Software Engineering Institute

Insider Threat Attributes and Mitigation Strategies

George J. Silowash

July 2013

TECHNICAL NOTE
CMU/SEI-2013-TN-018

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0000356

Table of Contents

Acknowledgments iii

Executive Summary v

Abstract vii

1 Monitor Phone Activity Logs to Detect Suspicious Behaviors 1
- 1.1 Case Study 1 1
- 1.2 Solutions 1
- 1.3 *Common Sense Guide* References 2

2 Monitor and Control Privileged Accounts 3
- 2.1 Case Studies 3
  - 2.1.1 Case Study 2 3
  - 2.1.2 Case Study 3 3
  - 2.1.3 Case Study 4 4
- 2.2 Solutions 4
- 2.3 *Common Sense Guide* References 5

3 Monitor and Control External Access and Data Downloads 6
- 3.1 Case Studies 6
  - 3.1.1 Case Study 5 6
  - 3.1.2 Case Study 6 6
  - 3.1.3 Case Study 7 7
- 3.2 Solutions 7
- 3.3 *Common Sense Guide* References 7

4 Protect Critical Files from Modification, Deletion, and Unauthorized Disclosure 9
- 4.1 Case Studies 9
  - 4.1.1 Case Study 8 9
  - 4.1.2 Case Study 9 10
  - 4.1.3 Case Study 10 10
- 4.2 Solutions 11
- 4.3 *Common Sense Guide* References 11

5 Disable Accounts or Connections upon Employee Termination 12
- 5.1 Case Studies 12
  - 5.1.1 Case Study 11 12
  - 5.1.2 Case Study 12 12
  - 5.1.3 Case Study 13 13
- 5.2 Solutions 13
- 5.3 *Common Sense Guide* References 14

6 Prevent Unauthorized Removable Storage Mediums 15
- 6.1 Case Study 15
  - 6.1.1 Case Study 14 15
  - 6.1.2 Case Study 15 15
  - 6.1.3 Case Study 16 16
- 6.2 Solutions 16
- 6.3 *Common Sense Guide* References 17

7 Understand All Access Paths into Organizational Information Systems 18
7.1 Case Studies 18
7.1.1 Case Study 17 18
7.1.2 Case Study 18 19
7.1.3 Case Study 19 19
7.2 Solutions 20
7.3 *Common Sense Guide* References 21

References 23

Acknowledgments

We thank our sponsors at the U.S. Department of Homeland Security, Office of Cybersecurity and Communications, Federal Network Resilience Division for supporting this work.

Executive Summary

Organizations that want to create an insider threat program need a place to start. One challenge is deciding what mitigation strategies to implement. Vendors tout products that claim to provide some sort of insider threat prevention or detection capabilities. How can an organization be sure that such products can do what they claim? This technical note discusses the attributes insider threat tools should have in order to detect and/or prevent potential attacks by malicious insiders.

The CERT® Division of the Software Engineering Institute, part of Carnegie Mellon University, selected these attributes based on its insider threat database of more than 700 cases involving malicious insiders. CERT insider threat staff reviewed each case to determine what technical or behavioral characteristics allowed the insider to carry out their activity. The top 10 technical attributes associated with the various cases were selected for further analysis. Three of these attributes had similar mitigation strategies and so were combined, leaving 7 attributes associated with many insider threat cases.

Selecting products that address these insider threat attributes is not the ultimate solution for mitigating insider threats. Rather, an organization must implement a holistic approach that includes individuals from various departments, including human resources, legal, physical security, data owners, information technology, and software engineering. The *Common Sense Guide to Mitigating Insider Threats, 4th Edition* discusses 19 best practices that organizations should implement to mitigate insider threats. These practices are based on the same database used to develop this technical note, but they provide a more holistic approach.

This technical note focuses on common characteristics gleaned from numerous cases. A single technical or behavioral attribute of an insider does not necessarily indicate malicious intent. Rather, insiders exhibit many characteristics that can be used to determine if a particular action is associated with malicious insider activity. These characteristics cannot be used in a vacuum. The organization should incorporate these characteristics into a comprehensive insider threat program as outlined in Best Practice 16 of the *Common Sense Guide to Mitigating Insider Threats, 4th Edition*.

The organization should consult legal counsel to ensure the organization operates any insider threat program within company policy and the confines of the law before implementing any product or recommendation. Technical products and recommendations should be thoroughly tested in a nonproduction environment before deploying to a production environment.

Abstract

Malicious insiders pose a threat to the confidentiality, integrity, and availability of an organization's information. Many organizations look for hardware and software solutions that address insider threats but are unsure of what characteristics to look for in a product. This technical note presents seven common attributes of insider threat cases, excluding espionage, drawn from the CERT® Division's database. The note maps the seven attributes to characteristics insider threat products should possess in order to detect, prevent, or mitigate the threat. None of these attributes alone can identify a malicious insider. Rather, each attribute is one of many data points that an organization should consider when implementing an insider threat program.

1 Monitor Phone Activity Logs to Detect Suspicious Behaviors

Malicious insiders can use the organization's phone system to communicate with outsiders who may be acting as co-conspirators. Phone calls may be used to exfiltrate sensitive data or to receive instructions from another party. If the organization utilizes a Voice over Internet Protocol (VoIP) phone system or another system capable of generating logs when a call is made or received, then the organization could log information about the call to a central Security Information and Event Management (SIEM) system.

Logs noting the call's source and destination, date and time, and duration should be centrally stored and regularly reviewed by those who are familiar with the caller's job position and current projects. This will reduce the amount of time required to research call data. Only those with a bona fide need to know should be able to access the logs.

