to get approval of 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 were not involved.

---

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

Practice 3: Implement strict password and account management policies and practices.

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

What to do?

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

- is controlled so that unauthorized access is not possible
- is logged and monitored so that suspicious access can be detected and investigated
- can be traced from the computer account to the individual associated with that account

Password policies and procedures should ensure that all passwords are strong,[6] employees do not share their passwords with anyone, employees change their passwords periodically, and all computers execute password-protected screen savers. As a result, all activity from any account should be attributable to its owner. Employees should also report all attempts at account compromises rather than permit a compromise to happen due to ignorance of potential consequences or lack of a reporting mechanism.

Periodic account audits combined with technical controls enable identification of

- backdoor accounts that could be used later for malicious actions by an insider, whether those accounts were specifically set up by the insider or were left over from a previous employee
- shared accounts whose password was known by the insider and not changed after that person's termination

The need for every account should be reevaluated periodically. Limiting accounts to those that are absolutely necessary, with strict procedures and technical controls so that all online activity by those accounts can be traced directly 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.

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

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

A disgruntled software developer downloaded the password file from his organization's UNIX server to his desktop. Next, he downloaded a password cracker from the Internet and proceeded to "break" approximately 40 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 his root password. As a result, his organization modified its policies and procedures to implement countermeasures to prevent such attacks in the future. System administrators were permitted to run password crackers and notify users with weak passwords, and it improved security training for employees on how and why to choose strong passwords.

A second case also illustrates the importance of employee awareness of password security. Two temporary data entry clerks and one permanent employee were able to embezzle almost $70,000 from their company by fraudulently using other employees' computer accounts. The system's role-based access provided the other employees' accounts with access to privileged system functions. The clerks used those accounts without authorization to subvert the business process governing vendor payment. First, they entered valid data into the database using their own accounts. Then they used the other, unauthorized accounts to modify the vendor's name and address to that of a friend or relative, issued the check from the system, and then modified the data back to the original, valid vendor information. The fraud was discovered after almost five months when an accountant in the general ledger department noticed that the number of checks issued was larger than normal, and further investigation revealed the irregularities in the handling of the checks.

Practice 4: Log, monitor, and audit employee online actions.

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

What to do?

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

Auditing in the financial community refers to examination and verification of financial information. In the technical security domain it refers to examination and verification of various network, system, and application logs. To prevent or detect insider threats, it is important that auditing involve the review and verification of *all* of the organization's critical assets.[7] Furthermore, auditing must examine and verify integrity as well as the legitimacy of logged access.

Automated integrity checking should be considered for flagging suspicious transactions that do not adhere to predefined business rules for manual review. 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. Likewise, data audits typically involve manual processes, such as comparing electronic data modification history to paper records or examining electronic records for suspicious discrepancies.

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

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

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

enough unpredictability to the process to deter an insider from launching a contemplated attack.

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

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

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

- The insider convinced his supervisor that he needed privileged access to the entire purchasing system for the warehouse.
- Next, he added a fake vendor to the list of authorized suppliers for the warehouse.
- Over the next two years, he entered 78 purchase orders for the fake vendor, and, although no supplies were ever received, he also authorized payment to the vendor.

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

Practice 5: Use extra caution with system administrators and privileged users.

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

What to do?

System administrators and privileged users[8] 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

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

Even if online actions can be traced to the person who engaged in the action, it is unreasonable to expect that all user actions can be monitored proactively. Therefore, while the practices discussed above ensure identification of users following detection of suspicious activity, additional steps must be taken by organizations to defend against malicious actions before they occur. For instance, system administrators and privileged users have access to all information within their domains. Technologies such as encryption can be implemented to prevent such users from reading or modifying sensitive files to which they should not have access.

Policies, procedures, and technical controls should enforce separation of duties and require actions by multiple users for all modifications to critical systems, networks, applications, and data. In other words, no single user should be permitted or be

[8] The term “privileged users” refers to users who have an elevated level of access to a network, computer system, or application that is short of full system administrator access. For example, system administrators, network administrators, database administrators (DBAs), and webmasters have the ability to create new user accounts and control the access rights of users within their domains.

technically able to release changes to the production environment without online action by a second user.

Finally, organizations must be particularly careful in disabling access by former system administrators and privileged users. Thoroughly documented procedures for disabling access can help ensure that stray access points are not overlooked. In addition, the two-person rule should be considered for the critical functions performed by these users to reduce the risk of extortion after they leave the organization.

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

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

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

Practice 6: Actively defend against malicious code.

While insiders frequently use simple user commands to do their damage, logic bombs and other malicious code are used frequently enough to be of concern.

What to do?

Many organizations defend against malicious code using antivirus software and host or network firewalls. While these defenses are useful against external infections, their value is limited in preventing attacks by malicious insiders in two important respects: they do not work against new or novel malicious software (including destructive software logic bombs planted by insiders) and they are concerned primarily with material spread through networking interfaces rather than material installed directly on a machine. To deal with these limitations, a more systematic and active approach is needed.

First, organizations should identify baseline software and hardware configurations. A given organization may have several baseline configurations, given the different computing and information needs of different users (accountant, manager, programmer, receptionist). But as configurations are identified, the organization should characterize the hardware and software that makes up those configurations.

The characterization can be simply a catalog of information, such as versions of installed software, hardware devices, and disk utilization. However, very basic characterizations are often simple to defeat, 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 re-collecting the information and comparing it against the baseline copy. Any discrepancies can then be investigated to determine whether they are benign or malicious. Using these techniques, changes to system files or the addition of malicious code will be flagged for investigation. There are tools called *file integrity checkers* that partially automate this process and provide for scheduled sweeps through computer systems.[9]

Computer configurations do not remain fixed and unchanged for very long. Therefore, characterization and validation should be part of an organization's configuration management process. For protection against malicious insiders, part of the configuration management process should be separation of duties. For example, validation of a

[9] Examples include TRIPWIRE (www.tripwire.com), Integrit (http://integrit.sourceforge.net/), AIDE (http://www.cs.tut.fi/%7Erammer/aide.html), and yafic (http://www.saddi.com/software/yafic/).

configuration should be done by a person other than the one who made changes so that there is some opportunity to detect and correct malicious changes (including planting of logic bombs).

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

A system administrator at a manufacturing firm had begun employment as a machinist. Because of his technical ability he also, over a ten-year period, created the company's network from scratch and had sole authority for system administration. The company eventually expanded and began to open additional offices and plants, both nationally and internationally. The insider

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

He received a verbal warning, two written reprimands, was demoted, and was finally fired as a result of his actions. A few weeks later a logic bomb was released on the company's network that deleted one thousand critical manufacturing programs from the company's servers. The company estimated the cost of damage in excess of $10 million, which led to the layoff of approximately 80 employees. The investigation revealed that the insider had actually run a test version of the logic bomb three times on the company's network prior to his termination.

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

One organization had automated logging and monitoring built into its custom-developed software that sent automatic notification to the security officer any time a highly restricted function was used to modify information stored in the database. Role-based access control restricted access to this function to only a few very high-level users, and the automated notification provided a second layer of defense against illegal modification of data using that function. However, one of the developers of the application, who also happened to have access to that function, modified the code so that the automated notification was no longer sent. He then proceeded to use the function to steal a large sum of money from his employer.

Interestingly, the organization also had a comprehensive logging system in place for software changes. Any time a program was compiled, a report was produced listing which files were compiled, by which computer account, and when. It also listed which modules were added, modified, or deleted. Unfortunately, this report was not monitored,

and therefore the changes made to the application were not detected during the year and a half over which the fraud was committed. Had it been monitored, or had a configuration control system been in place to enforce the 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.

Practice 7: Use layered defense against remote attacks.

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

What to do?

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

The vulnerabilities inherent in allowing remote access suggest that multiple layers of defense should be built against remote attack. Organizations may provide remote access to email and non-critical data but should strongly consider limiting remote access to the most critical data and functions. Access to any data or functions that could inflict major damage to the company should be limited to employees physically located inside the workplace. This should be the rule rather than the exception. Remote system administrator access should be limited to the smallest group practicable, if not prohibited altogether.

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

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

- disabling remote access accounts (such as VPN and dial-in accounts)
- disabling firewall access
- changing the passwords of all group accounts (including system administrator, database administrator (DBA), and other privileged group accounts)
- closing all open connections

A combination of remote access logs, source IP addresses, and phone records usually helps to identify insiders who launch remote attacks. Identification can be straightforward because the user name of the intruder points directly to the insider. Of course, corroboration of this information is required, because the intruders might have been trying to frame other users, cast attention away from their own misdeeds by using other users' accounts, or otherwise manipulate the monitoring process.

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

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

In an interview for the Insider Threat Study, the insider said that group trading (trading by a team of traders), rather than individual trading, can help mitigate an organization's risks, because it is easier to detect illegal or suspicious trading practices when there are multiple team members trading from the same account.[10] In this case isolated trading, along with the anonymous nature of remote access, emboldened the insider to continue a fraud in which he otherwise might not have engaged.

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

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

Practice 8: Monitor and respond to suspicious or disruptive behavior.

One method of reducing the threat of malicious insiders is to proactively deal with difficult employees.

What to do?

An organization's methods of dealing with difficult individuals should start in the hiring process. A consistent practice of performing background checks and evaluating individuals based on the information received can reduce insider threats. The background checks should investigate previous criminal convictions and verify credentials and past employment, and should include discussion with prior employers regarding the individual's competence and approach to dealing with issues in the workplace. While this information may not be the dominant component in the hiring process (and, arguing fairness, should not be), the information gathered may help in dealing proactively with the individual. Our research has revealed a surprisingly high number of malicious insiders who had prior criminal convictions when hired.[11] This proactive management should not be punitive in nature; rather, the individual should be cultivated into the organizational climate with appropriate care and thoroughness.

After employment, if an employee's behavior becomes suspicious, the organization must act with due care in dealing with it. Policies and procedures must exist for employees to report their concerns or to report disruptive behavior by others to a single contact point enterprise wide, and reports should always be investigated. (Some checks and balances must exist to limit frivolous reporting.) Disruptive employees should not be allowed to migrate from one position to another within the enterprise, evading documentation of disruptive or concerning activity. Threats, malicious boasting ("You wouldn't believe how easily I could trash this net!") and other negative sentiments should also be treated as concerning behavior. Many employees will have concerns and grievances from time to time in an organization, and the provision of a formal and accountable process for addressing those grievances may act to satisfy those who might otherwise resort to malicious activity. In general, any employee experiencing difficulties in the workplace who also has access to critical information assets should be aided in the resolution of those difficulties.

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

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

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

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

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

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

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

Practice 9: Deactivate computer access following termination.

It is important that organizations follow rigorous termination procedures that disable all open access points to the networks, systems, applications, and data.

What to do?

While employed, insiders have legitimate, authorized access to the organization's network, system, applications, and data. However, once employment is terminated, whether under favorable or unfavorable circumstances, it is important that the organization have in place and execute rigorous termination procedures that disable all open access points. Otherwise, the organization's network is vulnerable to access by a now illegitimate, unauthorized user.

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 points of access will be overlooked. Research in the Insider Threat Study shows that insiders can be quite resourceful in exploiting obscure access mechanisms that were neglected in the termination process. Once a formal process is established, it must be strictly followed for all terminations. It is also critical that organizations remain alert to new insider threat research and periodically review and update these processes.

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

Accounts that are sometimes overlooked in the termination process are group accounts. Group accounts are typically shared among multiple users to implement a two-person rule. Examples of such accounts are system administrator accounts and DBA accounts. In addition, some applications require administrative accounts that are frequently shared among multiple users. It is important that the organization meticulously maintain a record of every shared account and every user who knows the password to each.

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

In summary, a layered defensive model 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, 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. Also, keep in mind that if the terminated insider was responsible for establishing accounts for others, such as employees, customers, or external website users, then those accounts could also be accessible to the terminated insider.

Finally, termination procedures must include steps to prevent physical access. Some insiders have been known to exploit physical access as a means of gaining access to their former employer's computer system.

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

The system administrator at a credit union was terminated suddenly with no previous 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 his home and found that his replacement had failed to disable his access through the company firewall. Although his replacement had disabled his user account, she had failed to change the password of the system administrator account. The insider used that account to shut down the organization's primary server, one that had been having problems and had in fact crashed the previous weekend (which had taken him an entire weekend to bring up again). It took the credit union three days to bring the server back into service; during that time none of its customers were able to access the money in any of their accounts in any way. This case illustrates the necessity of thoroughly disabling access, as well as the consequences when an organization has no competent backup for a single system administrator.

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

The login was then traced to a specific computer that happened to be located physically at a subsidiary of the company. Further investigation showed that the same computer had logged into the company's system periodically for the past month. Active monitoring by both the victim company and the subsidiary then showed that a former employee of the victim organization had accessed up to sixteen computer systems belonging to his former employer. This access occurred on a daily basis during working hours. The insider

- gained access to at least 24 user accounts
- read electronic mail
- reviewed source code for his previous project

- deleted two software modification notices for the project

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

Practice 10: Collect and save data for use in investigations.

Collecting and saving usable evidence preserves response options, including legal options.

What to do?

The first questions that often follow any computer incident, whether malicious or not, are "what happened?" and "who is responsible?" In the cases where malicious insiders are suspected, these questions are particularly urgent. Answering these questions in an actionable manner requires a detailed record of system and network actions. However, malicious insiders may act to corrupt, falsify, or delete such a record, impacting options for corrective and responsive actions.

To best protect critical information and equipment, multiple sources of information should be maintained, particularly sources that may support one another. This includes logging

- data access (reading, modifying, or deleting data)
- application usage (when applications were started and exited and by which user)
- system commands and file change logs
- method of connection (console, local-area networked, dial-in, Internet)
- the source and destination of connections

Phone system and physical access records should also be maintained. As this information is collected, it should also be placed on backup media for archival storage.

As difficult as collecting all this information is, analysis of it is often harder. The signs of malicious insider activity can be subtle, such as an abnormal pattern or rate of data modification, or an off-hours download of information the insider is authorized to read. Log files need to be monitored periodically to try to identify such situations. Unfortunately, many of the publicly available log file analysis tools are not designed to do this type of analysis.

Organizations may need to involve a forensics specialist, both to design a routine analysis procedure for identifying malicious insiders and for more specialized analysis once the insider is identified. There have been insider threat cases in which inappropriate handling of system logs has rendered them unacceptable for prosecution. In the event of a suspected security incident, involve an expert in the investigation of electronic crimes.

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

An employee of a subcontractor for a government agency was nearing completion of his contract. Ordinarily, under these circumstances, the government agency would offer the employee a permanent position if his or her performance had been

satisfactory working for the subcontractor. The insider initiated this hiring process and was required to take a drug test. The drug test results came back positive for cocaine, so his employment possibilities for the agency were forfeited. He remained employed with his current employer for a few days until that organization was notified of his drug test results and terminated his employment immediately. His physical access cards were confiscated, he was escorted from the building, his personal computer account was disabled, and the password was changed on the system administrator account to which he had access.

The following Monday morning, the subcontractor's system was down. The logs showed that the system had been shut down via commands from a bogus account that was not associated with any legitimate user. Remote access logs showed that attempts to log in began Friday evening and continued through early Saturday before being successful. Once authenticated, the user had deleted a number of printer drivers in the system, altered and changed certain user passwords, and finally entered the command to shut down the system. The logs on the remote access server stored the phone number of the incoming connections, and it was traced to the home address of the terminated insider. These logs were key in successfully prosecuting the insider.

In contrast to the above case where logs were stored appropriately and used to identify the user for prosecution, the following case illustrates the opposite case: A contractor for a large company was responsible for handling customer service calls. A fraud scheme conducted by four employees over a period of almost three years resulted in losses for the company of $500,000. However, once the fraud was suspected by the company's fraud investigator, it was discovered that, since the company "recycled" its computer logs, they only provided specific activity by login name and computer terminal as far back as one month. Fortunately, one of the employees involved testified as to the history and duration of the fraud. This case illustrates the importance of securely backing up system logs for long time periods in case they are needed for investigations or prosecution.

Practice 11: Implement secure backup and recovery processes.

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

What to do?

Prevention of insider attacks is the first line of defense. However, experience has taught that attacks can be prevented only up to a point. Unfortunately, there will always be avenues for an insider to successfully compromise a system. Effective backup and recovery processes need to be in place and operational so that if compromises do occur business operations can be sustained with minimal interruption. Our research has shown that effective backup and recovery mechanisms can make the difference between several hours of downtime to restore systems from backups and weeks of manual data entry when backups are not available. When possible, multiple copies of backups should exist, with redundant copies stored offsite in a secure facility. Different people should be responsible for the safekeeping of each copy so that it would require the cooperation of multiple individuals to compromise the means to recovery.

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

- deleted backups
- stole backup media
- performed actions that could not be undone due to faulty backup systems

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

- backups are performed and periodically tested
- media and content are protected from modification, theft, or destruction
- separation of duties and configuration management procedures are applied to backup systems just as they are to other system modifications

Unfortunately, attacks against networks may interfere with common methods of communication, thereby increasing uncertainty and disruption in organizational activities, including recovery from the attack. This is especially true of insider attacks, since insiders are quite familiar with organizational communication methods and, during attack, may interfere with communications essential to the organization's data backup process. Organizations can mitigate this effect by *multi-homing*, an approach that maintains trusted communication paths outside of the network with sufficient capacity to

ensure critical operations in the event of a network outage. This kind of protection would have two benefits: the cost of strikes against the network would be mitigated, and insiders would be less likely to strike against connectivity because of the reduced impact.

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

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

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

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

Practice 12: Clearly document insider threat controls.

To ensure consistent handling and to protect against accusations of discrimination, procedures for dealing with malicious insiders must be clearly documented.

What to do?

Cases involving malicious insiders are difficult to handle. Relationships between management and employees may be strained, with individuals taking sides with the organization or with the employee. A clearly written set of policies and procedures, developed with protection of the rights of everyone involved in mind, may help to defuse this situation. All of the organization's efforts to control damage by malicious insiders should be identified, together with circumstances under which these efforts are appropriate. As individuals join the organization, they should receive a copy of this description that clearly lays out what is expected of them, together with the consequences of violations. Evidence that each individual has read and agreed to the organization's policies, such as the individual's signature, should be maintained.

This description should also form the basis of ongoing training as described in Practice 1. If the organization experiences damage due to a malicious insider or if other risks evolve, such as new forms of internal or external attack, the description and training should be updated. The training should be given periodically to all employees, to help individuals act properly in the organization.

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

An insider accepted a promotion, leaving a system administrator position in one department and taking 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 organization 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 administrative 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 brought against the analyst for misuse of computing systems. These charges were eventually unsuccessful, 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.

C. References/Sources of Best Practices

Alberts, C; Dorofee, A; Killcrece, G; Ruefle, R; & Zajicek, M. *Defining Incident Management Processes for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.cert.org/archive/pdf/04tr015.pdf.

Allen, Julia H. *The CERT® Guide to System and Network Security Practices*. Boston, MA: Addison-Wesley, 2001.

BS7799/ISO17799
http://www.itgi.org

CERT® Security Improvement Modules
http://www.cert.org/security-improvement/

COBIT
http://www.itgi.org
http://www.isaca.org

ITIL (IT Infrastructure Library)
http://www.ogc.gov.uk/

ISF (Information Security Forum)
http://www.isfsecuritystandard.com/index_ie.htm

NIST 800-14, "Generally Accepted Practices and Principles for Securing Information Systems" (http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf).