Spotlight On: Malicious Insiders with Ties to the Internet Underground Community

March 2009

Michael Hanley
Andrew P. Moore
Dawn M. Cappelli
Randall F. Trzeciak

This work was funded by

CyLab
www.cylab.cmu.edu

Software Engineering Institute | Carnegie Mellon

Spotlight On: Malicious Insiders with Ties to the Internet Underground Community

This report is the second in the quarterly series, *Spotlight On*, published by the Insider Threat Center at CERT and funded by CyLab. Each report focuses on a specific area of concern and presents analysis based on hundreds of actual insider threat cases cataloged in the CERT insider threat database. For more information about CERT's insider threat work, see http://www.cert.org/insider_threat/.

In this article, we focus on insider threat cases in which the insider had relationships with the internet underground community. We begin by defining what we mean by the internet underground as it is used in the context of this article. We then provide a snapshot of the cases that focuses on who, what, why, and how. Next, we provide references to best practices that might have been effective in countering these incidents.

We would like to thank William Shore, retired Special Agent with the FBI who is now the Manager of Security at the Software Engineering Institute. Shore provided insights from the law enforcement perspective for this article. We would also like to thank our colleagues in CERT - including Julia Allen, Robert Seacord, and Carol Woody - who provided expertise related to the internet underground community, and Craig Lewis, who provided input on technical countermeasures for the cases in this article.

What is the internet underground?

The FBI defines organized crime as "…any group having some manner of a formalized structure and whose primary objective is to obtain money through illegal activities."[1] Whereas the word underground, "…describes an activity that is secret and usually illegal."[2] Initially, this article was intended to include insider crimes involving either the internet underground or organized crime due to anticipated similarities between the cases. However, after reviewing cases from the CERT database, we realized that organized crime and the internet underground produce very different types of insider threat. We use the following definition of Internet Underground for the purposes of this paper:

> *The Internet Underground is a collection of individuals with shared goals where there is some degree of hierarchical structure and the primary communication mechanism or agent of electronic crime involves the internet. Further, it may demonstrate some degree of pseudo-anonymity and/or secrecy, which may be useful for organizing and carrying out electronic crimes.*

Both the internet underground and organized crime are somewhat covert in their operations. Back room conversations are replaced by short-lived IRC chat servers while crime bosses and an ordered hierarchy of leadership is replaced by a forum administrator and a loosely cohesive set of followers. A point of interest, however, is that there are varying tiers of organization in the internet underground community. While the norm seems to be the looser tier of organization already mentioned, many of the top tier underground organizations are highly professional, extremely organized, and run in a fashion not very different from what

[1] See *Federal Bureau of Investigation – Organized Crime – Glossary* for more information. http://www.fbi.gov/hq/cid/orgcrime/glossary.htm

[2] See definition on *Cambridge Dictionaries* at http://dictionary.cambridge.org/

we think of as traditional organized crime. These are interesting facets of the problem to bear in mind as we continue our discussion of the internet underground community.

It is important to note that the goal of this article is not to recommend detection methods for locating insiders who are potentially involved with the internet underground. This type of activity would be prohibitively expensive and would likely have a fairly high false-positive detection rate given that several tools and forums in the underground do have legitimate uses in the technology world. Further, our emphasis on implementing best practices is not changed by the subject matter of this article. Rather, we hope that this article serves to demonstrate how motivated insiders can use the internet underground community and its resources as a lever of sorts, a force multiplier to amplify the impact of their attacks against the victim organizations in our incident examples. Also, the article attempts to demonstrate how implementing best practices might have patched organizational vulnerabilities that the insiders in these examples were able to successfully exploit.

Snapshot of Malicious Insiders with Ties to the Internet Underground

The majority of these incidents were IT Sabotage cases[3], which follow the escalation patterns documented in CERT's MERIT model of insider IT sabotage.[4] We believe it is important that organizations recognize the patterns described in the MERIT model and implement proactive measures to prevent or provide early detection of potential insider threats. The insiders discussed in this article were often the most technical individuals in their organizations; special care should be used when employing technically-skilled individuals with known or suspected connections to internet underground communities.

Range of Involvement

The case sample for this article reflects varying degrees in which insiders were involved with the internet underground community. At the low end of this range is a system administrator who worked for a market research firm and stole personal information he found on servers to which he had restricted access and that belonged to one of his employer's business partners. There was no evidence that he distributed the stolen data via the internet underground, rather he appeared to enjoy the thrill of collecting it and bragging about it in online IRC chat rooms.

Most of the insiders in the cases for this article used their ties to the internet underground to generate support for their attack. One insider had access to confidential trade secrets relating to anti-piracy technology used by an organization to protect its primary business service. The insider stole the information and actively distributed it throughout the hacker community to promote piracy of the organization's services. In another case, a system administrator for a retail clothing firm was terminated over issues with a server for which he was responsible. He then engaged the internet underground community for assistance in organizing and executing a denial-of-service attack against his former employer using passwords and access mechanisms provided by him.

[3] See *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* for more details on insider IT sabotage. http://www.cert.org/archive/pdf/insidercross051105.pdf

[4] See *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures* for a description of CERT's MERIT model of insider IT sabotage. http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tn041.pdf

Who they are

This article discusses ten incidents from CERT's insider threat library that include evidence of malicious insider involvement with the internet underground community. The sample incidents represent significant, although varying, degrees of association with the internet underground community. Of these ten cases, the majority of the insiders held technical roles, such as system administrators and technology architects. Only three of the insiders were in positions that were purely managerial or otherwise non-technical. Further, each of the insiders who demonstrated ties with the internet underground were male. Some of the insiders were characterized by fellow employees and their organization's leadership as the most technically valuable employees in the organization.

Why they strike

Eight of the ten insiders in this study were motivated by revenge against their employer. The other two insiders had motivators such as looking for recognition, proving some ideological point, or supporting an underground movement.

What they strike

Most attacks targeted the organization directly. For example, insiders deleted critical files, disrupted system operations by changing system configurations, and denied access by withholding passwords. Others used organization systems for their own illicit activities, by running sniffers and port scans of governmental systems. One targeted an unsuspecting outsider by changing her status to deceased in a critical government database. Other employees or contractors transmitted proprietary information to hacker sites, collected personally identifiable information (PII), and broke into systems and defaced web sites for fun. Some provided information to outsiders who used it to commit cyber crimes, including one person who posted instructions to an online hacker group on how to break into his organization's systems, and another who posted employees' personal information to a website.

How they strike

Sixty percent of the insiders were separated from their employers prior to the attack, and half of all attacks used remote access. The attacks themselves involved, at a high-level, the following technical methods:

- Exploitation of unpatched vulnerabilities
- Organized distributed denial-of-service (DDoS) attacks
- Theft of trade secrets by scanning physical documents
- Unauthorized use of a coworker's account or computer
- Malicious modification of data
- Use of backdoor accounts and unknown access paths[5]

[5] In the MERIT model of insider IT sabotage CERT defines an access path as "a sequence of one or more access points that lead to a critical system". Unknown access paths are access paths that are known to malicious insiders but not known to others in the organization.

Organizational Vulnerabilities Exploited and Potential Countermeasures

There are several overarching themes in our sample of cases; they have been categorized according to the organizational vulnerabilities exploited below.

Use of Unknown Access Paths Following Termination

In the cases summarized below, one employee used his underground connections to assist in carrying out a well-planned attack against his former employer, and one threatened to use his connections to carry out additional attacks. In a third case, an employee had been using his underground connections at work to download illegal materials, including hacking tools used later to attack the organization following termination. A fourth had a long ongoing history of internet piracy and electronic crimes.

In these cases, procedures for ensuring secure separation of employees at the conclusion of their employment were not sufficient to prevent an insider attack. Insiders were able to exploit access that was not disabled upon termination, allowed to copy data before leaving the facility for the final time, or able to access previously created privileged backdoor accounts used to attack the organization after termination.

1. A system administrator for a retail company was terminated over issues with a server for which he was responsible. Following his termination, the insider recruited members of an online hacking group to help him attack his former employer's systems. The insider relayed to the underground group passwords and other access control information that he held as part of his former role, and provided detailed instructions on how to use those credentials to break into his former employer's network. The insider was able to organize the group and execute a coordinated denial-of-service attack against the retailer that lasted from the day before Thanksgiving until the Sunday after Thanksgiving – commonly recognized as the busiest shopping days of the year.
2. A computer technician was fired shortly after starting work because he refused to give his social security number to the human resources department and he failed to disclose prior criminal convictions. Before leaving the organization, the insider stole personally-identifiable information related to 8,000 employees and posted it to a website he had established to smear the organization's image. The website threatened to publish more information and link it to underground sites known to facilitate and engage in identity theft and fraud. The insider had been with the organization for only a short time and was given root access to the systems he attacked within his first few weeks at the organization.
3. A systems administrator was fired after he had a confrontation with his manager over the possibility of being laid off. The manager had suggested that since systems were performing well, the employee's help may no longer be needed. Outraged by this, the employee immediately created a set of fictitious accounts with full access to all networked machines within his control and distributed a malicious application that would erase hard drives on command. The day after his termination, he remotely triggered the execution of that application and wiped out several devices at the organization. Several months after the initial attack, the insider attacked the organization a second time by modifying the DNS registration for the organization's external-facing website. He redirected the DNS name so that it resolved to a website that hosted pornographic images, racial slurs, and defamatory statements against the victim organization. During the investigation, it was discovered that during his employment he had broken into other sites while at work, and had accumulated a wealth of hacking material from various underground forums and websites that may have helped him launch his attack against his

former employer. In addition, investigators found disk loads of pornography, passwords, hack tools, credit card information, and music downloads.

4. The sole security administrator for a small telecommunications firm quit his job with no advanced notice. During his tenure with the firm, he had expressed feelings of dissatisfaction due to insufficient gratitude and compensation for his work, and also had a series of conflicts with coworkers. He had a lengthy history of pirating material online and had committed prior electronic crimes related to unauthorized system and network access. Following his termination, a manager at the organization called him at home to request administrative passwords since he had not turned them over to anyone when he quit his job. He refused to disclose the administrative passwords until he received additional pay to which he felt entitled. He turned them over three days later, after locking the organization out of all administrative functions. For a month afterward, he used backdoor accounts he had created previously to remotely access the organization's systems and delete files that he had created during his employment. He also changed the DNS records for the internet-facing servers to point to another server named to slander the organization, and launched other offensive attacks from within the organization's network, such as using the victim's network to run network scanning tools against government military networks.

Organizations should develop a formal employee termination process. The process should involve, at a minimum, mechanisms for inventorying known accounts and access paths so that they can be disabled immediately upon termination. To facilitate the execution of these plans, organizations should periodically inventory and audit all computer accounts so a relatively accurate list of valid accounts can be retrieved on short notice. In addition, access to shared accounts should be carefully controlled and tracked at all times so that access can be disabled upon an employee's termination.

Part of the termination process should include a debriefing of the employee before they exit the facility. If a non-disclosure or intellectual property agreement was signed by the employee as a condition of employment, he or she should be reminded of the legally-binding commitment to safeguard company trade secrets and other terms, such as a non-compete clause, after the separation. If possible, the exiting employee should be asked to sign another non-disclosure agreement as evidence that he or she understands the non-disclosure requirements for sensitive organizational information and how it may or may not be used in the future. If a former employee does disclose information in an unauthorized fashion, a signed NDA and proof that the individual was reminded of those responsibilities when exiting the organization provides substantial evidence for legal action taken against that former insider.

Termination procedures also should, when feasible and when necessary, attempt to identify any pre-established unknown access paths. The MERIT model describes the typical pattern of behavior in insider IT sabotage cases; organizations should go to greater lengths to attempt to uncover unknown access paths that might have been created by a terminated employee if this pattern of behavior is evident, because the behavior suggests increased risk of attack following termination.

Employee termination procedures should also include communication to the rest of the organization that the trust relationship with the former employee has been terminated, and that the employee should not be allowed physical or electronic access from that point forward.

One additional item of note pertains to the last two cases described in this section, both of which redirected external DNS registrations to crafted sites meant to disrepute and slander the victim organization. Authorization to maintain DNS registration falls under a special category of highly-privileged, but infrequently used functions that require special documentation. Because these functions are used infrequently, access to them may go unnoticed and be forgotten when an administrator leaves the organization. This leaves a potential access path for a disgruntled insider to exploit for months, if not years, after the separation takes place. A suggested countermeasure is to maintain an inventory of privileged functions and a list of employees who have authorization to execute those functions. A regular review of this inventory for necessary changes based on job function or employment status can help mitigate the risk of items such as this that may slip through the cracks with serious consequences.

Insufficient Access Controls and Monitoring

One of the cases below resulted in the posting of trade secrets associated with anti-piracy technology to an online underground community, and two exposed customers' personally identifiable information and credit card information to underground individuals and newsgroups dedicated to credit card fraud. These incidents demonstrate the consequences of insufficient access controls and monitoring of access to highly-sensitive information and materials.

1. The insider in this case was an unofficial employee of a document-imaging firm, contracted by a law firm that was working for a telecommunications provider as outside counsel. The insider was unofficially employed in that his uncle was an employee of the document-imaging firm, but was bringing in his nephew, the insider, to help with a backlog of work at night. The insider converted scanned .TIF images of trade secret documentation associated with anti-piracy technology to PDF format and transmitted them to the leader of an online community whose purpose was to pirate the services offered by the telecommunications firm. The forum administrator who was contacted by the administrator originally refused to post the information for the community, stating it was too sensitive to be released, but eventually did so anyway under pressure from the insider.

2. A database administrator responsible for a very large database containing personal employee information for an insurance company became frustrated over time by what he perceived to be unfairly low pay. He lashed out at the organization by downloading personal information associated with employees from the database to removable media. In the end, he had stolen over 60,000 employee records from his employer. In an attempt to damage the victim organization even further, he solicited bids for the sale of the information over the internet. He used message boards to advertise the availability of the information to underground individuals, whom he hoped would be able to abuse the information in damaging ways. He also leveraged newsgroups dedicated to credit card fraud to post employee credit card numbers and encouraged the malicious use of these credit cards and suggested that readers of the newsgroup use the information he was providing to obtain additional credit cards in the names of victim employees. Law enforcement eventually captured the insider when an undercover agent posed as a potential buyer of the insider's stolen information.

3. A system administrator had authorized access to sanitized databases of customer information on an FTP server hosted by one of his organization's business partners; the business partner was contracted by financial institutions and phone companies to perform services using customer data. He located an unsanitized version of these customer databases when looking around on the FTP server. The databases were protected with passwords and encryption. The insider ran a password cracking utility and obtained over 300 passwords he could use to access the protected information. He found original and complete phone records, billing information, and other personally-identifiable information for millions of Americans. He proceeded to download millions of customer records from the databases,

including social security numbers, birthdates, and other personal information. The insider bragged in online IRC channels about his access to confidential and personal data, and was asked at one point by another individual in the chat room to provide data on an FBI agent who was actively investigating him. The insider provided the information within minutes. The ongoing FBI investigation of that individual led back to the insider, who was found with dozens of CDs and other media containing millions of customer records in his apartment. There was no evidence of broad scale distribution of the data, rather he appeared to be stealing the information to brag about it in IRC chat rooms.

A common theme in these cases is largely unrestricted access to proprietary data by the insiders, due to poor data handling policies and practices and lack of granular access controls. In the first example, company trade secrets were left largely unsecured in the hands of a contractor. Trade secrets should be protected appropriately given their value. For example, leveraging physical security standards for document storage and placing a security guard charged with safeguarding the data at the contractor site might have been in order. Similarly, in the third case, proprietary information from the organization's customers was inadequately protected from access by another trusted business partner. Legal controls to ensure contractor compliance with organizational data handling policies could be employed to protect against the extended pool of insiders created by working with vendors and other external partners. These measures would allow contractors to perform their work, while protecting the victim organization's sensitive information.

The second case involves an insider with uncontrolled and unmonitored access to proprietary data. Although it is difficult to control access by database administrators, countermeasures should be considered for critical organizational data. For example, a "two sets of eyes" policy could be implemented and technically enforced, whereby two database administrators together are required to perform sensitive functions. Other possible solutions involve delegation models that use technical measures to limit the control that any one account has over the environment, or cryptographic controls that require the use of specifically-trusted devices that cannot be removed from a controlled area to perform sensitive functions. These techniques limit the insider's capacity to misuse access to systems or data without having at least one accomplice.

Inadequate Environmental and Situational Monitoring and Awareness

In the cases below, one insider enlisted the assistance of an associate from the internet underground in planning and executing his attack, and another threatened his organization with those actions. In an interesting twist, a third insider retaliated against an underground associate using access to his employer's data. A common element of concern in these cases involves insufficient network and environment situational awareness. Insiders were able to execute actions that required some form of elevated access or that put networked systems at risk without being readily detected by the organization's technical and non-technical security controls. For example, network scanners, critical database changes, and privileged backdoor accounts are all items of concern that should be detected and should generate alerts, as appropriate.

1. An employee working in a technical support role was caught with unauthorized software on his computer, and had his internet access suspended as a result. Angered by this, he recruited a friend to help him retaliate. Both the insider and his friend were active members of the hacking group, and regularly attended the organization's meetings. They used IRC channels to communicate back and forth with one another and relay information under assumed hacker names in an attempt to mask their identities. The two were able to gather enough information about the organization's systems that they successfully defaced the organization's website. Network sniffers were used to obtain a set of user accounts and passwords with which to launch the attack.

2. A system administrator and several of his colleagues were laid off by a financial firm. After receiving the bad news, the insider contacted the victim organization and threatened them. He stated that if he did not receive a significantly larger severance package and good employment recommendations, he would recruit his friends from an underground internet hacking ring to attack the victim organization. He also claimed to have opened backdoors throughout the victim organization's systems to facilitate such an attack. The insider was arrested before the attacks ever came to fruition.

3. A government claims representative had a confrontation in an online chat room that was unrelated to his organization. Because the representative, as part of his employment, had access to a critical U.S. government database, he was able to target the host of the chat room and make a malicious change to the host's data in the government database. The insider changed the chat room host's status in the database so that she appeared as deceased. This action caused the host enormous inconvenience in financial transactions that were disrupted due to her deceased status.

There are many tools and practices available to assist organizations in achieving a greater degree of awareness about what is occurring on their networks. In these cases, insiders employed port scanning utilities, network packet capture tools, made unauthorized database changes to critical fields that went unnoticed, and claimed to create backdoor accounts; the existence of which could not be confirmed by the victim organization. Several of these actions can be detected via system monitoring and auditing. For example, by tracking critical database changes, such as changing a person's status to deceased, the changes can be reviewed by a second person to reduce the number of human errors or malicious changes that are entered into the production database.

Conclusions

The threat of insider actions associated with the internet underground is very real. As shown in the case examples, the actions observed in our case database occur primarily out of revenge that stems from unmet expectations and disgruntlement over salary or other work issues. Many of the attacks occurred offsite, after an employee's termination, using access and prior knowledge the employee had as part of his job role. Further, nearly all attacks involved the use of at least one form of compromised account, such as an authorized third-party account or a backdoor account created specifically for the execution of the insider's attack plans. Finally, all but two of the insiders in our case sample were considered to be highly-technical and were working in some kind of system administration role for the victim organization.

Of course, it is not always readily apparent that employees have connections with the internet underground. Employers can institute measures to block certain illicit communication channels at the workplace, or monitor and investigate their use. In addition, it is important that managers of technical employees exercise good management practices, including attempting to maintain a degree of awareness of employees' morale, and suspicious behaviors both at work and outside the workplace. A summary of the attributes of the cases is provided in the table below.

Case ID	1	2	3	4	5	6	7	8	9	10	Totals
Revenge			X	X	X	X	X	X	X	X	80%
Remote Attack	X			X	X	X				X	50%
Sabotage			X	X	X	X	X	X	X	X	80%
Theft	X	X	X				X		X		50%
Used own account	X			X		X			X		40%
Compromised account	X			X	X	X	X	X	X		70%
Backdoor account					X	X					20%
Coworkers account								X	X		20%
Attacked Alone	X	X	X		X	X		X	X	X	80%

The article also suggests how implementing best practices might have patched organizational vulnerabilities that the insiders in these examples were able to successfully exploit. In addition to some of the countermeasures discussed earlier in this article, CERT has published a separate report, *The Common Sense Guide to Prevention and Detection of Insider Threats,*[6] which provides 16 best practices that organizations should consider for preventing or mitigating insider attacks. While CERT identified these best practices based on the data collected and analyzed, organizations need to carefully consider which best practices are appropriate based on their unique organizational context. Practices that have special significance to this article have been summarized below.

PRACTICE 1: *Consider threats from insiders and business partners in enterprise-wide risk assessments.* Several of the cases in this article support the need to consider trusted business partners as insiders when

[6] http://www.cylab.cmu.edu/pdfs/CommonSenseGuideInsider-Threats-V3.pdf

performing enterprise-wide risk assessments. The scope of insider threats has expanded due to organizations' growing reliance on business partners with whom they contract and collaborate. As seen in a few of the case examples in this article, it is important for organizations to take an enterprise-wide view of information security, first determining its critical assets, then defining a risk management strategy for protecting those assets from both insiders and outsiders

PRACTICE 2: *Clearly document and consistently enforce policies and controls.* In the cases in this article, some of the employees felt that they were being treated unfairly. In addition, policies were not always enforced consistently. One insider was hired without providing his social security number – a policy violation in most US organizations. Policies should be documented, advertised to employees, and enforced with unambiguous and plain language. Publishing policies that are easy for employees to understand, and that stress the value of the data the policies are trying to protect, will help foster a culture of compliance.

PRACTICE 4: *Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.* Our case sample included a prime example of the importance of detecting suspicious behavior as early as the hiring process. Failure to provide a social security number and failure to investigate a system administrator's criminal background before granting root access to systems turned out to be a disastrous error in this case. Organizations should be especially aware of attempted deception on the part of employees or potential employees during the hiring process. Furthermore, several employees in these cases displayed disruptive behavior prior to termination; awareness of the patterns in insider IT sabotage cases could have alerted the organization to a potential attack.

PRACTICE 5: *Anticipate and manage negative workplace issues.* Various negative workplace issues were apparent in these cases, including performance problems, lay-offs, and compensation issues. Managers need to carefully handle these types of issues so that they do not escalate out of control. Finally, contentious employee terminations must be handled with utmost care, as most insider IT sabotage attacks occur following termination.

PRACTICE 7: *Implement strict password and account management policies and practices.* Seven cases in this sample involved the unauthorized use of some form of compromised account. Two cases actually involved the use of privileged backdoor accounts in their attack. Organizations should consider procedures to audit account creations to detect the creation of backdoor accounts. Organizations should also consider tight controls over credentials used for privileged administration, service accounts, and infrequently performed functions such as DNS registration. A periodic review and periodic password changes can help enforce least privilege on these types of accounts and limit the chance of an event such as redirection of an external DNS registration as carried out in two case examples described in this article. Organizations should also carefully review group privileges and periodically review group members. The scope of privileged groups, such as domain administrators and groups responsible for account creation, should be reviewed to ensure that individuals cannot escalate their own privileges.

PRACTICE 8: *Enforce separation of duties and least privilege.* A primary point of failure in several of these cases lied in the fact that the insider was in a highly-technical role and had unrestricted root administrator access to the entire network. Implementing both technical and non-technical controls over the use of privileged accounts can limit the amount of damage an insider can do without collusion. In fact, only one of the insiders in this sample required the willing cooperation of another individual to carry out their illicit action. Several access control models support delegating varying degrees of control over systems and can be used to support least privilege practices.

PRACTICE 10: *Use extra caution with system administrators and technical or privileged users.* The insiders described in our case examples were referred to as some of the most technical people in the organization by fellow employees and their managers. To put the importance of this practice into context, 80 percent of our insiders in this sample were in technical job roles, such as a system or database administrator. These individuals are particularly dangerous, as they have detailed knowledge of security controls, network architecture, and weaknesses in the technical environment that they could potentially exploit. As already noted, enforcing separation of duties and least privilege can limit damage done by technical attacks, and is especially important for defending against insider action from your most technically skilled users.

PRACTICE 11: *Implement system change controls.* Two insiders in this article made changes that could have been detected via change controls: planting of malicious code and modification of critical data in a database. Many insider attacks rely on malicious modification to systems and data that are within the insider's reach. There are strong incentives for organizations to use reasonable change control standards to prevent, or at least detect, unauthorized changes. Toolsets exist that can provide everything from file hash comparison to detect unauthorized data modification to measures that enforce separation of duties by blocking certain types of database changes without the approval of a second authenticated and consenting administrator.

PRACTICE 12: *Log, monitor, and audit employee online actions.* Some cases in our sample involved advanced preparation for an attack prior to the insider's separation from the organization, while others showed significant precursors that would have identified the insider as a significant threat long before the attack took place. Continued monitoring of privileged functions, access to sensitive data, and use of network resources can help identify patterns of usage that might be categorized as threatening or suspicious. Consider logging and monitoring as an early warning system for unauthorized access and attack preparation.

PRACTICE 14: *Deactivate computer access following termination.* Another recurring theme in our case examples included the insider's use of access that was not disabled upon termination of employment to carry out their attack. In fact, we know that four of the insiders in our sample struck remotely, after being separated from the organization. Having a standardized plan whereby an employee's computer accounts, building access, and remote VPN access can quickly be inventoried and deactivated upon separation can eliminate a potential retaliatory act Further, if there is a concern that the employee may have attempted to establish unknown access paths, effort should be put forth to identify and close these paths as well.

About the Insider Threat Team

The Insider Threat team is part of the Threat and Incident Management (TAIM) team in CERT. The TAIM team helps organizations improve their security posture and incident response capability by researching technical threat areas; developing information security assessment methods and techniques; and providing information, solutions, and training for preventing, detecting, and responding to illicit activity. TAIM team members are domain experts in insider threat and incident response, and team capabilities include threat analysis and modeling; development of security metrics and assessment methodologies; and creation and delivery of training, courses, and workshops. Our insider threat database management system allows us to examine broad and specific trends.

For additional information regarding the content of this article or other research conducted at The Insider Threat Center at CERT, please contact Dawn Cappelli (dmc@cert.org).