1.1 Case Study 1

The insider worked as a branch manager of a national banking institution. The insider's father, who had a criminal history, had met a man in prison who would eventually run an identity theft scheme. The father, sometime after being released, put his prison friend (the outsider) in touch with his son (the insider) in hopes that his son would help steal account information using his privileged access. The outsider offered to pay the insider $1,000 for each account. While the insider initially refused, his father eventually persuaded him to take part in the fraud scheme. Over a three-month period, the outsider asked the insider for the information on a total of 25 specific accounts, which the insider divulged over the phone at work and on paper documents outside of work. Using the account information, the outsider made fake IDs and gave them to a team of female cashiers who would walk into banks and make fraudulent withdrawals. In total, $228,000 was stolen. Once investigators received reports from customers whose accounts had been compromised, they traced the fraud to the insider using the access logs of customer records. The insider admitted to the scheme and even helped investigators conduct a sting operation on the outsider. Because he helped catch the outsider, who had an extensive criminal history and numerous charges against him, the insider was sentenced to time served and two years of supervised release.

1.2 Solutions

Suspicious phone calls may indicate that an insider is misusing company resources or is involved in malicious activity. Detecting suspicious behavior from phone calls depends heavily on phone system logging capabilities. Any one of these events alone does not necessarily indicate a malicious insider; additional information or the context of the event are required. A combination of events from the SIEM system can be used to help provide additional context, but not the entire scope, of the phone call. Sample calling patterns that the organization may want to consider reviewing (depending on the organization's mission and employee's role) include

- making or receiving calls to/from a foreign country—Monitor call logs for calls to a foreign country where the company does not have a business relationship or presence.

- calls to geographical areas where the company does not have a business relationship—Call logs that indicate someone is calling another city or state in which the company does not have a business relationship or presence may be cause for further investigation.
- calls to known competitors—Call logs that indicate someone is calling a known competitor could be cause for further investigation.
- calls outside of normal working hours—Typically, organizations have defined working hours for staff. Calls made outside of working hours may be cause for concern. For example, an employee makes a call at 8 p.m. from their desk phone but is only scheduled to work until 5 p.m.
- specific calling patterns
    - Various roles in the organization may develop calling patterns over time. For example, a particular group of employees within the sales department always calls their customers in a particular territory on a particular day of the week. Any deviance from these patterns may be cause for further investigation.
    - Employees accessing sensitive information and making an outbound call may be cause for concern depending on the individual's role. For example, an employee accesses sensitive information and then calls a foreign phone number.

1.3 *Common Sense Guide* References

- Practice 12: Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.

2 Monitor and Control Privileged Accounts

System administrators have access to the internal workings of the IT system's operating system and data. Administrative users are not typically bound by Access Control Lists (ACLs) that protect systems from tampering and protect data from inappropriate access by regular users. Organizations must rely solely on the privileged user to follow company policy and best practices for handling of sensitive information.

It is not enough to rely on the perceived goodwill of an administrator. A disgruntled systems administrator is capable of altering or destroying systems and data, causing downtime or reducing availability. The malicious insider could configure systems so that the destructive payload is only activated by a predetermined condition. For example, a malicious insider could plant a logic bomb on production servers that erases all of the organization's data if the insider's name is removed from the payroll system or does not log in for a predetermined amount of time.

2.1 Case Studies

2.1.1 Case Study 2

The insider, a contractor, was employed as a systems administrator by the victim organization, a government entity that was operating in Europe. The insider, who owned his own company, became disgruntled when his contract proposal to replace a fellow system administrator was rejected and the work was awarded to another firm. The insider decided to sabotage the victim organization's computer system to make the new system administrator look bad. Over a period of two days, the insider sabotaged the organization's systems by planting logic bombs on five servers, which were set to detonate (as a cron job) after he left to return to the United States. When the logic bomb detonated, three of the servers, which were used to track and plot the locations of ships, submarines, and underwater obstructions, and a computer database filter were damaged and went offline. Another system administrator searched for malicious code, uncovered the other two logic bombs, and was able to prevent the commands from affecting the other targeted computers. The victim organization took extensive steps to secure and restore the network. The insider was arrested, convicted, ordered to pay $25,000 restitution and a $10,000 fine, and sentenced to 12 months and 1 day of imprisonment followed by three years of supervised release.

2.1.2 Case Study 3

The insider was employed as a systems and network administrator by the victim organization, an internet service provider (ISP). The insider oversaw the operation of, and had complete control of, the organization's entire computer network. The insider left the company abruptly and without explanation. Subsequently, the organization declined the insider's request for back pay. The insider sued his former employer to collect approximately $2,000. Four months after his termination, the insider remotely attacked the victim organization's network on two occasions. The first attack wiped out all data, including all data and configuration settings on 12 machines in the organization's network, temporarily crippling the system for 15 hours. The organization's customers continued to experience sporadic service for several days, causing the organization's

business to suffer. The organization took steps to secure its system against similar attacks. Ten days after the first attack, the organization was hit with another electronic intrusion. The second attack erased various operating systems and configuration settings on unprotected machines not previously targeted. Computer forensics analyses revealed that the insider attempted to erase all electronic traces of his identity, but the attacks on the organization's system could be linked to other computers outside the organization that were in use or otherwise controlled by the insider. Among those outside computers was a computer that the insider was surreptitiously controlling as a slave intermediary computer from a remote location. The slave computer was sitting in the insider's former cubicle at a company where the insider had worked prior to joining the victim organization. The insider was arrested, convicted, ordered to pay $118,000 restitution, and sentenced to five months of imprisonment followed by five months of home confinement.

2.1.3 Case Study 4

The insider was originally employed as a contractor by the victim organization, a local ISP. Internet services were provided by computer-operated wireless radio (Wi-Fi) signals between the ISP's radio towers and customers' wireless access points. Radio towers and access points were computer controlled. After resigning from the victim organization over business and financial disputes, the insider went to work for a competitor ISP and eventually acquired ownership of it. Less than two weeks after the insider's resignation, he used remote access and administrator passwords to take control of the victim organization's network. The insider intentionally brought down wireless internet services across the region by executing written programs and commands on the radio-tower computer and reprogramming wireless access points. The insider's programs and commands locked the victim organization out of each access point and prevented the organization from repairing the damage remotely. The incident also caused the access points to repeatedly broadcast radio signals that interfered with the signals of another ISP. The victim organization had to manually repair the network, leaving 170 customers without internet services for as long as three weeks. The victim organization's losses exceeded $65,000. The insider was arrested, ordered to pay $65,000 restitution, and sentenced to 24 months of imprisonment followed by 36 months of supervised release, including 50 hours of community service.

2.2 Solutions

Instances of IT sabotage can be difficult to detect and prevent. An organization must be able to trust its current system configurations and data before implementing an IT sabotage detection program. That is, an organization must be able to trust that its systems are currently free from malicious configurations and the data stored on the systems is accurate. If the organization can confidently say that its systems are in order, then it should leverage its current configuration management program or implement one that will help detect changes to systems and data.

Software and hardware solutions should do the following to mitigate IT sabotage:

- monitor and alert for changes or deletions to critical system files or data—The organization's IT security team or IT department should identify critical files on systems that need protection and monitor these files for changes, including the deletion of these files.

- detect scheduled tasks or cron jobs and changes to these processes—Scheduled tasks or cron job information is typically stored in a file or multiple files. These files should be monitored for changes.
    - Microsoft Windows systems typically store scheduled tasks in %SYSTEMROOT%\Tasks
    - Linux cron jobs for individual users are typically found in /var/spool/cron/crontabs (each user with a cron job will have a file in this directory)
- require at least two administrators to accomplish a critical task or to change or delete critical files or data—Organizations should consider implementing controls that monitor and/or prevent a single user from manipulating or deleting critical files.
- monitor the use of administrative accounts
    - Give administrators should have a standard user account and an administrative account. Administrative accounts should be placed under additional monitoring and auditing controls.
    - Configure the SIEM to alert when employees log into the organization's networks remotely using an administrative account if this type of activity is outside the employee's normal job function. Organizations may want to consider prohibiting remote administrative access if it is unneeded. Otherwise, remote administrative access should be conducted only from an environment with additional monitoring and safeguards in place.
    - Review accounts on a regular basis. Verify that accounts are still needed and have not been dormant.
    - Ensure that all accounts associated with an employee have been disabled when the employee separates from the organization.
    - Require all administrators to change their passwords when a fellow administrator leaves the organization. This should include changing service account passwords.
- establish approved baselines for each type of system—Organizations should have a trusted baseline for each server and workstation. Each job function or server role may have a trusted baseline as well. If properly maintained, a trusted baseline image can be compared against production systems to detect changes. Changes to systems should have an associated, approved change request and/or helpdesk ticket.
- require independent code reviews for any script or code that is implemented on a production system—Organizations should require someone other than the author of the script or source code to review it before it is placed on a production system. The programs should not be implemented by the person who developed it.

2.3 *Common Sense Guide* References

- Practice 10: Institute stringent access controls and monitoring policies on privileged users.
- Practice 19: Close the doors to unauthorized data exfiltration.

3 Monitor and Control External Access and Data Downloads

Organizations commonly use Virtual Private Networks (VPNs) for teleworking, allowing employees and trusted business partners the ability to work from any location in the world with an internet connection. VPNs keep employees productive and connected while away from the office. However, they can be an avenue of attack by a malicious insider, who could use remote access to damage systems and pilfer valuable intellectual property (IP). The organization must carefully monitor and control the use of VPNs.

Organizations should consider regularly reviewing VPN logs. SIEM systems can consolidate and automate this process. Furthermore, organizations should implement two-factor authentication solutions, not only to control authorized access, but to help mitigate the risk of a recently departed insider accessing the systems. For this particular solution to work, access tokens should be collected and logical access should be terminated when an employee leaves the organization.

3.1 Case Studies

3.1.1 Case Study 5

The insider, a contractor, was formerly employed as a consultant to the victim organization, a medical supply facility. The insider, who owned a consulting firm with a partner, was hired to set up networks at the organization. While working for the victim organization, the insider was observed probing its network, but no disciplinary actions were taken. One of the victim organization's clients also reported that insider was gathering information about him. The insider was bought out of the consulting partnership due to drug use. After the partnership dissolved, the insider threatened to get revenge against his former partner. At the time of the incident, the insider's former partner was employed as an information systems manager at the victim organization. Over the course of a month, the insider used unauthorized remote access to attack the organization. The insider installed remote control software, deleted and modified data, and changed administrative passwords to prevent access to the network. The insider also copied files from his previous partner's business. The incident was detected when the organization discovered that server passwords had changed. Remote access logs and ISP logs connected the insider to the incident. The insider was arrested and convicted, but he committed suicide prior to his sentencing.

3.1.2 Case Study 6

The insider was a former chief financial officer of the victim organization, but his contract was not renewed after a set of heated emails between the insider and the general manager reached the news. One month later, the insider used the username and password of a current employee of the organization to remotely access the organization's computer system from his home, send at least 13 emails from coworkers to his personal email account, download some files, and delete information. The information technology director discovered the insider's unauthorized access through a routine check of the email system and filed a police report. The insider was interviewed by a detective and admitted his actions. During the interview, the insider bragged about using the password belonging to other employee of the organization and told the detective he accessed the computers illegally to prove the computer system was not secure. The insider was arrested and

charged with 13 counts of computer crime with intent to defraud, 7 counts of modifying information without authority, and 1 count of deleting information from the victim organization's computer system. He was released from county jail on pretrial conditions.

3.1.3 Case Study 7

The insider was previously employed as a network engineer at a retail organization. The organization used USB VPN tokens for remote access, and before the insider was fired, he created a token in the name of a fake employee. A month after termination, the insider contacted the IT department using the fictional ID he created and convinced them to activate the VPN token. Several months later, the insider accessed the VPN and deleted virtual machines, shut down a Storage Area Network (SAN), and deleted email mailboxes. It took the IT staff 24 hours to restore operations and cost the organization more than $200,000.

3.2 Solutions

Organizations must carefully control and monitor VPN usage, as it must for other accounts on the system. VPN concentrators and access gateways should be configured to log connection attempts that include date and time, username, source IP address, and any information about the connecting client (Windows, Linux, hostname, etc.). Information about the connecting client could prove useful for discerning if the client machine is a company owned or authorized asset.

The following data points may help in identifying malicious insiders:

- VPN bandwidth utilization—Utilization that exceeds normal, similar users may be indicative of a problem. Baselining normal usage is key to implementing this indicator.
- client details of the connecting system—VPN clients may provide additional details about the host connecting to the system, such as host name and operating system. This is not a foolproof method, but it does help detect unsophisticated users. Also, this could be useful in alerting on clients with unrecognized values. For example, if the organization allows VPN connections from laptops, and all laptop hostnames begin with *LT-*, any connecting laptop hostname that does not match this pattern may be cause for concern.
- connection times—VPN connection times that fall outside of the user's normal work hours may be cause for concern.
- connection locations—The organization could build a connection profile of a particular user by understanding the user's connection habits and metadata. For example, if the user typically works from home and connects from a particular ISP's net block, a SIEM should be able to detect users connecting from a different IP address range.
- connection protocols and remote control software
    - The organization should implement firewall rules for blocking communications to unauthorized services.
    - Systems should be monitored for unauthorized software or attempts to install unauthorized software.

3.3 *Common Sense Guide* References

- Practice 7: Implement strict password and account management policies and practices.
- Practice 12: Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
- Practice 13: Monitor and control remote access from all end points, including mobile devices.
- Practice 14: Develop a comprehensive employee termination procedure.

- Practice 17: Establish a baseline of normal network device behavior.
- Practice 19: Close the doors to unauthorized data exfiltration.

4 Protect Critical Files from Modification, Deletion, and Unauthorized Disclosure

Organizations produce sensitive information as part of day-to-today business operations. This information may be stored across a variety of systems and media throughout the organization. Users may store sensitive files on their personal workstation, a central file server, or a removable device, such as a USB flash drive. Newly created files typically inherit the security permissions (ACLs) of the folder in which they are placed, so security permissions for new files need to be assessed as new content and may need to have additional permissions set to be commensurate with the protection needed or be moved to a location that affords additional protections. Additionally, files lose defined ACLs when they are copied to removable media.

A key concept to protecting the organization's data is to understand what must be protected. The organization must have policies, such as a data classification policy, that define what information it deems sensitive and how to protect it while at rest, in motion, and during processing. Furthermore, the organization must understand where all of its sensitive information lives. Possible locations for sensitive information include workstations, servers, removable media, cloud storage, backup tapes, and mobile devices.

Organizations that fail to protect critical information, including system configurations, risk giving a malicious insider the ability to create a denial-of-service (DoS) condition within the organization's systems. That is, a malicious insider could cripple the organization's systems by modifying or deleting critical files, causing systems to become unavailable.

4.1 Case Studies

4.1.1 Case Study 8

The insider was employed as a programmer by the victim organization, a state lottery. Prior to leaving his job at the victim organization, the insider copied his entire document folder to a CD. The folder contained personally identifiable information (PII), specifically names and social security numbers (SSNs), for 27,000 lottery winners. It also contained names, SSNs, and in some cases bank account and routing numbers for 639 current and former victim organization employees and more than 534 lottery retailers. The insider left the organization for a new job at another state entity. During his employment there, the insider copied the folder containing the PII from the CD to the hard drive on his work computer. The insider's new employer detected the stolen information on the insider's work machine. The insider was subsequently fired, and the information was turned over to criminal investigators. The insider later stated that the purpose of retaining the information was to preserve his computer programming work and personal files for future reference, specifically to acquire programming positions at other state agencies. There was no evidence that the information was otherwise misused. Verdict and sentencing details were unavailable.

4.1.2 Case Study 9

The insiders were formerly employed as executives by the victim organization, a hotel chain. The insiders were heads of the victim organization's luxury and lifestyle brands. A beneficiary competitor organization recruited the insiders for employment. During the last few months of employment, the insiders compiled and stole a minimum of 100,000 electronic documents related to the victim organization's highly successful luxury hotel chain. The insiders used email to transfer some of the documents and also physically shipped documents to their home addresses. After joining the beneficiary organization, the insiders used the stolen information to develop a similar luxury hotel chain. The information contained high-level instructions for launching a new hotel brand and saved the beneficiary organization the time and tens of millions of dollars required to develop a brand image. The stolen documents were placed on the beneficiary organization's servers, and at least 44 of the beneficiary organization's managers reviewed the documents. The victim organization's counsel discovered emails from the beneficiary organization's executives in which they discussed sanitizing the documents. The victim organization filed a corporate espionage suit against the insiders, the beneficiary organization, and others employed by the beneficiary organization, including its chief executive officer and its head of global development. The beneficiary organization responded by voluntarily returning more than 540,000 pages of stolen documents, claiming that they were not sensitive or confidential. The civil suit has been settled and requires the beneficiary organization to make a substantial payment to the victim organization. In addition, an injunction prohibits the beneficiary organization from starting any "luxury and lifestyle" hotels for two years, and two court-appointed monitors will oversee the beneficiary organization's compliance with the agreement.

4.1.3 Case Study 10

The insider was employed as program manager of the security division by the victim organization, a software development company. Unbeknownst to the victim organization, the insider was the founder and chief executive officer of a competitor organization, the beneficiary organization. The beneficiary organization held a patent for a specific technology. The insider claimed that he discussed allowing the victim organization to use the technology but that the victim organization rejected the offer and subsequently developed technology that infringed on the beneficiary organization's patent. The beneficiary organization planned to sue manufacturers that pre-installed the victim organization's software on computer systems because the software allegedly infringed on the beneficiary organization's patent. To strengthen the patent infringement case, the insider sought employment with the victim organization. The victim organization, believing the insider's claim that his competing organization had gone out of business, hired the insider. Over the course of three years, the insider accessed confidential business documents that were directly related to the patent infringement litigation but had no relation to his duties as an employee. The insider downloaded the information onto a laptop issued to him by the victim organization and subsequently deleted the files. To conceal his actions, the insider used software that overwrites deleted files. Four days after the victim organization accused the insider of trying to hide downloads of internal documents, the beneficiary organization filed its patent infringement lawsuit. Four months later, the victim organization fired the insider. The victim organization filed a civil suit against the insider and the beneficiary organization. Terms of the settlement were confidential. The suit also settled the patent infringement case filed by the beneficiary organization.

4.2 Solutions

Organizations need to protect critical files from unauthorized modification, deletion, and disclosure. These files may contain sensitive information, IP, device configurations, and other important data. To protect critical files, organizations should consider solutions that have the following characteristics:

- automatically protect files that contain critical data—Data loss prevention (DLP) solutions may use document tagging, keywords, or other means for protecting sensitive data. When a DLP solution finds sensitive data, the solution places certain protections on the data.
- automatically encrypt or stop critical information as it moves to untrusted destinations or media—An insider threat solution should automatically detect the sensitivity of information and protect it accordingly. DLP solutions should detect data leaving the system through an enclave exit point, which includes data leaving the organization's control through network-based communications or removable media.
- detect changes and access attempts to critical information
    - Organizations must protect information deemed mission-critical from unauthorized modification, deletion, or access.
    - Auditing for critical files should be enabled. Audit logs should reflect successful and unsuccessful accesses or modifications to files.
    - Multiple solutions may be needed to detect changes to company data and device configurations.
    - Device configurations should be monitored daily—Changes should be reconciled with a change management request or helpdesk ticket. Also, a solution that is able to retrieve the device's current configuration and compare it against a trusted configuration could facilitate detection of malicious insiders.
    - Monitor and alert for changes or deletions to critical system files or data—The organization's IT security team or IT department should identify critical files on systems that need protection and monitor these files for changes, including the deletion of these files.
- carefully monitor printing of critical files—DLP solutions should be able to detect and/or prevent unauthorized printing of sensitive files.
- create layers of defense for both internal and external-facing systems

In addition to these solution requirements, organizations need to be prepared for DoS attacks before they occur. This includes understanding the characteristics and traffic patterns of the organization's internal and external networks. Organizations should design network topologies that allow systems to be partitioned off the network in the event of a malicious attack and allow control of access to network resources. A segmented internal network topology can allow an organization to prevent attacks and respond to a malicious insider that may be harming systems or data. For example, employees in the sales department should not need access to systems in the human resources department. Therefore, separate VLANs can be created for these two departments with firewall or routing ACLs to prohibit access.

4.3 *Common Sense Guide* References

- Practice 6: Know your assets.
- Practice 8: Enforce separation of duties and least privilege.
- Practice 10: Institute stringent access controls and monitoring policies on privileged users.
- Practice 11: Institutionalize system change controls.

5 Disable Accounts or Connections upon Employee Termination

Many malicious insiders take advantage of their organization's lack of timeliness in disabling user accounts when an employee separates from the organization. Organizations may neglect to do this or do not have established policies and procedures for disabling accounts. When an employee departs, the organization must immediately terminate the employee's access to all accounts, including email, all information systems, cloud services, and any other account the employee may have had access to. Additionally, organizations should change the passwords to shared accounts and service accounts. If the former employee was a privileged user as part of a larger team, the organization should consider forcing a password reset on all other privileged user accounts to prevent the use of a compromised password by the former employee.

The IT department should also verify that no open connections exist that could allow the former employee back into the system. This includes closing all open VPN connections associated with the former employee. The organization should immediately collect all company-owned equipment given to the former employee, including laptops and mobile devices. Two-factor authentication tokens should also be collected. While collecting these devices does mitigate some risk of unauthorized remote connectivity, it is not enough to block access to all technical users. Therefore, access logs should be monitored for abnormal activity, especially activity associated with the former employee, for at least the next 30 days.

5.1 Case Studies

5.1.1 Case Study 11

The insider was formerly employed as a software engineer by the victim organization, a high-technology company that developed and manufactured computer chips. The insider was responsible for managing an automated manufacturing system. During the work week, the insider maintained a constant remote access connection from his home to the organization's network. The insider, who had previously worked in another department at the organization, was terminated due to poor performance. Prior to informing the insider of his termination, the organization terminated the insider's network access, but it failed to check if the insider's remote access connection was active. The day after the insider's termination and outside of working hours, the insider, under the influence of alcohol, used the open remote access connection to attempt to completely shut down the organization's manufacturing system by deleting critical files. Due to the insider's actions, the organization lost four hours of manufacturing time and had to load backup data to restart the manufacturing process. The incident cost the organization $20,000 to remedy. Connection and activity logs connected the insider to the incident. The insider was arrested and convicted, but sentencing details were unavailable.

5.1.2 Case Study 12

The insider was formerly employed as director of information technology and promoted to vice president of technology by the victim organization, which published financial market information. During his employment, the insider was responsible for overseeing the company's computer

network and internal email system. Three years after his termination, the insider remotely accessed the organization's internal email system. The insider was able to remotely access the company's network because user IDs and passwords remained virtually unchanged over the three-year period. The insider spied on email traffic for more than five months and intercepted emails of the human resources director and high-level executives. The insider focused on emails that discussed terminating employees. The insider used a Yahoo! email account to notify two employees of their potential terminations, and those employees reported the incidents to their supervisors. The victim organization spent more than $100,000 investigating the hacker. Remote access log files as well as records from Yahoo! and the insider's ISP connected him to the crime. The insider was arrested, convicted, ordered to pay $32,000 in fines and restitution, and sentenced to one year of probation with the first six months to be served under home confinement.

5.1.3 Case Study 13

The insider was originally employed as a programmer by the victim organization, a power company. The insider was responsible for programming the models that controlled the management of power facilities. The insider was terminated for poor performance. The organization escorted the insider off of the premises, but it failed to disable his VPN access and collect his company-issued laptop. Hours after his termination, the insider used his VPN to modify and delete files from the organization's intranet. The insider also transferred proprietary information to a personal email account. Company logs showed that the VPN connection was from the insider's home IP address. While logged into the VPN, the insider sent an email to the engineering group operating a nuclear reactor. In the message, the insider asked what would happen if the load of the reactor were increased to 99.7 percent capacity. The incident stalled the organization's energy forecast system for one day, costing the organization $26,000. It appears that the insider was never prosecuted for the incident. The only court document found was a search warrant for the insider's home.

5.2 Solutions

To reduce the likelihood of a former employee gaining access to the organization's systems and data, the organization should consider security solutions that are able to

- link human resources information systems to logical access systems
  - When the human resources department out-processes an employee, this information could be used to initiate account suspension actions across the organization. Additionally, the HR system could also be linked to the physical security access system to revoke building access privileges across the organization.
  - Accounts should be locked for employees who will be on extended leave or vacation if they will not have a business need for access to the organization' systems.
- regularly audit user accounts
  - Software that can facilitate regular, automated auditing and reporting of accounts will help the organization detect dormant accounts. Software should be able to determine when the account was last used. Accounts that have not been logged into within the organization's defined time frame should be disabled either by the reporting application or by an administrator.
  - Active account lists should be regularly compared to the current employee list to detect unauthorized accounts.

- implement two-factor authentication for critical systems, including remote access gateways—An added benefit of two-factor authentication is that the access token can be collected if the employee leaves the organization. Without the token, remote access to the organization's systems will be less likely.

5.3 *Common Sense Guide* References

- Practice 7: Implement strict password and account management policies and practices.
- Practice 10: Institute stringent access controls and monitoring policies on privileged users.
- Practice 13: Monitor and control remote access from all end points, including mobile devices.
- Practice 14: Develop a comprehensive employee termination procedure.

6 Prevent Unauthorized Removable Storage Mediums

Organizations may need to use removable media for various business purposes. However, if not properly monitored and controlled, removable media can be used by malicious insiders to copy valuable IP or sensitive data.

Organizations must carefully control and monitor who has access to removable media and the devices capable of using the media. The organization should consider what types of media are authorized and needed by the organization. Removable media include USB flash drives, external hard drives, mobile devices, and recordable CDs or DVDs. The organization should also review what devices are capable of using removable media, including laptops, workstations, servers, and mobile devices. Policies and procedures can be designed that address the types of media that are approved and which devices are authorized to use the media.

6.1 Case Study

6.1.1 Case Study 14

The insider left his position at the victim organization after accepting a position at a new employer. Up to a week before departure, the insider attached at least three external storage devices including one 3-TB external hard drive. The insider accessed and downloaded tens of thousands of customer files, confidential information, and nonconfidential proprietary information. These files included quotes, deals, proposals, contracts, and files containing forecast analysis, market analysis, and information downloaded from a third-party database. After departing from the victim organization, the insider used the information to identify four other employees who had relationships with high-profile customers. The insider convinced these employees to leave their positions at the victim organization and to accept positions at the new employer. Prior to leaving the victim organization, the recruited employees also attached external storage devices and downloaded confidential and nonconfidential proprietary information. After the employees departed from the victim organization, one of the recruited employees accessed his email account from the victim organization and forwarded emails from this account to a personal email account. This alerted the victim organization a possible breach of information and triggered a detailed investigation that directed the victim organization to the other employees recruited as well as the recruiting ex-employee. The victim organization alleges that the new employer and the previous employees used the downloaded information knowingly to identify and gain new customers.

6.1.2 Case Study 15

The insider was employed as a product engineer by the victim organization, an automobile manufacturer. As a function of his job, the insider had access to the organization's trade secrets and design specification documents. Two years prior to leaving the organization, the insider downloaded design specification documents, which contained trade secrets of the victim organization. The insider used this information to help him acquire employment with a foreign competitor. A year and a half later, the insider accepted a job offer from a U.S.-based company that manufactured automotive electronics in China, the primary beneficiary organization. After

accepting the offer, the insider remained with the victim organization for two months. The night before leaving the victim organization, the insider downloaded 4,000 documents, including sensitive design documents, onto an external hard drive. The insider downloaded design specifications for trade secrets such as the engine and transmission mounting subsystem, electrical distribution system, electric power supply, electrical subsystem, and generic body module. The documents were valued between $24 million and $32 million. The majority of these documents were not related to the insider's job. The insider traveled to the primary beneficiary organization in China. Two weeks later, the insider submitted his resignation to the victim organization via email. Subsequently, the insider began working for the primary beneficiary organization. Fifteen months later, the insider began working for a secondary beneficiary organization, the victim organization's direct foreign competitor. Nine months later, the insider returned to the United States and was arrested at the airport. At the time of his arrest, the insider was carrying a laptop he acquired from the secondary beneficiary organization. A forensic examination of the laptop revealed that the insider had stolen thousands of confidential, proprietary documents from the victim organization and another unnamed organization. The insider was arrested and convicted, sentenced to 70 months of imprisonment as well as two years of supervised release, and fined $12,500.

6.1.3 Case Study 16

The insider was employed as a chemist by the victim organization, which manufactured paint. The insider, accompanied by a coworker, made a business trip to a foreign nation to work with one of the victim organization's foreign subsidiaries. The coworker noticed that the insider was unusually interested in a foreign competitor organization. Prior to resigning, the insider visited the competitor organization and negotiated employment with it. The insider abruptly resigned, raising suspicion at the victim organization. Subsequently, the victim organization investigated the insider. The victim organization examined the insider's returned company laptop and discovered that the insider had deleted all of the temporary files in an attempt to conceal his history. The victim organization also discovered a hidden file that contained a prohibited data copy program and 44 GB of unauthorized data, including some trade secret information. When the insider was attempting to fly to the foreign nation, authorities executed a search warrant for the insider's luggage and discovered a USB drive containing the victim organization's trade secret information, including formulas for products that the insider should not have had access to. A search of the insider's home revealed that the insider had taken numerous documents and other materials from the victim organization's offices. Authorities also noticed that the insider's LinkedIn profile stated that he was employed by the foreign competitor organization. The duration of the incident was approximately five months, but the majority of the trade secret theft occurred in the two weeks prior to the insider's resignation. The insider was arrested, convicted, sentenced to 15 months of imprisonment followed by three years of supervised release and ordered to pay $30,000 restitution.

6.2 Solutions

Solutions that mitigate the risks of removable media should be able to

- restrict the use of unauthorized media
    - Software solutions should be able to detect and prevent certain types of media from being used within the organization.

    - The organization may wish to limit usage to approved devices by allowing data transfers to select devices with certain serial numbers.
    - Only approved users and/or workstations should be permitted to access and transfer data. Software solutions, including built-in operating system controls, should be able to control user access to removable media. Workstations and users who are permitted to transfer files should be under additional auditing to detect unauthorized transfers or media.
    - Consider limiting the capacities of removable media to the minimum amount required to complete day-to-day business operations. Smaller capacity devices limit the amount of data that can be copied at one time, increasing the chances of drawing attention to a malicious insider.
    - Limit the number of authorized devices issued to an employee. Organizations should be cautious about the number of devices issued because the aggregate capacity of all of the devices could allow an employee to exfiltrate large amounts of data. SIEM systems should log all removable media events.
- prevent sensitive data from being moved to certain media types
    - Only information that is deemed an acceptable risk may be permitted to be moved to removable media. The organization should implement solutions that limit the types of data that can be copied to removable media. For example, public information, such as press releases, may be permitted to be transferred to a USB flash drive, but sensitive information, such as customer PII, should not be permitted to be copied to any type of media.
    - The organization should automatically encrypt sensitive data as it is moved to storage mediums.
- alert on media usage
    - If the organization allows removable media company-wide as deemed necessary by a risk assessment, the organization should implement additional auditing on all systems to alert on any type of removable media usage. These alerts should be stored on a central log server or SIEM for further analysis.
    - Central logging systems should be able to detect anomalous behavior among users and alert on transfers of information that are above predefined thresholds.
    - Organizations should consider comparing media purchase records with a list of personnel to whom the media are issued. For example, this could help detect someone using excessive amounts of CD/DVD media, which may require further investigation into that user's removable media usage.

6.3 *Common Sense Guide* References

- Practice 6: Know your assets.
- Practice 10: Institute stringent access controls and monitoring policies on privileged users.
- Practice 12: Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
- Practice 17: Establish a baseline of normal network device behavior.

7 Understand All Access Paths into Organizational Information Systems

Organizations should fully understand all methods of entry into corporate systems. Access paths can be broken down into two groups: physical and logical.

Physical access paths include

- wired networks
- wireless networks
- Bluetooth devices
- cellular modems or aircards
- USB devices
- VPN gateways and concentrators

Logical access paths include

- remote control software (e.g., GotoAssist, WebEx)
- cloud services (e.g., Microsoft SkyDrive, Google Drive, Dropbox)
- VPN clients
- malicious software

A malicious insider might use physical or logical technologies that the organization does not normally employ, so simply not using a particular technology does not protect an organization from that attack vector. Organizations need to have policies and procedures in place for detecting and documenting both authorized and unauthorized entry points into the system. Depending on the organization's tolerance for risk, as defined by a risk assessment, the organization may want to consider implementing countermeasures to prevent unknown access paths into their systems.

7.1 Case Studies

7.1.1 Case Study 17

The insider, a former employee managing shareholder officer and member of the victim organization's board of directors, and two conspirators abruptly quit the victim organization to join another company belonging to one of the conspirators. Prior leaving the firm, they deleted 5 percent of the victim organization's backup tapes for a particular group of client files and took 78,000 files from the victim organization's computer system. They also installed Dropbox software that gave the insider continuing access to the victim organization's computer network through remote access in order to direct some of the victim organization's clients to their new employer. According to forensic investigation, the stolen files were automatically transmitted to the cloud. The insider owned the building that housed the victim organization, and when the insider quit, he locked his office and the offices of the two conspirators that left with him, preventing the firm from retrieving its company-issued computers and stopping the transfer of the files to the cloud. The case was settled out of court. The terms of the settlement are unknown.

7.1.2 Case Study 18

The insider, a contractor, was employed by the victim organization, a high technology company that developed and manufactured various computer components. The insider worked for the organization for a few years before moving to the division where the incident occurred. The insider worked in the supercomputer division (SCD), which was devoted to creating extremely valuable supercomputers used for functions such as ensuring nuclear weapons safety. The computers were password protected, and the highly sensitive data was stored in an encrypted form. The division experienced a problem with its email systems, leading to a dispute between the insider and a systems administrator. The insider became disgruntled when his suggested approach to addressing the problem was not applied, and the systems administrator ultimately resolved the email issue with a different approach. The insider decided to leave this division of the organization because he felt that any decision he made would be superseded by the systems administrator. The organization disabled the insider's passwords to all but one of the supercomputers (Computer X). Subsequently, the insider began working as a contractor for another division within the victim organization. A year after the insider's dispute with the systems administrator, a colleague noticed that the insider was running a gate program, which enabled the insider to remotely access the organization's computers. The organization's security policies explicitly prohibited using gate programs because they breach firewall programs the organization uses to prevent computer intrusions. The colleague confronted the insider, who responded that he used the program to access his email while he was traveling but was aware that it violated the organization's security policy, and he agreed to modify the program. Five months later, the same colleague noticed that the insider was using another gate program and confronted the insider again. The insider requested that his account for that specific computer be closed, and transferred his gate program to Computer X. The insider downloaded a password cracking program and ran it on Computer X. The insider obtained a password for one of Computer X's authorized users, which he then used to log onto Computer X and copied its complete password file. The insider uploaded this password file to another SCD computer and used it to obtain 35 user passwords for those working in the SCD. The insider's goal was to use the breach to demonstrate that the security in the SCD had declined when the insider departed and to regain the respect he lost when he left the SCD. The insider ran the crack program on another SCD computer and used it to obtain additional information to demonstrate the inadequacy of the SCD's security. A colleague noticed that the insider was running the crack program and that the insider's password for Computer X had not been disabled. The colleague reported this to a network security specialist and the local police department. The insider was arrested, convicted, ordered to pay $68,000 restitution, and sentenced to five years of probation followed by 480 hours of community services. If the insider did not fulfill these obligations, he was to serve 90 days in jail. The restitution order was reversed, and an appellate court later expunged the conviction.

7.1.3 Case Study 19

The insider was part of the IT staff for a financial institution. The insider planted malicious code on more than 100 ATMs and stole more than $300,000 over a seven-month period. (Authorities later recovered $167,000). The malicious code allowed the insider to withdraw money without creating a record of the transaction. The bank discovered the loss through internal controls and notified the authorities, who captured the insider. The insider pled guilty to one count of unauthorized computer access for installing the malware.

7.2 Solutions

To prevent malicious insiders from using or creating unknown entry points into your systems, insider threat solutions should be able to

- detect changes to network devices
  - Organizations should monitor network device configuration changes for unauthorized changes. All changes should be approved by a change request and have supporting documentation.
  - Organizations should monitor device configuration changes for new interfaces, changes to routing tables, VPN gateway modifications, and VLAN changes.
- regularly scan networks
  - Information security staff should have a complete record of all devices connected to any organizational system. Unauthorized or unknown devices should be removed from the system upon detection.
  - Complete inventories of systems should include the specifications of all systems. IT staff should have device inventories of the make and model of the system, operating system, storage capabilities (hard drive capacity, CD/DVD burners, memory card reader/writer, etc.), network capabilities (wired, wireless, cellular, Bluetooth, etc.), whether or not the device has a built-in camera, and the approved baseline number of the device.
  - Organizations may find it helpful to coordinate inventorying of new systems with the receiving department and configuration manager. This will ensure that the physical device is recorded into the organization's property management system, and the configuration manager (or designee) can install the appropriate baseline onto the devices. The details of the device can be entered into the property management system at this time as well.
- scan for unauthorized wireless access points—Organizations should look for rogue access points by conducting regular wireless site assessments. Despite any relevant policies that the organization may have, a malicious insider may be able to connect wireless routers or access points to the organization's systems, creating an unknown access path.
- maintain an inventory of dual-homed hosts—If the organization requires certain systems to have multiple network interface cards configured with different subnets, then these hosts should be documented along with their business justification. The organization should maintain host-based firewalls on these systems to prevent unauthorized traffic from entering or leaving a particular network.
- prevent tethering of mobile devices (smartphones, cellular modems, etc.) when connected to organizational systems—Mobile device tethering can create a back door into a system by creating a dual-homed host. The mobile device could bridge the organization's trusted network with an external, untrusted network.
- restrict access to unauthorized software
  - Unauthorized software can create access paths into the organization. In case study 17, a cloud service provider used a client software package installed on a user's workstation. This allowed the malicious insider to synchronize sensitive, proprietary files with the cloud provider. The insider could then log into the service remotely to retrieve the files or synchronize with an unauthorized device. File synchronization can allow the malicious insider to manipulate files on any system, violating the confidentiality, integrity, and availability of the data.
  - Remote management software can allow a malicious insider to remotely control the organization's systems. These software packages are often used for authorized remote support or teleconferencing. Some of these software packages

allow the user to manipulate computer settings and copy files to and from a remote system.
    - VPN client software may have a business use with the organization's systems. However, end users should not be permitted to configure the software because it could be used to connect to an untrusted network, exfiltrate data, and create an unknown path into the organization.
- detect, prevent, and remove malicious software—Organizations should implement antivirus and antimalware software to prevent a malicious insider from installing malware that could be used to remotely access the system or exfiltrated data.

7.3 *Common Sense Guide* References

- Practice 6: Know your assets.
- Practice 11: Institutionalize system change controls.
- Practice 13: Monitor and control remote access from all end points, including mobile devices.
- Practice 19: Close the doors to unauthorized data exfiltration.

References

URLs are valid as of the publication date of this document.

[Silowash 2012]
Silowash, G.; Cappelli, D.; Moore, A.; Trzeciak, R.; Shimeall, T.; & Flynn, L. *Common Sense Guide to Mitigating Insider Threats, 4th Edition* (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, 2012.
http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	July 2013	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Insider Threat Attributes and Mitigation Strategies	FA8721-05-C-0003

6. AUTHOR(S)

George J. Silowash

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2013-TN-018

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
ESC/CAA 20 Schilling Circle, Building 1305, 3rd Floor Hanscom AFB, MA 01731-2125	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Malicious insiders pose a threat to the confidentiality, integrity, and availability of an organization's information. Many organizations look for hardware and software solutions that address insider threats but are unsure of what characteristics to look for in a product. This technical note presents seven common attributes of insider threat cases, excluding espionage, drawn from the CERT® Division's database. The note maps the seven attributes to characteristics insider threat products should possess in order to detect, prevent, or mitigate the threat. None of these attributes alone can identify a malicious insider. Rather, each attribute is one of many data points that an organization should consider when implementing an insider threat program.

14. SUBJECT TERMS	15. NUMBER OF PAGES
insider threat product capabilities, countermeasures, indicators	34

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL