Software Engineering Institute
Carnegie Mellon University

Common Sense Guide to Mitigating Insider Threats, Fifth Edition

The CERT Insider Threat Center

December 2016

TECHNICAL NOTE
CMU/SEI-2015-TR-010

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense 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.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0003388

Table of Contents

List of Figures

List of Tables

Acknowledgments

The effort to produce the fifth edition of the CERT Common Sense Guide to Mitigating Insider Threats was led by Matthew Collins and includes contributions from Michael Theis, Randall Trzeciak, Jeremy Strozer, Jason Clark, Daniel Costa, Tracy Cassidy, Michael Albrethsen, and Andrew Moore. Due to the high number of contributors, we have chosen to make this, and future versions of the Common Sense Guide, authored by the CERT Insider Threat Center. The authors would like to thank Richard Bavis and past graduate students at the CERT Insider Threat Center for their work reviewing cases, generating updated statistics, and providing input on topics throughout the report. We would also like to thank Claire Dixon, our colleague and technical editor at the SEI who reviewed and improved this work.

We would like to thank the authors of past editions of the *Common Sense Guide to Mitigating Insider Threats* including Dawn Cappelli, George Silowash, Lori Flynn, and Tim Shimeall. In addition to the work done by the CERT Insider Threat Center, this guide is much improved from the work, research, and input from countless organizations and individuals who have worked with us to address the challenge of insider threats. We are grateful for your support and input in our work.

Executive Summary

This fifth edition of the *Common Sense Guide to Mitigating Insider Threats* provides the CERT Insider Threat Center's most current recommendations from the CERT® Division, part of Carnegie Mellon University's Software Engineering Institute. These recommendations are based on our continued research and analysis of an expanded corpus of over 1,000 cases of insider threat. The problem of insider threat impacts organizations across all industries. Although the attack methods vary depending on the industry, the primary types of attacks we have identified—theft of intellectual property, sabotage, fraud, and espionage—continue to hold true. This edition of the *Common Sense Guide* also considers unintentional insider incidents.

The definition of a malicious insider remains unchanged from the fourth edition and is defined as a current or former employee, contractor, or business partner who meets the following criteria:

- has or had authorized access to an organization's network, system, or data
- has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

In addition to intentional insider threats, a recent focus for our team has been the unintentional insider threat. We define unintentional insider threats as a current or former employee, contractor, or other business partner who:

- has or had authorized access to an organization's network, system, or data and
- had no malicious intent associated with his or her action (or inaction) that caused harm or substantially increased the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

In our work with public and private industry, we continue to see that insider threats are influenced by a combination of technical, behavioral, and organizational issues. To address these threats, we recommend that an organization consider policies, procedures, and technologies to mitigate insider threats in all areas of the organization. This guide has recommendations and information relevant to an organization's staff in the following areas:

- Management
- Human Resources
- Legal Counsel
- Physical Security
- Information Technology
- Information Assurance
- Data Owners
- Software Engineers

® CERT is a registered mark owned by Carnegie Mellon University.

The recommendations in this guide are designed for decision makers to work together to effectively prevent, detect, and respond to insider threats.

The CERT Insider Threat Center's previously identified patterns of insider threat behavior—intellectual property (IP) theft, IT sabotage, fraud, and espionage—have continued to appear as the primary forms of malicious insider threats. New research, however, has lead us to understand the patterns related to unintentional insider threats. These threats represent a significant risk for organizations and potential attack vectors for malicious insiders and external adversaries. In addition to unintentional insider threats, the formal definition of an insider threat may soon expand to include workplace violence as a physical form of a malicious insider. While the CERT Insider Threat Center recognizes this as an important area for potential future work, our current corpus of cases does not include a focus on workplace violence or physical threats. Though the CERT Insider Threat Center believes that many indicators will be shared between physical and technical malicious insiders, physical insider attacks require a focused study to determine unique indicators and patterns of such an attack.

This edition of the guide describes 20 practices that organizations should implement across the enterprise to prevent and detect insider threats. Each practice includes challenges to implementation, quick wins and high-impact solutions for small and large organizations, and information on relevant security standards. This edition retains the fourth edition's emphasis on six groups within an organization—Human Resources, Legal, Physical Security, Data Owners, Information Technology, and Software Engineering—and provides quick reference tables noting to which of these groups each practice applies. The updated appendices provide a revised list of information security best practices, the CERT Insider Threat Center's view on employee privacy, a mapping of the guide's practices to established security standards, a breakdown of the practices by organizational group, and checklists of activities for each practice. All of the case studies and data in this version have been updated with our latest numbers and information from our insider threat corpus.

The insider threat program is the state of the art in insider threat prevention, detection, and response. The CERT Insider Threat Center has seen success with this approach in both public and private organizations and we have incorporated recent findings into the best practice of "Developing an Insider Threat Program." Though more technology and tools will be produced to target insider threats, the organization must have some structure that supports the running and analysis of these tools, as well as correlation with data sources that are not yet automated within the organization. To aid those running an insider threat program, we have re-organized the best practices to better the process of establishing a program.

Table 1: The Best Practices of the CERT Common Sense Guide

CSG V5 Order	Best Practice	CSG V4 Number
1	Know and protect your critical assets.	6
2	Develop a formalized insider threat program.	16
3	Clearly document and consistently enforce policies and controls.	2
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	4
5	Anticipate and manage negative issues in the work environment.	5
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.	1
7	Be especially vigilant regarding social media.	18
8	Structure management and tasks to minimize unintentional insider stress and mistakes.	---
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	3
10	Implement strict password and account management policies and practices.	7
11	Institute stringent access controls and monitoring policies on privileged users.	10
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.	12
13	Monitor and control remote access from all end points, including mobile devices.	13
14	Establish a baseline of normal behavior for both networks and employees.	17
15	Enforce separation of duties and least privilege.	8
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.	9
17	Institutionalize system change controls.	11
18	Implement secure backup and recovery processes.	15
19	Close the doors to unauthorized data exfiltration.	19
20	Develop a comprehensive employee termination procedure.	14

Abstract

This fifth edition of the *Common Sense Guide to Mitigating Insider Threats* provides the most current recommendations of the CERT® Division (part of Carnegie Mellon University's Software Engineering Institute), based on an expanded corpus of more than 1,000 insider threat cases and continued research and analysis. It introduces the topic of insider threats, explains its intended audience and how this guide differs from previous editions, defines insider threats, and outlines current patterns and trends. The guide then describes 20 practices that organizations should implement across the enterprise to prevent and detect insider threats, as well as case studies of organizations that failed to do so. Each practice includes features new to this edition: challenges to implementation, quick wins and high-impact solutions for small and large organizations, and relevant security standards. This edition also focuses on six groups within an organization—Human Resources, Legal, Physical Security, Data Owners, Information Technology, and Software Engineering—and maps the relevant groups to each practice. The appendices provide a revised list of information security best practices, a new mapping of the guide's practices to established security standards, a new breakdown of the practices by organizational group, a new look at considerations for employee privacy, and new checklists of activities for each practice.

New Content in the Fifth Edition

The fifth edition of the Common Sense Guide reflects the movement toward insider threat programs. The best practices are reordered to better align with the development of an insider threat program. Significant updates have been made to the best practices “Know and protect your critical assets,” ”Building an insider threat program,” “Deploy solutions for monitoring employee actions and correlating information from multiple data sources,” and “Establish a baseline of normal behavior for both networks and employees.”

The revisions to the first two practices will help managers of insider threat programs to identify their most important assets and to develop a plan to build an insider threat program. The best practice “Building an insider threat program” now includes information on governance of an insider threat program.

The revisions of practices focused on data analysis provide insider threat programs with potential data sources and methods of analysis. These practices reflect our recent experience with monitoring and analysis capabilities in operational environments.

A new best practice, “Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees,” emphasizes the importance of user training for detecting intentional insider threats and preventing unintentional insider incidents. Our recent work has highlighted the potential impact of unintentional insider threats including phishing and accidental data loss.

This update contains all new case study examples for each best practice, updated data containing our latest statistics, updated mappings to include the NITTF minimum standards, and an appendix on Insider Threat Privacy.

How to Use the Common Sense Guide

The fifth edition of the Common Sense Guide has been re-organized to better provide insider threat program managers with a roadmap for building an insider threat program. Readers of this guide should have a general understanding of the issues of insider threats, the solutions that are proposed in this guide, and their responsibility to the insider threat program and overall insider threat awareness.

Executives & Decision Makers

Executives can use this guide to gain familiarity with the requirements and the scope of an insider threat program. The guide can help with understanding the importance of an insider threat program and the potential impact to the organization of not having one. Additionally, executives should pay close attention to the specific policies and procedures that are essential to the success of the program. These can most easily be found in "Appendix E: Checklists of Quick Wins and High-Impact Solutions."

Insider Threat Program Managers

Managers can use this guide learn the best practices and how best to engage them for insider threat prevention, detection, and response. Additionally, this guide can be used to effectively communicate to their organization's decision makers the importance of creating a program and in influencing them in building the program and implementing the necessary policies and procedures. Program building can be achieved by studying the provided case studies and their impacts to the organizations involved. Furthermore, managers can take the proposed solutions and apply them to their programs. With the re-organization of the guide, new insider threat program managers can use the guide sequentially to start building their programs.

Security Practitioners

Practitioners can use this guide to understand the best practices for an insider threat program and the requirements those practices bring to the program. It is the practitioners' responsibility to ensure that they and other members of the program are following and fully implementing the best practices. Additionally, by having this improved understanding, practitioners will be able to both assist their managers in improving the program and recognize if something is missing.

Introduction

What is an Insider Threat?

The CERT Division's definition of a malicious insider is a current or former employee, contractor, or business partner who meets the following criteria:

- has or had authorized access to an organization's network, system, or data
- has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, availability, or physical well-being of the organization's information or information systems or workforce.

For the purpose of this guide, an unintentional insider threat is defined as a current or former employee, contractor, or other business partner who meets the following criteria:

- who has or had authorized access to an organization's network, system, or data and who, through
- their action/inaction without malicious intent
- cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

This guide does not include cases of espionage involving classified national security information nor does it include the physical manifestation of insider threats, such as workplace violence.

While traditional insider threats are current or former employees, the CERT Insider Threat Center also recognizes the following actors and influences in many of our case studies:

- **Collusion with outsiders:** Many insiders who stole or modified information were actually recruited by outsiders, including organized crime and foreign organizations or governments. The CERT Division has analyzed characteristics of employees who may be more susceptible to recruitment.
- **Business partners:** The CERT Insider Threat Center has noted an increase in the number of insider crimes perpetrated by employees of trusted business partners who have been given authorized access to their clients' networks, systems, and data.
- **Mergers and acquisitions:** There is a heightened risk of insider threat in organizations being acquired by another organization. Organizations should recognize the increased risk of insider threat both within the acquiring organization and in the organization being acquired, as employees endure stress and an uncertain organizational climate. Readers involved in an acquisition should pay particular attention to the practices in this guide.
- **Cultural differences:** This guide reflects many of the behavioral patterns observed in the CERT Division's insider threat modeling. However, cultural issues could influence employee behaviors; people who were raised outside of the United States or spent extensive time abroad might not exhibit those same behavioral patterns in the same manner.
- **Issues outside the United States:** Until this year, the CERT Division's insider threat research was based only on cases that occurred inside the United States. The CERT Division

has begun to gather insider threat data from outside the United States; however, this guide does not include that data or its analysis. It is important for U.S. companies operating branches outside the country to understand, in addition to the influence of cultural differences on employee behavior, that portions of this guide will need to be tailored to legal and policy differences in other countries.

Are Insiders Really a Threat?

The threat of attack from insiders is real and substantial. The *2015 U.S. State of Cybercrime Survey*, sponsored by the CERT Insider Threat Center, United States Secret Service, CSO Magazine, and PWC, found 23% of electronic crime events were suspected or known to be caused by insiders. The survey also revealed that 45% of the respondents thought that damage caused by insider attacks was more severe than damage from outsider attacks. According to the survey, the most common insider incidents were customer records compromised or stolen, confidential records (trade secrets or intellectual property) compromised or stolen, and private or sensitive information was unintentionally exposed [PWC 2015].

The definition of insider threat is trending towards the inclusion of physical threats to departmental resources, including to personnel. Due to the CERT Insider Threat Center's limited experience and research on this topic, we are not making formal recommendations regarding issues of workplace violence by insiders. We do recommend that organizations take this threat into consideration and work to produce an approach to physical security that addresses both the technical and physical threat. Workplace violence has become more prevalent in recent years and is often perpetrated by insiders. The CERT Insider Threat Center plans to research the physical aspect of insider threat with the possibility of incorporating this information into its next revision of *The Common Sense Guide*.

Since 2001, the CERT Insider Threat Center has conducted a variety of research projects on insider threat. One of our conclusions is that insider attacks have occurred across all organizational sectors, often causing significant damage to the affected organizations. Examples of these acts include the following:

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

In many of these crimes, damages extend beyond immediate financial losses to negatively impact the organization's reputation and brand.

Insiders have a significant advantage over external attackers. Historically, organizations have focused on external-facing security mechanisms such as firewalls, intrusion detection systems, and electronic building access systems. Insiders, however, are not only aware of their organization's policies, procedures, and technology: they are often also aware of their vulnerabilities, such as loosely enforced policies and procedures or exploitable technical flaws in networks or systems. In some cases, the malicious insider can even be the one who configured the organization's security.

As part of its research into insider threat cases, the CERT Division examined how each victim organization could have prevented the attack or, at the very least, detected it earlier. The research indicates that implementation of widely accepted best practices for information security could have prevented many of the examined insider attacks.

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

Who Should Read This Guide?

This guide serves as a valuable resource to those tasked with building insider threat programs or those who need to meet newly issued standards related to insider threats. Though the guide will provide the most value to managers of insider threat programs, we wrote this guide for a diverse audience. Decision makers across an organization will benefit from reading it because insider threats are influenced by a combination of technical, behavioral, and organizational issues and must be addressed by policies, procedures, and technologies. Staff members of an organization's management, HR, Legal, Physical Security, Data Owners, IT, and Software Engineering groups should all understand the overall scope of the problem and communicate it to all employees in the organization. This guide identifies the organizational groups that have a role in implementing each practice so that readers can quickly access relevant recommendations.

Can Insiders Be Stopped?

The insider threat is ever evolving and changing. We believe by building an effective insider threat program, an organization can significantly reduce its exposure to the problem and prevent the most damaging insider attacks. The program must implement a strategy with the right combination of policies, procedures, and technical controls. Management from all areas of the organization, especially at the executive level, must appreciate the scale of the problem and work together to modify the organization's business policies and processes, culture, and technical environment. The practices in this guide, if followed by the victim organizations, would have prevented or detected the insider attacks in our corpus.

Patterns and Trends Observed by Type of Malicious Insider Activity

The CERT insider threat corpus currently includes more than 1,000 cases of insider threat. Of these, we analyzed 734 that involved malicious insider attacks against organizations. These cases did not include espionage or unintentional damage. The patterns and trends we have observed indicate four classes of malicious insider activity:

- information technology (IT) sabotage—an insider's use of IT to direct specific harm at an organization or an individual
- theft of IP—an insider's use of IT to steal IP from the organization. This category includes industrial espionage involving outsiders.
- fraud—an insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information that leads to an identity crime (e.g., identity theft or credit card fraud)
- miscellaneous—cases in which the insider's activity was not for IP theft, fraud, or IT sabotage

Excluding the 122 miscellaneous cases, Figure 1 shows the number of insider threat cases analyzed for this guide per class and their overlap, where cases fell into more than one class.

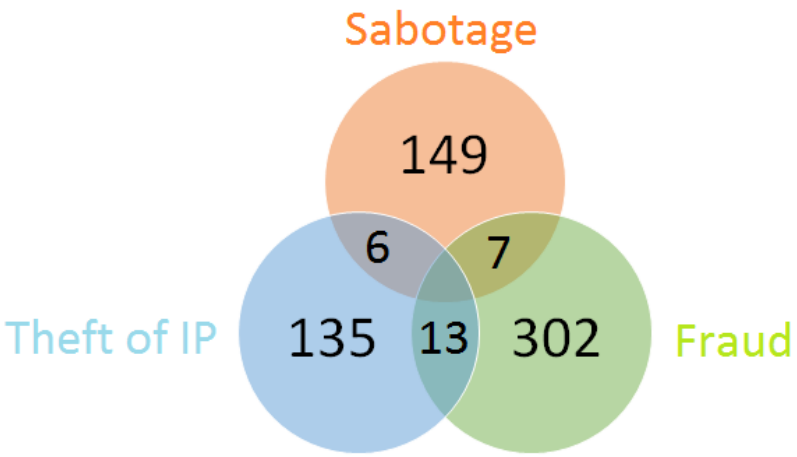

Figure 1: Number of Insider Threat Cases per Class, Excluding Miscellaneous Cases

Figure 2 shows the six infrastructure sectors that most frequently suffer insider fraud, sabotage, and theft of IP.

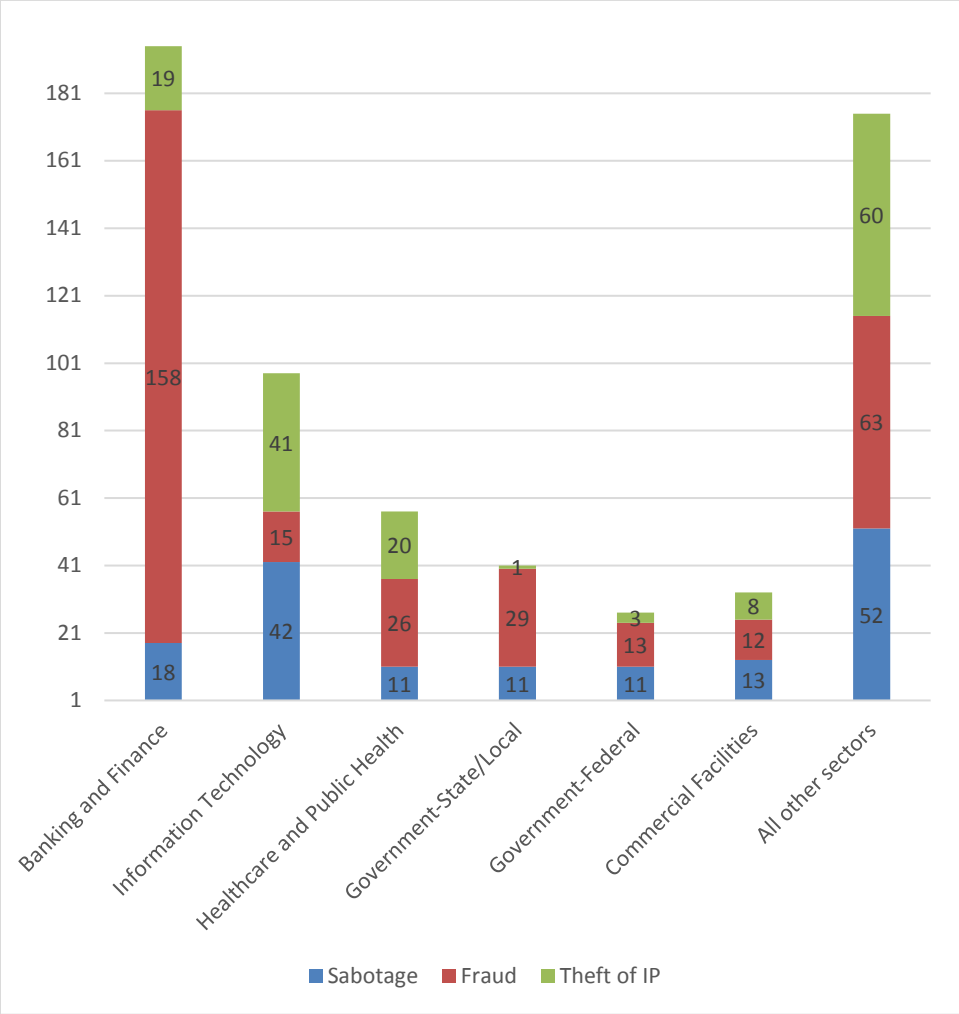

Figure 2: Top Six Infrastructure Sectors for Fraud, Sabotage, and Theft of IP[1]

[1] The chart represents 715 total cases of fraud, sabotage, and theft of IP.

Patterns and Trends Observed by Type of Unintentional Insider Threat

The CERT insider threat database currently contains more than 150 cases of Unintentional Insider Threat (UIT). Due to the type of case, none of these was adjudicated; therefore, guilt was not confirmed.

Our research has led us to categorize UIT cases in four main classes. Three of these four categories had previously been identified and defined by Privacy Rights Clearinghouse to categorize types of data breaches. Though not all data breaches are cases of unintentional insider threats, we found that unintentional insider threats often result in data breaches and that these definitions best described the outcomes of unintentional insider incidents [PRC 2015].

- (DISC) Accidental Disclosure—sensitive information is posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail.
- Phishing/Social—an outsider's electronic entry is acquired through social engineering (e.g. phishing e-mail attack, planted or unauthorized USB drive) to acquire an insider's credentials or to plan malware to gain access.
- (PHYS) Physical Records—lost, discarded, or stolen non-electronic records, such as paper documents.
- (PORT) Portable equipment—lost, discarded, or stolen data storage devices, such as a laptop, smart phone, portable memory device, CD, hard drive, or data tape.

Features of the Common Sense Guide

This fifth edition of the *Common Sense Guide* has the following features to make it even more useful to insider threat prevention, detection, and response within organizations.

- re-organization of best practices to better aid managers of insider threat programs
- group tables—At the beginning of every practice, a table indicating the involved organizational groups makes it easy to identify relevant material.
- "Challenges" section—Each practice lists some of its challenges, allowing organizations to quickly identify areas they may need to address before implementing the practice.
- "Quick Wins and High-Impact Solutions" section—This section presents a basic list of quick wins per practice for jump-starting your organization's insider threat program. Some recommendations specifically address small or large organizations. Size is a subjective measure that each organization should determine for itself. However, for the purposes of this guide, an organization's size depends on its number of employees (some draw the line at 500 [CISCO 2012]), the extent of its network, and the size of its annual receipts. Small organizations may be unable to perform some tasks, such as separation of duties, because they have too few IT workers. Small organizations may also have insufficient cash flow to invest in certain security measures.
- "Mapping to Standards" section—We have mapped other best practices that closely align with those in the *Common Sense Guide*:
  - National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4: *Recommended Security Controls for Federal Information Systems and Organizations* [NIST 2015]
  - CERT® Resilience Management Model (CERT®-RMM) [Caralli, Allen et al. 2010]

- International Organization for Standardization (ISO) 27002 [ISO/IEC 2013]
- The NITTF Guidelines and Minimum Standards

Organizations may find it easier to implement the best practices identified in this guide if they already use one or more of the above best practice frameworks.

Appendix A defines the acronyms used in this guide.

Appendix B lists additional sources for best practices, beyond this guide.

Appendix C maps this guide's best practices to three major cybersecurity standards: NIST controls, CERT-RMM, and ISO 27002.

Appendix D maps the six organizational groups addressed in the guide—HR, Legal, Physical Security, IT, Software Engineering, and Data Owners—to a list of all 19 best practices. It also provides individual lists of the best practices that apply to each organizational group.

Appendix E compiles the "Quick Wins and High-Impact Solutions" checklists from each best practice, for convenient reference.

Appendix F is an Insider Threat Privacy Appendix.

Practice 1: Know and protect your critical assets.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	✓

The most basic function of an insider threat program is to protect the assets that provide your organization with a competitive advantage. According to ISO 55000 an asset is something with potential value to an organization and for which the organization has a responsibility [Riso 2012].

We further elaborate on this definition by stating that a critical asset can be thought of as something of value that which if destroyed, altered, or otherwise degraded would impact the confidentiality, integrity, or availability and have a severe negative affect on the ability for the organization to support essential missions and business functions.

Critical assets can be both physical and logical and can include facilities, systems, equipment, and technology. An often-overlooked aspect of critical assets is intellectual property. This may include proprietary software, customer data for vendors, schematics, and internal manufacturing processes. The organization must keep a close watch on where data is at rest and in transport. Current technology allows more seamless collaboration than ever, but also allows the organization's sensitive information to be easily removed from the organization.

A complete understanding of critical assets (both physical and logical) is invaluable in defending against attackers who will often target the organization's critical assets. The following questions help the organization to identify and prioritize the protection of its critical assets:

1. What critical assets do we have?
2. Do we know the current state of each critical asset?
3. Do we understand the importance of each critical asset and can we explain why it is critical to our organization?
4. Can we prioritize our list of critical assets?
5. Do we have the authority, money, and resources to effectively monitor our critical assets?

The role of the program manager is to work with all of those across all areas of the organization to answer the questions above. Once those questions are answered within each division, input from senior level management should be obtained to prioritize protection across the organization.

Once critical assets are identified and prioritized, the organization must identify those high-risk users who most often interact with the critical systems or data. This will help the organization to identify the best approaches to successfully identify potential insider threats.

1.1 Protective Measure - Conducting a Risk Assessment

One of the best ways for an organization to know its assets and protect them from attack, including from insiders, is to conduct a risk assessment. A risk assessment will teach an

organization about the types of data its systems process, who uses the data, and where it is stored. According to NIST, the risk assessment framework includes six steps [NIST 2012]:

1. *Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.*
2. *Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions.*
3. *Implement the security controls and document how the controls are deployed within the information system and environment of operation.*
4. *Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*
5. *Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.*
6. *Monitor and assess selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials.*

Each of these steps requires the organization to understand its assets. Key questions that an organization must answer before it can move forward with a protection strategy include the following:

1. What types of data are processed (medical information, personally identifiable information, credit card numbers, inventory records, etc.)?
2. What types of devices process this data (servers, workstations, mobile devices, etc.)?
3. Where is the data stored, processed, and transmitted (single location, geographically dispersed, foreign countries, etc.)?

Answering these questions will help an organization to inventory the data and systems that must be protected from various attacks. NIST Special Publication 800-61 Volume 2[2] identifies data types that may exist in an organization and the protection levels they should be afforded.

Federal Information Processing Standards (FIPS) Publication 199 (FIPS PUB 199) provides guidance on categorizing information and information systems based on their security objectives (confidentiality, integrity, and availability) and the potential impact of events jeopardizing them (low, moderate, or high).[3]

---

[2] NIST Special Publication 800-60 is available at http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf.

[3] FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, is available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

1.2 Protective Measure - Asset Tracking

A reliable method of both identifying and tracking the organization's critical assets is essential to keeping the insider threat effort tied to the organization's need. This list of critical assets should be regularly updated, as it serves as a guide and provides a focus for the organization's insider threat program. Continuously updating the list of critical assets may require both manual and automatic processes to be put in place. The two methods for creating a complete inventory are service based and hardware based.

To perform a **service-based inventory**, organizations have a service catalog, rather than a conventional inventory, that contains the information services an organization needs to fulfill its mission. For example, an online store may define its web page as a critical service; a communications company may identify email as a critical service. A service-based inventory establishes a hierarchy of assets, starting with a top-level service, branching into the information assets that support it, branching again into the assets that support them, and so on. The organization then inventories the bottom-level assets. For instance, if email is the critical service, then hardware and software are its supporting assets. They, in turn, are supported by the email server, the antivirus appliance, the antivirus program, and the email application, which are the assets the organization should identify and inventory.

For a **hardware-based inventory**, a basic walkthrough of a data center is an effective method of collecting hardware information for an inventory. However, hardware itemization does not constitute a complete inventory. Organizations need to work closely with system administrators to become fully aware of the logical assets contained within each piece of hardware. Data center system administrators must be able to provide the following information:

- a list of all supported servers, with designation of type (Windows, Linux, virtual machine systems, etc.), platform (Oracle, Java, etc.) and environment (production, integration, model, or development)
- for each server, a list of what is running on the server (e.g., client-server application, web application, or database) and the IT support contact for each of these items
- for each virtual system instance, a list of what is running within the platform and the owner or contact for each of these items

With this information, the organization should produce a hardware asset hierarchy similar to the software asset inventory, starting with the top-level hardware asset and branching successively into supporting assets. The organization should identify and inventory the topmost and bottom-most assets.

In addition to an asset inventory, another approach to identifying critical assets involves monitoring the network traffic of your systems. This monitoring will reveal the most frequently used services and parts of the network. From analysis of this data, one might infer the most critical hardware, pages of the organization's website, file servers, file downloads, and other frequently used assets.

Once the organization has identified its information assets using one of the above methods, it should ask the IT department to add any unidentified assets and their business owners' contact information, ask those business owners to confirm the added assets, and condense all the

inventory information into a spreadsheet. With the inventory complete, the organization should assign each asset a set of attributes, which will help determine the asset's priority. Organizations can define any attributes they need but should consider at least the following:

- environment (production, integration, model, or development)
- security categorization (confidentiality, integrity, and availability[4])
- criticality (high, medium, low, or not applicable)

1.3 Metrics

One of the major difficulties facing organizations is being able to rank and score accurately the different critical assets provided to the decision makers. Our experience shows us that many stakeholders within an organization will often state "*the asset they know about and control*" is in their opinion the most critical. Instead of providing subjective and biased ranking of critical assets, we suggest using various metrics and discussing them internally with various employees of the organization. The table below is not meant to be exhaustive but instead gives a sense of the types of metrics that might be considered.

Table 2: Metrics to Consider in Ranking Critical Assets [Wikoff 2015]

Metric	Explanation
Time to restore	How long in terms of time (months, weeks, hours) will it take to "restore" the critical asset should it become unavailable?
Loss if it fails	What is the loss either monetary or perhaps even loss of life if the critical asset were to fail?
Mission and customer impact	What would be the impact to the organization's mission and its customer base if the critical asset were unavailable or otherwise not working correctly?
Probability of failure	What is the percentage probability of the critical asset failing?
Popularity of the critical asset (data)	How often is the critical asset downloaded, searched for, and viewed?

When attempting to rank and score the potential pool of critical assets, we suggest leveraging a statistical tool known as Pairwise Rankings. This approach will essentially allow a group to perform the ranking by comparing two critical assets at a time and giving each a numerical rating. The numerical ratings are then added up and sorted in ascending order to show the most critical asset. For more information on ranking critical assets, the reader is urged to visit http://www.thesecurityminute.com/ranking-critical-assets

1.4 Challenges to Asset Identification

1. Receiving the appropriate buy-in from leadership necessary to spend the time, money, and energy required to accurately understand and prioritize the organizations critical assets.
2. Determining and utilizing the appropriate metrics to determine what in fact a critical asset is. Simply asking all of the stakeholders to report back on their critical assets likely will lead to over-reporting.

[4] FIPS PUB 199 provides attribute values for criticality, integrity, and availability.

3. Understanding and containing the scope of your critical assets, especially if the organization utilizes the cloud, remote sites, and virtual systems.
4. Finding time and funding to do a complete inventory—inventorying or cataloging assets takes worker time and thus funding. Considering the importance of this work and the risks, financial and otherwise, if the work is not complete could help justify the necessary funding and worker hours.
5. Maintaining inventory lists as changes occur—as changes occur, it is vital that the lists continue to be correct. This requires the importance of this work to be prioritized and emphasized over time.
6. Once the list of critical assets is known, the challenge becomes accurately prioritizing the critical assets based on the appropriate metrics.

1.5 Case Studies

A hospital facility employed the insider, a contractor, as a security guard. The insider was extensively involved with the Internet underground and was the leader of a hacking group. The insider worked for the victim organization only at night and was unsupervised. The majority of the insider's unauthorized activities involved a heating, ventilation, and air conditioning (HVAC) computer. This HVAC computer was located in a locked room, but the insider used his security key to obtain physical access to the computer. The insider remotely accessed the HVAC computer five times over a two-day period. In addition, the insider accessed a nurses' station computer, which was connected to all of the victim organization's computers, stored medical records, and patient billing information. The insider used various methods to attack the organization, including password-cracking programs and a botnet. The insider's malicious activities caused the HVAC system to become unstable, which eventually led to a one-hour outage. The insider and elements of the Internet underground were planning to use the organization's computer systems to conduct a distributed-denial-of-service (DDoS) attack against an unknown target. A security researcher discovered the insider's online activities. The insider was convicted, ordered to pay $31,000 restitution, and sentenced to nine years and two months of imprisonment followed by three years of supervised release.

This case illustrates how a single computer system can cause a great amount of damage to an organization. In this case, the damage could have been life threatening because the attack took place at a hospital facility. Modifying the HVAC system controls and altering the organization's environment could have affected temperature-sensitive drugs and supplies and patients who were susceptible to temperature changes. With additional steps to bypass security, the insider could have potentially modified and impaired patient records, affecting treatment, diagnoses, and care. It is critical that management and information security teams work with other departments within an organization to identify critical systems. In this case, the HVAC computer was located in a locked room, not a data center or server room, which would have afforded the system additional protections and may have prevented the insider from manipulating the system.

In addition, the insider was able to access a nurses' station computer, which had access to other critical organizational systems. If the organization had fully understood the potential impact a compromised workstation could have on other parts of the organization, it could have implemented additional layers of protection that would have prevented this type of attack.

1.6 Quick Wins and High-Impact Solutions

1.6.1 All Organizations

- ☐ Conduct a physical asset inventory. Identify asset owners' assets and functions and identify the type of data on the system.
- ☐ Understand what data your organization processes by speaking with data owners and users from across your organization.
- ☐ Identify and document the software configurations of all assets.
- ☐ Prioritize assets and data to determine the high-value targets.

1.7 Mapping to Standards

- NIST: CP -2 (8) Contingency Plan | Identify Critical Assets, CM-2 (Baseline Configuration), CM-8 (Information System Component Inventory), PM-5 (Information System Inventory), PM-8 Critical Infrastructure Plan, RA-2 (Security Categorization)
- NITTF: B-2
- Minimum Standards: G-1-b, G-1-c
- CERT-RMM:
  - Asset Definition and Management
  - Enterprise Focus
- ISO 27002:
  - 7.1.1 Inventory of assets

Practice 2: Develop a formalized insider threat program.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	✓

The formalized insider threat program provides an organization with a designated resource to address the problem of insider threat. The trust that organizations place in their workforce can leave them vulnerable to malicious insiders, who often use particular methods to hide their illicit activities. Only by taking commensurately specialized action can organizations effectively detect, prevent, and respond to the unique threat from insiders. The best time to develop a process for mitigating malicious insider incidents and the unintentional insider threat is before they occur, not as one is unfolding. When an incident does occur, the process can be modified as appropriate based on postmortem results from prior incidents.

2.1 Protective Measures

Increasingly, organizations, including the federal government, are recognizing the need to counter insider threats and are doing it through specially focused teams. In January 2011, the federal Office of Management and Budget (OMB) released memorandum M-11-08, Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems [Lew 2011]. It announced the evaluation of the insider threat safeguards of government agencies. This action by the federal government highlights the pervasive and continuous threat to government and private industry from insiders, as well as the need for programs that mitigate this threat. In October 2011, President Obama signed Executive Order (E.O.) 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information [Obama 2011]. It requires all federal agencies that have access to classified information and systems to have a formal insider threat program. In addition, the National Industrial Security Program Operating Manual is expected to require defense contractors to establish and maintain an insider threat program with many of the requirements of E.O. 13587.

An insider threat program is an organization-wide program with an established vision and defined roles and responsibilities for those involved. All individuals participating in the program must receive specialized awareness training. The program must have criteria and thresholds for conducting inquiries, referring to investigators, and requesting prosecution. Inquiries must be controlled by a process to ensure privacy and confidentiality because the team will be a trusted group for monitoring and resolution. Most importantly, the program must have management's support to be successful.

The CERT Insider Threat Center, along with other organizations such as the Intelligence National Security Alliance, has documented the most common components found in insider threat

programs within the government as well as non-government organizations [INSA 2013]. This practice recommends that a program include, as a minimum, the following components:

- Formalized and Defined Program: Directives, authorities, mission statement, leadership intent, governance, budget.
- Organization-wide Participation: Active participation from all components that eases data access, sharing, and provides visible senior leader support for the program, especially when data necessary to an insider threat program is in silos (HR, Security, IA, CI, LE, IG, Finance, etc.).
- Oversight of Program Compliance and Effectiveness: Governance structure, such as an Insider Threat Program Working Group/Change Control Board that helps the program manager produce standards and operating procedures for the insider threat program and recommends changes to existing practices and procedures. Also, an Executive Council/Steering Group that approves changes recommended by the working group/change control board. Oversight includes annual self-assessments, as well as third-party assessments of the compliance and effectiveness of the program.
- Confidential Reporting Mechanisms and Procedures: Not only enable reporting of suspicious activity, but when closely coordinated with the insider threat program (InTP), these ensure that legitimate whistleblowers are not inhibited or inappropriately monitored by an insider threat program.
- Insider Threat Incident Response Plan: More than just a referral process to outside investigators. These plans detail how alerts and anomalies will be identified, managed, escalated. This includes timelines for every action and formal disposition procedures.
- Communication of Insider Threat Events: Appropriate sharing of event information with the correct components, while maintaining confidentiality and protecting privacy until allegations are fully substantiated. Includes communication of insider threat trends, patterns, and probable future events so that policies, procedures, training, etc., can be modified as required.
- Protection of Employees' Civil Liberties and Rights: Legal Counsel review at all stages of program development, implementation, and operation.
- Policies, Procedures, and Practices that support the InTP: Formal documents that detail all aspects of the program (including mission, scope of threats, directives, instructions, standard operating procedures).
- Data Collection and Analysis Techniques and Practices: The UAM data collection and analysis portion of a program. Requires detailed documentation for all aspects of data collection, processing, storage, and sharing to ensure compliance with privacy and civil liberties.
- Insider Threat Training and Awareness: Provides training for three aspects of the program (see Section 5.2.2.3). Insider threat awareness training for all organization personnel; Training for InTP personnel; Role-based training for mission specialists who are likely to observe certain aspects of insider threat events (e.g. HR, IA, CI, LE, Behavioral Sciences, IG, Finance).
- Prevention, Detection, and Response Infrastructure: Network defenses, host defenses, physical defenses, tools and processes, and other components.

- Insider Threat Practices Related to Trusted Business Partners: Agreements, contracts, and processes reviewed for insider threat prevention, detection, and response capabilities.
- Insider Threat Integration with Enterprise Risk Management: Ensure all aspects of risk management include insider threat considerations (not just outside attackers) and possibly a standalone component for insider threat risk management.

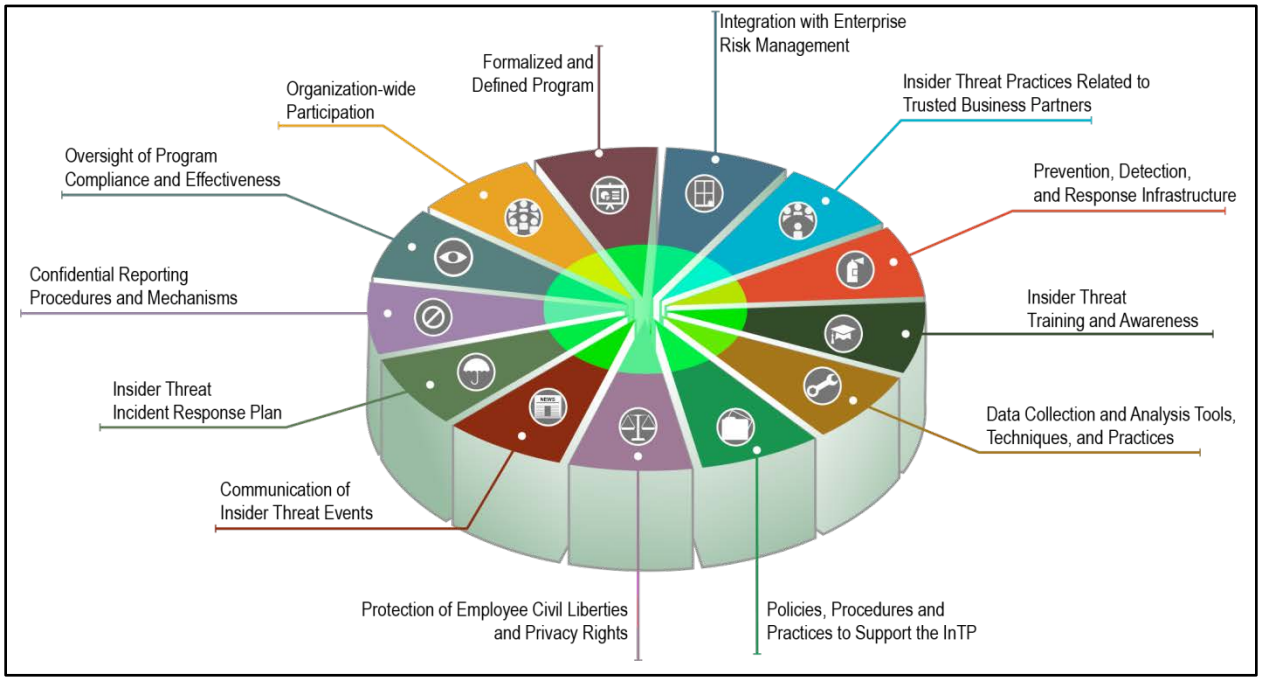

Figure 3: *Components Common to Insider Threat Programs*

A well-grounded insider threat program will have policies and procedures encompassing Human Resources, Legal, Security,[5] Data Owners, Information Technology, Software Engineering, and Contracting. The organization needs to have an established incident response plan that addresses incidents perpetrated by insiders, has an escalation chain, and delineates authorities for deciding disposition.

Organizations should implement best practices (noted in brackets) regarding

- identification of critical assets including IP and sensitive or classified data [1]
- access control to identified data and assets [19, 10]
- monitoring of access to critical data and assets [17, 12, 19]
- monitoring of employees with privileged access [11]
- specialized monitoring (30-day rule, outside normal hours, to external sites, etc.) [17, 4]
- separation of duties [14]
- quality assurance [software engineering best practices]

[5] Physical Security and Personnel Security are referred to as *Security* in this best practice. These two teams may be separate entities in an organization but often share the same chain of command.

Documents specifying these particular best practices should require the use of technical mechanisms that ensure proper monitoring, alerting, and reporting.

Insider threat programs help organizations detect, prevent, and respond to an insider incident. A formalized insider threat team encompasses members of different teams from across the enterprise and does not need to be a separate, dedicated entity. People from across the organization can fill many of the team's roles as needed. However, it is important to identify these individuals and roles before an insider incident occurs. To be prepared to handle such events in a consistent, timely, and professional manner, an insider threat program needs to understand

- whom to involve
- who has authority
- whom to coordinate with
- whom to report to
- what actions to take
- what improvements to make

An insider threat team is similar to a standard incident response team in some ways; both teams handle incidents, however the insider threat team responds to the incidents that are suspected to involve insiders. However, the information handled by the insider threat team may be sensitive, requiring individuals to handle cases with the utmost discretion and due diligence particularly because the team members and the insiders work for the same company, and disclosure could wrongfully harm someone's career and private life. Ensuring privacy and confidentiality will protect accused insiders who are actually innocent, as well as the integrity of the inquiry process itself.

Individuals from teams across the organization need to work together to share information and mitigate threats. Organizations should consider involving the following teams and personnel, who can provide their perspectives on potential threats, as part of the prevention, detection, and response aspects of an insider threat program:

This practice contains some guidance specific to federal agencies as well as non-governmental organizations. For example, Table 3 lists position titles for both types of organizations.

Table 3: Titles for Insider Threat Program Positions

Business Components	Subject Matter Experts
C-level managers	Data Architect (or functionality)
Security (physical, personnel, and information)	System Network Architect
Cybersecurity (if not included in security)	Information Assurance Specialists
Human Resources (HR/Human Capital (HC)	Senior Technologist
Information technology (CIO, CTO)	HR/HC Specialists
Legal	Financial Specialists
Privacy	Legal Specialists
Civil Liberties (if not included with Legal or Privacy)	Investigation Specialists
Ethics and compliance	Counterintelligence Specialists (if organic)
Acquisition/Contracting/Purchasing	Law Enforcement Specialists or liaison
Law enforcement or investigations group (if organic and not included in another group)	Behavioral Sciences Specialists
Critical lines of business (products, services, data owners, trusted business partners as appropriate)	Records Management Specialists

Each of these teams plays a key role in the insider threat program because each has access to information or a perspective that others in the organization typically do not share. For example, Human Resources has sensitive information regarding an employee's performance that the insider threat team may need in order to effectively detect malicious insider activity. As the team's size grows, the value additional members add to the team must be balanced by the increased risk of disclosure of personal information or that an inquiry is being conducted. One way to balance information-sharing and privacy is to ask all the groups above to contribute their threat detection data and ideas, but have only a small, core insider threat team receive and analyze that information.

A significant consideration for any organization is how the insider threat program will be aligned within the organization. The CERT Insider Threat Center has seen varied models employed by government and non-government organizations. Some of the models we observed include examples such as having the insider threat program report to:

- CIO
- CISO
- HR
- Security (usually physical security)
- CFO
- Director of Administration (or COO)
- Chief Legal Counsel
- Ethics (or investigations unit)

Based on empirical observations from the various models we suggest that the insider threat program encounters the least complications and is most effective when it is directly aligned to the head of the organization. Directly reporting to the president/CEO/director/secretary or their principal deputy, such as the chief of staff/COO ensures the organization understands the commitment of senior leadership, provides for full cooperation of the rest of the C-level staff and their organizations, and ensures unfettered access to necessary data sources and subject matter expertise within the organization. Many organizations that originally aligned their insider threat program within intelligence, counterintelligence, investigations, or law enforcement discovered significant complications with regulatory compliance requirements that hindered the effectiveness of the program. In a similar fashion, those programs that were aligned with HR/HC, IT, Security, etc., discovered that the programs sometimes became too focused on the specific knowledge and skillsets of that organizational element. For example, alignment with HR/HC created a program predominately focused on the management of people, while a program aligned with IT was predominately focused on IT tools and data. Therefore, some organizations eventually realigned their programs to the senior executive or principal deputy to alleviate these types of issues.

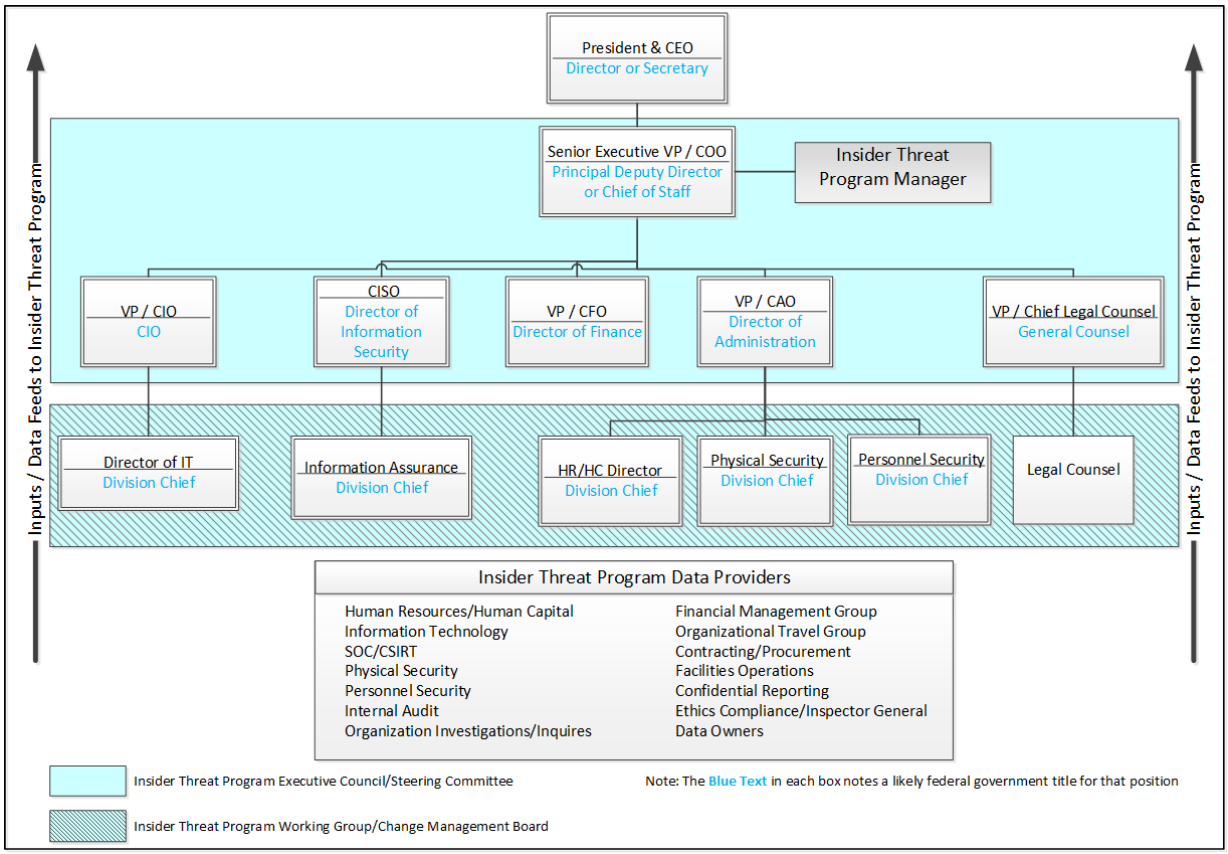

Figure 4: Example Insider Threat Program Organizational Structure and Data Providers

Figure 4 shows the notional alignment of the insider threat program, a governance structure, and illustrates the need for each team in the organization to provide input to the insider threat program. These inputs may be the result of a data call, or they may be a real-time, automated data feed. For example, the Human Resources management system may provide the insider threat team an automated listing of people who are leaving the organization. This information can then be

used to determine if any additional procedures need to be implemented. Each business unit should have a trusted agent who can provide data feeds or additional information. The insider threat team should identify trusted agents ahead of time, so they can be contacted immediately when an incident occurs. At a minimum, a current background check along with signing of an insider threat program non-disclosure agreement should be completed on trusted agents before they are placed into this role. The insider threat team may find that other departments within the organization are more willing to cooperate if it requests data only and performs its own analysis. For example, the team should request facility access logs from the Physical Security team and then conduct its own analysis.

The potential team members listed above might be helpful for prevention, detection, and/or response efforts. Not every team member need be alerted for every potential threat. Instead, the CERT Division recommends that organizations consider which team members need to be involved for each type of effort and, during a response, which members should be involved at different levels of response escalation. The team should meet regularly to ensure it remains active and effective. The team should discuss anomalies detected (proactive response) and allegations (reactive response) of potential insider activity. The team might meet in one physical space, or electronic communication such as videoconference meetings and discussions by secure email could be considered, which could enable team members in separate locations to quickly, conveniently, and cheaply collaborate. The team should follow procedures for security and discretion when using email because many people outside the team, such as system administrators and administrative assistants, might have access to the emails and be a person of interest or be friends with a person of interest. Security procedures should include encryption using public key cryptography, such as PGP. They should also specify that email can only briefly be decrypted and read while not connected to any network, must be stored in encrypted form, and must have its decrypted version securely deleted. Another factor to consider is that electronic meeting spaces could be impossible to use if the communications system is being attacked or the insider has the ability to monitor the meeting, so alternate plans should be created. Each organization is different and should create its particular insider threat team and plans according to its size, capabilities, and risk tolerance.

During an inquiry, the insider threat team must maintain the confidentiality of all related information to ensure privacy and hide the inquiry from the insider suspected of wrongdoing. It is important to note that once an allegation of suspected insider activity is made, that allegation can never be fully retracted. Even if the suspect is cleared of any wrongdoing, knowledge of the accusation will linger with those who were told of it, and it could ruin an individual's career. Therefore, it is of upmost importance to keep inquiries confidential and discuss them only with those who have a legitimate need to know. When the insider threat team is conducting an inquiry, it should be careful how it requests data. For example, if the team is inquiring about a person in the Accounting department and needs to see system logs to establish login and logoff times, the team should request logs from a larger data set, such as the Accounting department and another team within the organization, to avoid tipping off either the suspect or the data owner. The insider threat core team can then pare the logs to its specific needs. Organizations should include random audits of various data sources as part of policies and standard operating procedures. This can potentially reveal previously unidentified threats, as well as provide a good non-alerting cover for data requests made during active inquiries. Organizations should consult with legal counsel before implementing any type of auditing program.

Another way the insider threat team differs from an incident response team is that it has a proactive role. For example, previous research shows that employees who are engaged in their jobs are not only more productive but are also less likely to act in ways that are counter to the organization's interests [Sulea et al. 2012, Ariani 2013]. While more research is needed, this suggests that practices to improve employee engagement (e.g., strength-based management to increase employee-job fit), may be a good foundation for building an insider threat resistant enterprise. Other research has shown the productivity and retention benefits of employee engagement, so such practices may be a win-win situation for the organization and the employee [Gallup 2013]. The insider threat team should proactively deal with employee problems, working to prevent and identify potential threats in order to minimize harm.

Any insider threat program implemented within the organization must be lawful and abide by all rules and regulations that bind the company. Monitoring activities must be within bounds, as must the location where monitored information is kept and the people who have access to it. It is imperative that the organization involve legal counsel before implementing any insider threat program and during any inquiry. Legal counsel is vital during the information-gathering process to ensure all evidence is maintained in accordance with legal standards and to issue a prompt legal response when necessary. Legal advice is also necessary to assure that the insider threat team members share information properly, for instance, ensuring lawful privacy to workers regarding mental and physical health. Workplace violence prevention programs, such as the U.S. Department of Agriculture's,[6] similarly call for a threat assessment team from members from multiple departments, and the team works proactively and confidentially to identify and mitigate potential threats. The Occupational Safety and Health Act's General Duty Clause requires many employers to provide a safe workplace [OSHA 2015], so workplace violence prevention programs are now widely implemented. Those programs have solved the employee privacy issue under well-defined circumstances, and the insider threat team needs to do so as well.

The HR team will be instrumental in detecting possible signs of behavioral issues related to insider threats. To ensure employee privacy, HR will need to carefully screen any information involved in an inquiry and release only the minimum necessary amount on a need-to-know basis. The HR team may use internal findings to develop a watch list of personnel and release it to certain members of the IA and insider threat teams so they know what logs to review. Behavioral and technical indicators identified by the CERT Division and other insider threat research might be used as potential indicators, as part of the organization's insider threat program. Examples of employee behaviors that may signal a potential malicious insider include, but are not limited to

- repeated policy violations—indicator correlated to sabotage
- disruptive behavior—indicator correlated to sabotage
- financial difficulty or unexplained extreme change in finances—indicator correlated to fraud
- job performance problems—indicator correlated to sabotage and IP theft

The CERT Insider Threat Center's work includes analysis of various pathways to an insider eventually committing an attack or theft. While HR can flag certain behavioral indicators, it also has a responsibility to others in the organization. When an employee submits his or her

[6] *The USDA Handbook on Workplace Violence Prevention and Response*, http://www.dm.usda.gov/workplace.pdf

resignation or leaves the organization by other means, HR needs to notify members of the IT team so they can perform enhanced auditing on the exiting individual.

The following examples show a few of the many pathways to three categories of insider incidents and how an insider threat team should work for each.

IT sabotage:

1. Behavioral issues are reported by management to HR.
2. HR notifies the Computer Security Incident Response Team (CSIRT).
3. The insider threat team conducts an inquiry of past and present online activity and projects future online activity.

Theft of IP:

1. An employee who has access to sensitive IP (trade secrets, source code, engineering or scientific info, strategic plans, etc.) quits.
2. HR notifies the CSIRT insider threat team to conduct an inquiry of past and present online activity and project future online activity, with a particular focus on logs of activity for 30 days before and after the insider resigned.

Fraud:

1. An employee is experiencing extreme financial difficulty or has a sudden, unexplained change in financial status.
2. Management tells Security or HR, which tells the CSIRT insider threat team.
3. The insider threat team increases monitoring of financial transactions and data, such as personally identifiable information (PII) that could be sold. The team also investigates past and present online activity and projects future online activity.

The IT and IA teams must collaboratively devise a strategy for monitoring high-risk insiders, such as those on the HR team's watch list. The teams should identify all the systems and information the high-risk employee has access to and ensure that audit logs are capturing a sufficient level of information to identify[7]

- who performed an action (user name)
- what action was performed and what the outcome of the action was (success or failure)
- when the action took place (date and time)
- where the action was performed (workstation name, server name, etc.)

When implementing auditing controls to detect malicious insiders, it may be necessary to perform more granular and verbose auditing. Ideally, the IT and IA teams will have a SIEM system collect and correlate all security events.[8] Typically, SIEM systems can be customized to look for certain patterns or extract events having a given set of criteria. For further discussion of centralized logging, see the CERT Insider Threat Center's technical note *Insider Threat Control: Using*

---

[7] See Practice 10, "Implement strict password and account management policies and practices" (p. 35).

[8] See Practice 12, "Deploy solutions for monitoring employee actions and correlating information from multiple data sources." (p. 56).

Centralized Logging to Detect Data Exfiltration Near Insider Termination.[9] The IT and IA teams will also be instrumental in implementing safeguards to protect systems and data.

The Physical Security team should work with the IA team to collect physical access logs. When possible, Physical Security and IT should correlate their logs to facilitate detection of insider and other threats. Physical Security may be able to provide video surveillance history. Depending on the depth of the established program, legal counsel's advice, and management's risk tolerance, the Physical Security team may also assist investigations by seizing, storing, and processing evidence. Finally, the Physical Security team may need to escort individuals off the organization's premises.

An insider threat program must operate under clearly defined and consistently enforced policies. Regular meetings help the team ensure the program's compliance. They also allow team members from different departments to share information and create cross-enterprise situational awareness, maintaining the team's readiness to respond to insider threats. It takes inter-departmental communication and a cross-organizational team to successfully prevent, detect, and respond to insider threats.

[9] http://www.sei.cmu.edu/library/abstracts/reports/11tn024.cfm

2.2 Understanding and Avoiding Potential Pitfalls

There is the potential for insider threat programs themselves to be the source of organizational performance problems, or even worse, to exacerbate the insider threat that it is intended to mitigate. Previous work has elaborated several categories of potential negative unintended consequences of establishing and operating formal insider threat programs and suggestions for their mitigation:

- Interference with legitimate whistleblower processes and protections—Unintended consequences can occur if the insider threat program does not treat whistleblowing as a legitimate function with its own processes and procedures, or even if it does, employees do not trust that whistleblowers will be treated fairly.
- Disruption of relationships between and among insider threat programs management and employees—An insider threat program has the potential to strain the relationship between managers and the employees that they manage at all levels. An organization's employees may view the program staff in an adversarial way—"they are trying to catch us doing something bad!" Employees may start gaming the system, hiding their behavior, or neglecting to report coworker behaviors that the insider threat program depends on for an effective detection system. Employees, especially those that view the program adversarially, may infer the strategy of the InTP from the response that it takes to various behaviors and thus inhibit InTP effectiveness over time.
- Management's lack or loss of interest in the insider threat program—Support for the insider threat program from the chief executive through all levels of management is crucial for the continued success of the mission. Many organizations are mandated to establish an InTP, but if financial support is inadequate or there are other perceived higher priorities, support may dwindle for anything beyond paying lip service to the need. The situation may become worse if the program appears to be ineffective or if the false-positive rate is higher than expected. On the other hand, if the program seems to solve all insider problems, or no insider incidents actually occur, management may also want to move financial support to other activities. Finally, any way that the insider threat program appears to increase the liability of the organization, especially with regard to employment law, may discourage the support needed for effective program implementation.
- Purposeful misuse of the insider threat program by its staff or other employees—The intended function of legitimate and necessary activities can be subverted by individuals who have other goals in mind. The insider threat program could be used by unscrupulous individuals to falsely accuse or hide the malicious activities of staff members or fellow employees. Targeting certain employees over others or using program functions for purposes other than those intended, such as monitoring employee productivity as general performance evaluation, is counter to effective functioning. Insider threat programs themselves may cause problems by exaggerating the insider threat faced by the organization to garner greater support, taking resources away from possibly more critical functions within the organization. The unintended consequences can trigger other consequences described previously that relate to worsening relationships among the staff, management, and other employees.
- Misuse of the insider threat program by its staff or others—Some misuse of the program function can be unintentional in nature. These accidents may lead to violations of HR employment laws or unintentional disclosure of confidential information as part of the insider

detection function. A side effect of insider investigations might include harm to the reputation or career of someone who was under suspicion, but later cleared, of an illicit act.

- Until empirical evidence is available, we believe organizations should consider potential negative unintended consequences of the practices that they put in place and identify associated mitigations. The preliminary investigation conducted by the CERT may be helpful for organizations establishing resilient Insider Threat Programs [Moore et al. 2015].

2.3 Challenges

1. working together across the organization—Policies, processes, and technology for working together across the organization must be developed.
1. maintaining motivation—Organizations may not have many insider incidents. In these cases, a solely dedicated insider threat team is not necessary, but team members will need to be motivated to continue their mission when called upon.
2. justifying funding—It may be difficult to justify the insider threat team's existence in organizations that do not suffer from frequent malicious insider activity.
3. finding team participants—Small organizations may not have personnel dedicated to the various roles discussed above. As long as management knows whom to contact when an insider incident occurs and that person knows what to do, organizations should still be able to respond to an incident.
4. avoiding negative unintended consequences—It is difficult to foresee all the implications of complex organizational change. Insider threat program designers and managers need to think about negative unintended consequences that could happen in the planning stages and be vigilant for spotting them while in operation, and instituting mitigations as needed.

2.4 Governance of an Insider Threat Program

A mature governance structure is essential to effectively develop, deploy, and manage an insider threat program. The CERT Insider Threat Center recommends that the organization implement a governance structure that enables the insider threat program to

- Maintain an updated knowledge base related to insider threats including staying current with the latest research and capturing lessons learned.
- Provide support to the insider threat program stakeholders to ensure the groups are meeting their objectives, providing the appropriate inputs to the insider threat program manager and appropriately communicating results and decisions to other insider threat program stakeholders.
- Monitor governance practices to ensure that governing bodies are meeting insider threat program needs, to make recommendations for improvement, and to refine the measures as needed.
- Capture and communicate insider threat program success stories to internal and external stakeholders to increase program support.
- Execute a comprehensive program-risk-management approach and required procedures for insider threat program stakeholders.
- Perform processes including budgetary review, the development of future technical requirements, continuous operation procedures, and risk management.
- When applicable, facilitate both formal and informal Continuous Diagnostic Monitoring (CDM) governance training for the CDM program staff, departments and/or agencies (D/As), partners, and stakeholders.

- Maintain and execute the program schedule for updating charter guidance, procedures, and policies based on ongoing lessons learned (both internally and externally), best practices, and stakeholder input.

2.5 Case Studies

In a sabotage case, an information technology support business had employed the insider as a computer support technician. As part of his duties, the insider had administrator-level, password-controlled access to the organization's network. Late one weekend night three months after leaving the organization, the insider used his administrator account and password to remotely access the organization's network. The insider changed the passwords of all the organization's IT system administrators and shut down nearly all the organization's servers. The insider deleted files from backup tapes that would have enabled the organization to promptly recover from the intrusion. The organization and its customers experienced system failure for several days. Investigators traced the incident to the insider's home network. The insider was arrested, convicted, ordered to pay over $30,000 in restitution, and sentenced to between one and two years of imprisonment, followed by several years of supervised release. The insider was also ordered to perform 100 hours of community service lecturing young people on the consequences of illegal hacking.

This case highlights the need for an insider threat program. The insider was able to remotely connect to the organization's systems to commit a malicious act after separating from the organization. Had the victim organization's HR department communicated the insider's separation to its information assurance team, the insider's account could have been locked or deleted, preventing the incident. The victim organization should have had a comprehensive exit process, as described in Practice 20, "Develop a comprehensive employee termination procedure." The CERT insider threat database showed that the incident also took place under circumstances that have occurred in other cases of sabotage: after-hours access and remote use of administrative accounts. Customized rules in a SIEM solution would have helped the organization detect potential attacks by detecting such circumstances and alerting the IA team to review the suspicious activity. Further discussion of SIEM systems can be found in Practice 12, "Deploy solutions for monitoring employee actions and correlating information from multiple data sources." (p. 79). In addition, the organization should have carefully monitored remote access, as described in Practice 13, "Monitor and control remote access from all end points, including mobile devices" (p. 85).

The following fraud case similarly shows how an insider threat program could have prevented, detected, and responded to insider threats. An insider was employed as a bookkeeper by the victim organization. Over the course of approximately two years, the insider wrote more than 70 checks from the organization's account to pay for her personal expenses and altered the organization's computer accounting records to show a different payee. The insider embezzled almost $200,000 from the organization. The insider's activity was detected when a manager noticed irregularities in the electronic check ledger. The insider was convicted and sentenced to between one and two years of imprisonment. However, the court-ordered restitution was only $20,000, so the company permanently lost the vast majority of the embezzled funds. Prior to this incident, the insider had been convicted of a similar fraud. An insider threat team would have created policies and procedures calling for background checks, which could have prevented the

entire incident by ensuring her conviction would have been discovered during the screening process, likely disqualifying her for employment. An insider threat team would have established detection processes for unusual and suspicious events, so the first series of unusual changes to the electronic ledger might have been detected. Then the insider threat team could have more closely monitored the insider's activities and discovered the fraud much earlier. Earlier fraud detection would have reduced the losses.

Similarly, the losses in the following theft of IP case might have been prevented or reduced if an insider threat program had been in place. The insider was employed as a research chemist by the victim organization, responsible for various research and development projects involving electronic technologies. The insider accepted a job offer with a different company. In the four months prior to leaving the victim company, the insider accessed the organization's servers and more than 15,000 PDF files and more than 20,000 abstracts containing the victim organization's trade secrets. After he resigned, the victim organization detected the insider's substantial quantity of downloads. The insider started his new job at the competitor organization and transferred much of the stolen information to a company-assigned (competitor company) laptop. The victim organization notified the competitor organization that it had discovered the high volume of downloads. The competitor organization seized the insider's laptop and turned it over to the victim organization. The insider eventually was convicted, sentenced to between one and two years of imprisonment, and ordered to pay approximately $14,000 in restitution and a $30,000 fine.

After performing forensic analysis, the company determined that amount of data the insider downloaded was 15 times higher than that of the next highest user, and the data was not related to his research. An insider threat team might have prevented, detected earlier, or reduced harm from this insider by monitoring any unusual behavior on computer systems, which would have detected the insider's unusual downloads. The team then could have taken action with senior management and human resources to either immediately terminate the insider's employment and engage law enforcement or heighten monitoring and examine previous logs to gather more information about the scope of the insider's activities. The organization might have prevented the transfer of valuable IP (the court case did not ascertain if that competitor company or any other acquired or used the IP). At the very least, the IP was at a very high risk and out of control of the victim company for a period of time, and an insider threat team could have prevented, detected, and responded to the threat.

2.6 Quick Wins and High-Impact Solutions

2.6.1 All Organizations

- ☐ Ensure that legal counsel determines the legal framework the team will work in.
- ☐ Establish policies and procedures for addressing insider threats that include HR, Legal, Security, management, and IA.
- ☐ Consider establishing a contract with an outside consulting firm that is capable of providing incident response capabilities for all types of incidents, if the organization has not yet developed the expertise to conduct a legal, objective, and thorough inquiry.

2.6.2 Large Organizations

- ☐ Formalize an insider threat program (with a senior official of the organization appointed as the program manager) that can monitor for and respond to insider threats.
- ☐ Implement insider threat detection rules into SIEM systems. Review logs on a continuous basis and ensure watch lists are updated.
- ☐ Ensure the insider threat team meets on a regular basis and maintains a readiness state.

2.7 Mapping to Standards

- NIST: AT-2, AU-6, IR-4, SI-4
- NITTF: B
- Minimum Standards: G-1
- CERT-RMM:
  - Incident Management and Control
    - (detection through response)
  - Vulnerability Analysis and Resolution
- ISO 27002:
  - 6.1.2 Information security coordination
  - 15.1.5 Prevention of misuse of information processing facilities (deter users from using a system in unauthorized ways)

Practice 3: Clearly document and consistently enforce policies and controls.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	✓

A consistent, clear message on all organizational policies and procedures will reduce the chance that employees will inadvertently damage the organization or lash out at the organization for a perceived injustice. Organizations must ensure that policies are fair and punishment for any violation is not disproportionate.

3.1 Protective Measures

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

Organizations should ensure policies and controls provide:

- concise and coherent documentation, including reasoning behind the policy, where applicable
- consistent and regular employee training on the policies and their justification, implementation, and enforcement

Organizations should be particularly clear on policies regarding

- acceptable use and disclosure of the organization's systems, information, and resources
- use of privileged or administrator accounts
- ownership of information created as a work product
- evaluation of employee performance, including requirements for promotion and financial bonuses
- processes and procedures for addressing employee grievances

As individuals join the organization, they should receive a copy of organizational policies that clearly lay out what is expected of them and the consequences of violations. Organizations should retain evidence that each individual has read and agreed to organizational policies.

System administrators and anyone with unrestricted access to information systems present a unique challenge to the organization. Organizations should consider creating a special policy for acceptable use or rules of behavior for privileged users. Organizations should reaffirm this policy with these users at least annually and consider implementing solutions to manage these types of privileged accounts (see Practice 10: "Implement strict password and account management policies and practices.").

Employee disgruntlement has been a recurring factor in insider compromises, particularly in cases of insider IT sabotage. In each case, the insider's disgruntlement was caused by some unmet expectation, including

- insufficient salary increase or bonus
- limitations on use of company resources
- diminished authority or responsibilities
- perception of unfair work requirements
- feeling of being treated poorly by co-workers

Clear documentation of policies and controls can prevent employee misunderstandings that can lead to unmet expectations. Consistent enforcement can ensure that employees do not feel they are being treated differently from or worse than other employees. Organizations need to ensure that management is not exempt from policies and procedures. Otherwise, it appears that not everyone is held to the same standards and management does not fully support the policy or procedure.

Organizations are not static entities, and change in organizational policies and controls is inevitable. Organizations should review their policies regularly to ensure they are serving the organization well. Employee constraints, privileges, and responsibilities change as well. Organizations must recognize times of change as particularly stressful for employees, acknowledge the increased risk associated with these stress points, and mitigate the risk by clearly communicating what employees can expect in the future.

3.2 Challenges

The organization may face these challenges when implementing this best practice:

1. designing good policy—It can be difficult to develop policies that are clear, flexible, fair, legal, and appropriate for the organization.
2. enforcing policy—Organizations must balance consistent policy enforcement with fairness, especially under extenuating circumstances.
3. managing policy—Organizations must consistently review and update policies to ensure that they are still meeting the organizational need and to ensure updates are disseminated to all employees.

3.3 Case Studies

A government agency employed the insider as a lead software engineer. At the victim organization, the insider led a team developing a software suite. After major issues were found with the first implementation of the software suite, the organization's management requested that the insider document all source code and implement configuration management and central control of the development process. The insider later learned that the organization was going to outsource future development of the suite, demote him, reduce his pay, and move him to another office. While the project was still under the insider's control, he wrote the code in an obscure way to undermine the project's transition. The insider filed a grievance and took a leave of absence. The organization denied the grievance, and the insider resigned. Prior to resigning, the insider copied the source code to removable media and encrypted it with a password. The insider then deleted the source code from his laptop, which he turned in at the time of his resignation. He

explained that he had intentionally deleted the source code as part of wiping his laptop before turning it in, but did not disclose that he had retained a copy. The organization discovered that he had deleted the only copy of the source code for the system—a safety-related system that was being used in production at the time. The system executable continued to function, but the organization was unable to fix any bugs or make any enhancements due to the missing source code. Investigators eventually discovered the encrypted copy of the software at his home. After nine months the insider finally admitted his guilt and provided the cryptographic key. The insider was arrested, convicted, sentenced to one year of imprisonment, and ordered to pay $13,000 in fines and restitution.

In this case, the organization should have created and enforced clearly defined policies, procedures, and processes for software development. Had the organization held all software projects to these requirements, the incident may have been avoided because the developer would have known what his employer expected of him. In addition, since this was a mission-critical system, the organization should have had a change management program in place that would have required the submission of the source code to the change management program manager to maintain software baselines. This would have ensured that someone other than the insider would have had a copy of the source code.

In another case, an IT department for a government entity employed the insider as a network administrator. The insider, who built the organization's network, was the only person with the network passwords as well as true knowledge of how the network functioned. The insider refused to authorize the addition of any new administrators. The organization reprimanded the insider for poor performance. After being confronted by and subsequently threatening a co-worker, the insider was reassigned to a different project. The insider refused to give up the network passwords, so the organization terminated his employment and had him arrested. The organization was locked out of its main computer network for close to two weeks.

After the insider's arrest, the insider's colleagues discovered that he had installed rogue access points in hidden locations and had set up the organization's system to fail if anyone attempted to reset it without the proper passwords. The insider provided passwords to police, but none of the passwords worked. The insider later relinquished the real passwords in a meeting with a government official, who was the one person the insider trusted. The insider defended his actions, claiming that they were in line with standard network security practices. The insider was convicted and sentenced to four years of imprisonment and is awaiting a financial penalties hearing. The organization's incident-related loss was between $200,000 and $900,000.

This case illustrates the need for an organization to consistently enforce policies and procedures. The insider was able to control the organization's network with little oversight and became a single point of failure. More than one person in an organization should have knowledge of and access to its network. This reduces the likelihood of a system failing due to the loss or malicious action of an employee. It also allows a system of checks and balances in which other administrators monitor the network for hardware or software changes.

3.4 Quick Wins and High-Impact Solutions

3.4.1 All Organizations

The following considerations apply to organizations of all sizes. Some organizations may not have a department dedicated to security (physical security, IT security, etc.). However, the underlying theme of the practice still applies.

- ☐ Ensure that senior management advocates, enforces, and complies with all organizational policies. Policies that do not have management buy-in will fail and not be enforced equally. Management must also comply with policies. If management does not do so, subordinates will see this as a sign that the policies do not matter or they are being held to a different standard than management. Your organization should consider exceptions to policies in this light as well.
- ☐ Ensure that management briefs all employees on all policies and procedures. Employees, contractors, and trusted business partners should sign acceptable-use policies upon their hiring and once every year thereafter or when a significant change occurs. This is also an opportunity for your organization and employees, contractors, or trusted business partners to reaffirm any nondisclosure agreements.
- ☐ Ensure that management makes policies for all departments within your organization easily accessible to all employees. Posting policies on your organization's internal website can facilitate widespread dissemination of documents and ensure that everyone has the latest copy.
- ☐ Ensure that management makes annual refresher training for all employees mandatory. Refresher training needs to cover all facets of your organization, not just information security. Training should encompass the following topics: human resources, legal, physical security, and any others of interest. Training can include, but is not limited to, changes to policies, issues that have emerged over the past year, and information security trends.
- ☐ Ensure that management enforces policies consistently to prevent the appearance of favoritism and injustice. The Human Resources department should have policies and procedures in place that specify the consequences of particular policy violations. This will facilitate clear and concise enforcement of policies.

3.5 Mapping to Standards

- NIST: PL-1 (Security Planning Policy and Procedures), PL-4 (Rules of Behavior), PS-8 (Personnel Sanctions)
- NITTF:
- CERT-RMM:
  - Compliance
- ISO 27002:
  - 15.2.1 Compliance with security policies and standards

Practice 4: Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	✓

Organizations should proactively deal with suspicious or disruptive employees to reduce the risk of malicious insider activity.

4.1 Protective Measures

An organization's approach to reducing its insider threat should start in the hiring process. Background checks on prospective employees should reveal previous criminal convictions, include a credit check, verify credentials and past employment, and include discussions with prior employers regarding the individual's competence and approach to dealing with workplace issues. Organizations must consider legal requirements (e.g., notification to and consent from the candidate) when creating a background-check policy. Prior to making any employment decisions based on background information, organizations must consider legal guidance, including the Equal Employment Opportunity Commission's (EEOC) best practices[10] and state and local regulations limiting the use of criminal or credit checks [EEOC 2012]. The organization must use background information lawfully, with due consideration to the nature and duration of any offense, as part of a risk-based decision process to determine the employee's access to critical, confidential, or proprietary information or systems. The organization should require background checks for all potential employees as well as contractors and subcontractors, who should be investigated just as thoroughly.[11]

Organizations should assign risk levels to all positions and more thoroughly investigate individuals applying for positions of higher risk or that require a great deal of trust [NIST 2015]. Periodic reinvestigations may be warranted as individuals move to higher risk roles within the organization, again complying with all legal requirements.

Training supervisors to recognize and respond to employees' inappropriate or concerning behavior is a worthwhile investment of an organization's time and resources. In some insider threat cases, supervisors noticed minor but inappropriate workplace behavior, but they did not act because the behavior did not violate policy. However, failure to define or enforce security policies in some cases emboldened the employees to commit repeated violations that escalated in severity and increased the risk of significant harm to the organization. Organizations must consistently enforce policies and procedures for all employees, including consistent investigation of and response to rule violations.

[10] http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm

[11] See Practice 6, "Consider threats from insiders and business partners in enterprise-wide risk assessments" (p. 49),for further discussion on background investigations.

Because financial gain is a motive to commit fraud, organizations should be alert to any indication from employees of financial problems or unexplained financial gain. Malicious insiders have used IT to modify, add, or delete organizational data, as opposed to programs or systems, without authorization and for personal gain. They have also used IT to steal information that leads to fraud (e.g., identity theft, credit card fraud). Sudden changes in an employee's financial situation, including increased debt or expensive purchases, may be signs of potential insider threat. Again, organizations must consider legal requirements, such as employee notifications, when responding to such situations.

Organizations should have policies and procedures for employees to report concerning or disruptive behavior by co-workers. Consistent monitoring steps should be taken in response to concerning or disruptive behaviors, according to written policies, to eliminate biased application of monitoring or even its appearance. Organizations should investigate all reports of concerning or disruptive behavior until an appropriate organizational response is determined. If an employee exhibits concerning behavior, the organization should respond with due care. Disruptive employees should not be allowed to migrate from one position to another within the enterprise and evade documentation of disruptive or concerning activity. Organizations should also treat threats, boasts about malicious acts or capabilities ("You wouldn't believe how easily I could trash this net!"), and other negative sentiments as concerning behavior. Many employees will have concerns and grievances from time to time, and a formal and accountable process for addressing those grievances may satisfy those who might otherwise resort to malicious activity. In general, organizations should help any employee resolve workplace difficulties.

Once an organization identifies an employee's concerning behavior, it may take several steps to manage the risks of malicious activity. These steps can include evaluating the employee's access to critical information assets and level of network access, reviewing logs of recent activity by the employee, and presenting the employee with options for coping with issues causing the behavior, such as access to a confidential Employee Assistance Program (EAP).

Legal counsel should ensure all monitoring activities are within the bounds of law. For instance, private communications between employees and their doctors and lawyers should not be monitored. Additionally, federal law protects the ability of federal employees to disclose waste, fraud, abuse, and corruption to appropriate authorities. For this reason, federal worker communications with the Office of Special Counsel or an agency inspector general should not be monitored. For the same reason, an organization must not deliberately target an employee's emails or computer files for monitoring simply because the employee made a protected disclosure [NIST 2012].

4.2 Challenges

1. sharing information—Organizations may find it difficult to share employee information with those charged with protecting the systems. To ensure compliance with laws, regulations, and company policies, organizations must consult legal counsel before implementing any program that involves sharing employee information.
2. maintaining employee morale—Organizations must ensure that they do not convey a sense of "big brother" watching over every employee's action, which can reduce morale and affect productivity.

3. using arrest records—The EEOC recently issued updated guidance regarding the use of arrest or conviction records when making employment decisions including hiring, promotion, demotion, or as a reason to limit access to information or systems. The guidance clarifies that employers should not rely on arrest records as opposed to convictions, because arrest records are less indicative that the candidate actually engaged in the criminal conduct. Using arrest (versus conviction) records to make hiring decisions is contrary to best practices as clarified by the EEOC. Possibly limiting access to information or systems due to an arrest record has similar issues and thus, at this time, legal counsel is strongly recommended before using or disclosing arrest record information from a background check. Related to this, a previous CERT study showed that 30% of the insiders who committed IT sabotage had a previous arrest history. It turns out that correlation may not be meaningful. A 2011 study using a large set of data from the federal government showed that 30% of all U.S. adults have been arrested by age 23, and back in 1987 a study showed similar statistics, with 35% of people in California having been arrested between ages 18-29 [Tillman 1987]. Many of the insider crimes were performed by insiders over age 29. Future research that focuses on particular job categories may show different averages of previous arrest rates for insiders convicted in the United States. However, currently, use of arrest data is both legally and scientifically questionable.
4. monitoring only legally allowable communications—Special care must be taken to prevent monitoring of private communications between employees and their doctors and lawyers, as well as between federal workers and the Office of Special Counsel or an agency inspector general.

4.3 Case Studies

In one recent case, an organization employed a contractor to perform system administration duties. The contractor compromised the organization's systems and obtained confidential data on millions of its customers. Though the contractor's company told the hiring organization that a background check had been performed, the investigation of the incident revealed that the contractor had a criminal history of illegally accessing protected computers that would have been detected with a background check. This illustrates the need to contractually require contractors to perform background investigations on their employees.

In another case, a large shipping and storage corporation employed the insider as an executive-level officer. After 11 years of employment there, the insider had gained the company's trust. However, prior to his employment at the victim organization, he had stolen money from a few other companies he had worked for. The insider had been convicted, but he had served his sentence on work release. After claiming to have cleaned up his act, he was employed by the victim organization and quickly climbed to the executive-level position. The media often praised him for his innovative management and operational practices. In his last two years of employment, he devised and carried out a scheme to defraud his employer. He inflated prices of invoices charged to his department and collected part of the payments. Furthermore, the insider would pay an outside organization run by a conspirator for services never rendered. In return, the conspirator would wire back parts of the payment to the insider. A routine audit of the victim organization's finances discovered the insider's activities, and he was found to have stolen more than $500,000. The insider was sentenced to six years of imprisonment and ordered to pay full restitution. This case illustrates the need for organizations to consider a potential employee's

background before making a hiring decision. Management must evaluate a candidate's complete background and assess the organization's willingness to accept the risk before extending an offer to a candidate. Organizations must also ensure that legal agreements with trusted business partners convey the organization's requirements for background investigations.

In another case, the victim organization, a visual technology manufacturer and provider, employed the insider as a network administrator. The organization hired a new supervisor, who fired a number of employees but promoted the insider. The insider told co-workers that he had installed back doors and planned to use them to harm the organization, but the remaining co-workers were afraid to speak up due to the recent terminations. The insider displayed bizarre workplace behavior, including installing a video camera in the organization's computer room and calling people in the room to say he was watching.

When the organization hired him, the insider falsely claimed to hold a certification and to have been recommended by a headhunter. The organization failed to verify that claim. The insider also concealed his violent criminal history, including assault with a deadly weapon, corporal injury to a spouse, possession of a firearm, and fraudulent use of two Social Security numbers (SSNs). The insider also had assault weapons at his home, which he had shown to a co-worker. The semiautomatic weapons were registered to the insider's brother-in-law, who lived with the insider.

The organization became suspicious of the insider when he became resistant and evasive after being asked to travel abroad for business. The insider claimed he did not like flying, but he had a pilot's license. The insider also claimed that he did not have a proper birth certificate due to identity theft. The organization then discovered that the insider did not have the certification he claimed and terminated him. Initially the insider withheld his company laptop until the organization withheld his severance pay until they received the laptop. The insider complied, but the laptop was physically damaged and its hard drive was erased.

After the insider's termination, the organization noticed that the insider repeatedly attempted to remotely access its servers. The organization asked the insider to stop, but he denied having made such attempts. The organization anticipated the insider's attack and hired a computer security consulting firm. The consultants blocked the insider's Internet protocol address (IP address) at the organization's firewall, deleted his accounts, checked for back doors, and watched for illicit access. The consultants failed to check one server to which the insider had access. Later, the consultants performed a forensic examination and detected that the insider had used virtual private network (VPN) accounts to log in over the two-week period between the insider's termination and the incident. The organization was unaware of the existence of those accounts, which were created before the insider's termination. These accounts were in the names of his superiors and allowed him remote access to the organization's critical assets. The insider accessed the server, deleted crucial files, and rendered the server inoperable. The insider was arrested, convicted, sentenced to one year of imprisonment, and ordered to undergo mental health counseling.

The organization in this case failed to:

- verify the employee's credentials before hiring him
- conduct a thorough background investigation
- implement proper account management policies and procedures

The organization might have avoided this situation completely had it conducted a thorough background investigation, including verifying any industry certifications or credentials claimed by the individual. In this case, the insider should have never passed the background investigation process.

In addition, the organization should have noticed a number of early warning signs of a potential insider threat. The insider:

- told co-workers he implemented back doors into the organization's systems
- installed a surveillance camera in the server room and called co-workers saying that he was watching them
- resisted and evaded common business-related requests

Co-workers and management should have raised concerns about these events. Any employee who has concerns about another's actions should be able to report the issue without fear of reprisal. The availability of an anonymous employee reporting system, such as a tip line hosted by a third party, might have encouraged fearful co-workers to provide information that could have led the organization to further scrutinize the insider before the attack took place.

4.4 Quick Wins and High-Impact Solutions

4.4.1 All Organizations

- ☐ Ensure that potential employees have undergone a thorough background investigation, which at a minimum should include a criminal background and credit check.
- ☐ Encourage employees to report suspicious behavior to appropriate personnel for further investigation.
- ☐ Investigate and document all issues of suspicious or disruptive behavior.
- ☐ Enforce policies and procedures consistently for all employees.
- ☐ Consider offering an EAP. These programs can help employees deal with many personal issues confidentially.

4.4.2 Mapping to Standards

- NIST: PS-1 (Personnel Security Policy and Procedures), PS-2 (Position Risk Designation), PS-3 (Personnel Screening), PS-8 (Personnel Sanctions)
- NITTF: C-1-1, C-1-2
- Minimum Standards: H
- CERT-RMM:
  - Monitoring
  - Human Resources Management
    - SG3.SP4: Establish a disciplinary process for those who violate policy
- ISO 27002:
  - 8.1.2 Screening (partially applies, only covers hiring process)

–

Practice 5: Anticipate and manage negative issues in the work environment.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	✓

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

5.1 Protective Measures

Organizations must communicate their policies and practices to new employees on their first day. Such policies and practices include acceptable workplace behavior, dress code, acceptable usage policies, working hours, career development, conflict resolution, and other workplace issues. The existence of such policies alone is not enough. New employees and veteran employees must all be aware of such policies and the consequences of violating them. Organizations must enforce their policies consistently to maintain a harmonious work environment.[12] Inconsistent enforcement of policies quickly leads to animosity within the workplace. In many of the analyzed insider threat cases, inconsistent enforcement or perceived injustices within organizations led to insider disgruntlement. Co-workers often felt that star performers were above the rules and received special treatment. Many times that disgruntlement led the insiders to sabotage IT or steal information.

Raises and promotions (annual cost of living adjustments, performance reviews, etc.) can have a large impact on the workplace environment, especially when employees expect raises or promotions but do not receive them. Employees should not count on these awards as part of their salary unless they are assured by contract, and even then the award amount specified in the contract may be variable. However, when such awards become part of the company's culture, employees will expect them year after year. The end of a performance period is one time when employees can have unmet expectations. If management knows in advance that the organization will not be able to provide raises or promotions as expected, they should inform employees as soon as possible and offer an explanation. Additional times of heightened financial uncertainty in the workplace environment include the end of a contract performance period without any clear indication if the contract will be renewed, and any time the organization reduces its workforce. The organization should be extra vigilant and deploy enhanced security measures if employees know there will be a reduction in force but do not know who will be laid off. An incumbent contractor who loses a re-compete bid may be disappointed. In all cases of heightened uncertainty or disappointment surrounding raises, promotions, and layoffs, the organization should be on heightened alert to any abnormal behavior and enact enhanced security measures to better mitigate insider threats.

[12] See Practice 3: "Clearly document and consistently enforce policies and controls" (p. 37).

Employees with issues need a way to seek assistance within the organization. Employees must be able to openly discuss work-related issues with management or Human Resources staff without fear of reprisal or negative consequences. When employee issues arise because of external factors, including financial and personal stressors, employees may find a service such as an EAP helpful. These programs offer confidential counseling to assist employees, allowing them to restore their work performance, health, or general well-being. Cases in the CERT insider threat database show that financial and personal stressors appear to have motivated many of the insiders who stole or modified information for financial gain. If these insiders had had access to EAPs, they may have found an alternative way to deal with their problems.

5.2 Challenges

1. predicting financial conditions—Organizations may find it difficult to predict financial issues that could affect employee salaries and bonuses.
2. maintaining trust between employees and management—Employees may be reluctant to share information with their manager about work-related issues for fear of it affecting multiple aspects of their employment.

5.3 Case Studies

A manufacturing company employed the insider as a salesperson. The organization required salespeople to regularly update a proprietary customer- and lead-tracking system. After being warned he would be fired for not updating the system as required, the insider still neglected to do so, and then the organization penalized the insider with a $2,500 salary deduction instead of firing him. The insider became disgruntled and sought employment with a competitor. The insider informed the competitor that he planned to bring customer information with him if he were hired. The victim organization became suspicious of the insider's activities, causing the insider to tell his contact at the competitor to delete all their email correspondence, which the contact did. The insider received an employment offer from the competitor. Two weeks later, the insider accessed the victim organization's computer system and downloaded customer records to his home computer. The insider then sent an email to the victim organization saying that he was resigning immediately from the victim organization and began to work for the beneficiary organization the next day. The insider immediately began contacting customers from the victim organization and recruiting them for the beneficiary organization. Once the victim organization discovered the insider's actions, it notified law enforcement. Law enforcement examined the insider's computers and noticed that 60 MB of data had been deleted and that the computer had been defragmented several times. The victim organization filed civil lawsuits against the insider and the beneficiary organization. The outcome of those suits is unknown.

In this case, the insider was warned about his performance problems yet still became disgruntled when the organization reduced his salary. The victim organization should have placed the insider on a watch list either at the time he was warned or when his salary was reduced. Had this been done, the insider may have been stopped before he could disclose customer data. This case also underscores the need for nondisclosure agreements, acceptable use agreements, or even noncompetition agreements.

In another case, the victim organization, a bank, triggered a mass resignation of employees disgruntled over layoffs. Before resigning, these insiders copied information from the victim organization's customer database, pasted it into Word documents, and saved them to disks. One such insider signed a non-solicitation agreement on the day of his resignation and later stole customer information via remote access. Six months before these events, that insider and a former co-worker had planned to form a new company and hire their colleagues, with whom they held meetings. The organization filed a civil lawsuit against the insider.

This case highlights the need for organizations to proactively protect their data. Layoffs heighten tension and stress at an organization. This can lead to a negative atmosphere, and management should be aware of the insider threat risk such an atmosphere poses. As part of an organization's risk management process, it should identify critical IP and implement appropriate measures to prevent its unauthorized modification, disclosure, or deletion. If the victim organization in this case had implemented technical measures, including additional auditing of sensitive files, earlier detection and prevention may have been possible.

5.4 Quick Wins and High-Impact Solutions

5.4.1 All Organizations

- ☐ Enhance monitoring of employees with an impending or ongoing personnel issue, in accordance with organizational policy and laws. Enable additional auditing and monitoring controls outlined in policies and procedures. Regularly review audit logs to detect activities outside of the employee's normal scope of work. Limit access to these log files to those with a need to know.
- ☐ All levels of management must regularly communicate organizational changes to all employees. This allows for a more transparent organization, and employees can better plan for their future.

5.5 Mapping to Standards

- NIST: PL-4 (Rules of Behavior), PS-1 (Personnel Security Policy and Procedures), PS-6 (Access Agreements), PS-8 (Personnel Sanctions)
- NITTF: C-1-2
- Minimum Standards: E
- CERT-RMM:
  - Human Resources Management
    - SG3.SP4: Establish a disciplinary process for those who violate policy

- ISO 27002
  - 8.2.1 Management responsibilities
  - 8.2.3 Disciplinary process
  - 8.3.1 Termination responsibilities

Practice 6: Consider threats from insiders and business partners in enterprise-wide risk assessments.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	

Organizations need to develop a comprehensive, risk-based security strategy to protect critical assets against threats from inside and outside the enterprise, including from trusted business partners who are given authorized insider access. All of the organization's employees, not just the major stakeholders, should understand the stakes of system compromise and loss or exposure of critical data.[13]

6.1 Protective Measures

Most organizations find it impractical to implement 100 percent protection from every threat to every organizational resource. Instead, they should expend their security efforts commensurately with the criticality of the information or other resource being protected. A realistic and achievable security goal is to protect assets deemed critical to the organization's mission from both external and internal threats. Organizations must carefully determine the likelihood and potential impact of an insider attack on each of their assets [NIST 2010] including on human life.

An organization must understand its threat environment to accurately assess enterprise risk. Risk is the combination of threat, vulnerability, and mission impact. Enterprise-wide risk assessments help organizations identify critical assets, potential threats to those assets, and mission impact if the assets are compromised. Organizations should use the results of the assessment to develop or refine an overall network security strategy that strikes the proper balance between countering the threat and accomplishing the organizational mission.[14] Having too many security restrictions can impede the organization's mission, and having too few may permit a security breach.

Organizations often focus too much on low-level technical vulnerabilities. For example, many rely on automated computer and network vulnerability scanners. While such techniques are important, our studies of insider threat indicate that vulnerabilities in an organization's business processes are at least as important as technical vulnerabilities. In addition, new areas of concern have appeared in recent cases, including legal and contracting issues, as detailed in the "Case Studies" section below. Many organizations focus on protecting information from access by external parties but overlook insiders. An information technology and security solution that does not explicitly account for potential insider threats often gives the responsibility for protecting critical assets to the malicious insiders themselves. Organizations must recognize the potential

[13] See Practice 9, "Incorporate insider threat awareness into periodic security training for all employees" (p. 62).

[14] See http://www.cert.org/work/organizational_security.html for information on CERT research in organizational security.

danger posed by the knowledge and access of their insiders, and they must specifically address that threat as part of an enterprise risk assessment.

Unfortunately, organizations often fail to recognize the increased risk of providing insider access to their networks, systems, information, or premises to other organizations and individuals with whom they collaborate, partner, contract, or otherwise associate. Specifically, contractors, consultants, outsourced service providers, and other business partners should be considered as potential insider threats in an enterprise risk assessment. The boundary of the organization's enterprise needs to be drawn broadly enough to include as insiders all people who have a privileged understanding of and access to the organization, its information, and information systems.

An organizational risk assessment that includes insiders as a potential threat will address the potential impact to the confidentiality, integrity, and availability of the organization's mission-critical information and resources. Malicious insiders have affected the integrity of their organizations' information in various ways, for example, by manipulating customers' financial information or defacing their organizations' websites. They have also violated the confidentiality of information by stealing trade secrets, customer information, or sensitive managerial emails and inappropriately disseminating them. Many organizations lack the appropriate agreements governing confidentiality, IP, and nondisclosure to effectively instill their confidentiality expectations in their employees and business partners. Having such agreements better equips an organization for legal action. Insiders have also affected the availability of their organizations' information by deleting data, sabotaging entire systems and networks, destroying backups, and committing other denial-of-service (DoS) attacks. Finally, insiders have been perpetrators of workplace violence resulting in loss of life.

In the types of insider incidents mentioned above, current or former employees, contractors, or business partners were able to compromise their organizations' critical assets. Protection strategies must focus on those assets: financial data, confidential or proprietary information, and other mission-critical systems and data. In addition to IT assets, organizations' critical assets can also include physical assets such as plants or vehicles. Organizations should also work to protect their employees with appropriate safety and security training.

Mergers and acquisitions can also create a volatile environment that poses potential risks for the acquiring organization. Before the acquiring organization transitions staff members from the acquired organization to new positions, it should perform background checks on them. The organization should consult legal counsel before conducting any background investigations and prior to making any employment decisions based on the resulting information.

The acquiring organization should also understand the risks posed by the newly acquired organization's information systems. The acquirer should weigh the risks of connecting the acquired company's untrusted system to the parent company's trusted system. If they are to be connected, the acquiring organization should first conduct a risk assessment on the new systems and mitigate any threats found.

6.2 Challenges

1. assessing risk—Organizations may have difficulty comparing the levels of threats from insiders versus outsiders.
2. lacking experience—Organizations may not include insider threat as part of enterprise risk assessments, so participants may need training in order to learn how to do them well.
3. prioritizing assets—Data and physical information system assets may be complex (e.g., individual hosts running multiple virtual machines with different business needs) or even scattered across the organization, making it difficult to assign risk or prioritization levels. See Practice 1: "Know and protect your critical assets" for further discussion of asset prioritization.

6.3 Case Studies

In one case, a mortgage company employed a contractor as a programmer and UNIX engineer. The organization notified the insider that his contract would be terminated because he had made a script error earlier in the month, but the insider was permitted to finish out the workday. Subsequently, while on-site and during work hours, the insider planted a logic bomb in a trusted script. The script was designed to disable monitoring alerts and logins, delete the root passwords to the organization's servers, and erase all data, including backup data, on those servers. The insider designed the script to remain dormant for three months and then greet administrators with a login message. Five days after the insider's departure, another engineer at the organization detected the malicious code. The insider was subsequently arrested. Details regarding the verdict are unavailable.

This case illustrates the need to lock accounts immediately prior to notifying contractors that their services will no longer be needed. The organization must exercise caution once it notifies an employee or contactor of changes in the terms of employment. In this case, the organization should not have permitted the contractor to finish out the workday and should have had him escorted from the company's premises. This case also highlights the need to restrict access to the system backup process. Organizations should implement a clear separation of duties between regular administrators and those responsible for backup and restoration. Regular administrators should not have access to system backup media or the electronic backup processes. The organization should consider restricting backup and restore capabilities to a few select individuals, in order to prevent malicious insiders from destroying backup media and other critical system files and from sabotaging the backup process.

In another case, a government agency employed a contractor as a systems administrator. The contractor was responsible for monitoring critical system servers. Shortly after the contractor started, the organization reprimanded him for frequent tardiness, absences, and unavailability. His supervisor repeatedly warned him that his poor performance was cause for dismissal. The contractor sent threatening and insulting messages to his supervisor. This continued for approximately two weeks, on-site and during work hours. The contractor, who had root access on one server and no root access on another server, used his privileged account to create a file that enabled him to access the second server. Once inside the second server, the contractor inserted malicious code that would delete all of the organization's files when the total data volume reached a certain point. To conceal his activity, the malicious code disabled system logging, removed

history files, and removed all traces of the malicious code after execution. After the contractor was terminated, he repeatedly contacted the system administrators to ask if the machines and servers were functioning properly, which aroused the organization's suspicion. The organization discovered the malicious code and shut down the systems, removed the code, and restored system security and integrity. The contractor did not succeed in deleting the data. He was arrested, convicted, ordered to pay restitution, and sentenced to over one year of imprisonment followed by three years' supervised release. On his job application to the organization, the contractor had failed to report that he had been fired from his previous employer for misusing their computer systems.

Organizations should consider including provisions in contracts with trusted business partners that require the contractor to perform background investigations at a level commensurate with the organization's own policies. In this case, the malicious insider might not have been hired if the contracting company had conducted a background investigation on its employees.

6.4 Quick Wins and High-Impact Solutions

6.4.1 All Organizations

- ☐ Have all employees, contractors, and trusted business partners sign nondisclosure agreements (NDAs) upon hiring and termination of employment or contracts.
- ☐ Ensure each trusted business partner has performed background investigations on all of its employees who will have access to your organization's systems or information. These should be commensurate with your organization's own background investigations and required as a contractual obligation.
- ☐ If your organization is acquiring companies during a merger or acquisition, perform background investigations on all employees to be acquired, at a level commensurate with your organization's policies.
- ☐ Prevent sensitive documents from being printed if they are not required for business purposes. Insiders could take a printout of their own or someone else's sensitive document from a printer, desk, office, or from garbage. Electronic documents can be easier to track.
- ☐ Avoid direct connections with the information systems of trusted business partners if possible. Provide partners with task-related data without providing access to your organization's internal network.
- ☐ Restrict access to the system backup process to only administrators responsible for backup and restoration.

6.4.2 Large Organizations

- ☐ Prohibit personal items in secure areas because they may be used to conceal company property or to copy and store company data.
- ☐ Conduct a risk assessment of all systems to identify critical data, business processes, and mission-critical systems. (See NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems* for guidance [NIST 2002].) Be sure to include insiders and trusted business partners as part of the assessment. (See Section 3.2.1, "Threat-Source Identification," of NIST SP 800-30.)

- ☐ Implement data encryption solutions that encrypt data seamlessly and that restrict encryption tools to authorized users, as well as restrict decryption of organization-encrypted data to authorized users.
- ☐ Implement a clear separation of duties between regular administrators and those responsible for backup and restoration.
- ☐ Forbid regular administrators' access to system backup media or the electronic backup processes.

6.5 Mapping to Standards

- NIST: RA-1(Risk Assessment Policy and Procedures), RA-3 (Risk Assessment), PM-9 (Risk Management Strategy)
- NITTF: B-2, C-6
- Minimum Standards: E-1, G, J
- CERT-RMM:
  - External Dependencies Management
    - [to address trusted business partners, contractors]
  - Human Resources Management
    - [to address internal employees]
  - Access Control and Management
    - [to address authorized access]
- ISO 27002:
  - 6.2.1 Identification of risks related to external parties
  - 6.2.2 Addressing security when dealing with customers

6.2.3 Addressing security in third-party agreements

Practice 7: Be especially vigilant regarding social media.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	

Insiders using social media sites can intentionally or unintentionally threaten the organization's critical assets. Organizations should provide training, policies, and procedures about how employees, business partners, and contractors should use social media.

The recommendations in this best practice are based on malicious insider cases, the *2015 CyberSecurity Watch Survey*[15] results [PWC 2015], and information security analysis of this threat vector. This best practice is also considers findings from the CERT Division's research on unintentional insider threat cases [SEI 2013, 2014; Strozer et al. 2014].

7.1 Protective Measures

Social media sites allow people to easily share information about themselves with others. Information about everything from birthdays and family members to business affiliations and hobbies can all be obtained from a user's social media profile or a search using any popular search engine. This information opens employees who use social media to possible social engineering.

> *Social engineering may be defined as obtaining information or resources from victims using coercion or deceit. During a social engineering attack, attackers do not scan networks, crack passwords using brute force, or exploit software vulnerabilities. Rather, social engineers operate in the social world by manipulating the trust or gullibility of human beings.* [Raman et al. 2009]

Social media sites, such as Facebook and LinkedIn, can be used to determine who works at a particular company. Malicious users could use this information to develop spear phishing email attacks against an organization, in which narrowly targeted, malicious emails are crafted to seem authentic.

These sites can also be used to determine who within an organization may be more susceptible or willing to participate in an insider attack. For example, if an employee participating in a social networking site posts negative comments about his or her job or company, attackers may see this as a sign that the employee is disgruntled and possibly open to participating in a malicious insider attack. Malicious users can also use these sites to map an organization's staff structure and then identify people in high-value roles (C-level executives, financial personnel, etc.) for targeted attacks.

Organizations and individuals alike need to practice good operations security (OPSEC) with social media. What may seem like a simple social media interaction can reveal a lot about an

[15] The *2011 CyberSecurity Watch Survey* was conducted by the United States Secret Service, the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute, *CSO Magazine*, and Deloitte.

individual or organization. For example, an employee who uses an online support forum to troubleshoot a device or software product may unintentionally reveal sensitive organizational information, such as a particular product name and version or IP address.

Social media profiles and web searches can reveal a large amount of personal information, which attackers could use to compromise personal accounts. For example, resetting a user's email password may require answering a few security questions, such as those about place of birth, date of birth, mother's maiden name, ZIP code, name of favorite sports team, or name of hometown. Attackers may find the answers to these questions on social networking sites, making it relatively simple to reset another user's email password. Memorizing and using a bogus legend for hometown, pets, and schools is one way around that vulnerability. However, if this bogus information is consistently used, a vulnerability remains: if attackers compromise the information, they could use it to access data from any other site using that same password-recovery information. To mitigate this risk, social media users could enter bogus password recovery information unique to each site. Password recovery would be more complicated for users of multiple sites, but the password-recovery threat vector would be lessened.

Organizations need policies and procedures to protect against insider threats, unintentional or otherwise. Policies should address what is and is not acceptable employee participation in social media sites.[16] Companies should take into consideration what their employees might post, no matter how harmless it may seem. For example, a policy prohibiting the posting of company projects or even company affiliations may be appropriate because social engineers or competitors could use this information to their advantage.

Every organization needs to include social engineering training in its security awareness training program. This training could include a live demonstration about what types of data can be collected from a randomly selected profile. To avoid embarrassing an employee, the trainer should select the profile of a person not affiliated with the company or use screen captures of an employee's profile with identifying information redacted.

Organizations must ensure the legality of their social media policies. In her third report on the legality of language in employers' social media policies [Purcell 2012], the National Labor Relations Board's Acting General Counsel recommends avoiding policy language that

- prohibits posts discussing the employer's nonpublic information, confidential information, and legal matters (without further clarification of the meaning of these terms)
- prohibits employees from harming the image and integrity of the company; making statements that are detrimental, disparaging, or defamatory to the employer; and prohibiting employees from discussing workplace dissatisfaction
- threatens employees with discipline or criminal prosecution for failing to report violations of an unlawful social media policy

If organizations monitor social media, they must do so with caution. Employers must be careful not to penalize or fire employees for discussing work conditions online, such as pay. Protected speech may even include complaints about supervisors. Another concern is that using social

[16] A list of social media policies and templates are available at http://socialmediagovernance.com/policies.php.

media could inform an organization about certain characteristics of an employee, contractor, business partner, or candidate for a position, such as race, disability, parenthood, or sexual orientation, which could open the door to discrimination lawsuits. Many states have legislated against employers requesting access to an employee's social media password [NCSL 2015]. Maryland was the first state to legislate against employers requesting access to an employee's social media passwords in 2012 [Deschenaux 2012].

7.2 Challenges

1. establishing, monitoring, and enforcing policy—Organizations may find it difficult to control what employees post on social media sites. Training that includes a personal takeaway may help increase awareness and compliance. Organizations will also find it challenging to monitor all social media sources, especially when employees utilize the sites' privacy controls.
2. classifying data—Organizations should have a data classification policy that establishes what protections must be afforded to data of different sensitivity levels. This will require review of the organization's information, and the organization must train all its employees to understand the data classification levels.
3. monitoring social media legally—Organizations must monitor social media with the assistance of legal counsel, if at all. The legal landscape in this area is currently changing, so related policies should be reviewed and changed as needed.

7.3 Case Studies

A security researcher created a fictitious social media profile for a nonexistent, young, female cyber threat analyst at a government defense agency. Relying on her allegedly extensive experience in the information security arena and her list of contacts or friends, she established connections to high-ranking officials in government and defense agencies. Based solely on her online profile, she was even offered jobs, speaking engagements, and dinner engagements. One individual even shared a picture, taken while he was on patrol overseas, which contained embedded geolocation data. Another person had exposed sensitive password-recovery information in his profile, while yet another exposed sensitive personal information. The fictional character established a network of 300 well-connected individuals, some of whom had sensitive job positions and should have known the risks of social media [Waterman 2010].

This story illustrates that many individuals place too much trust in the information they find online. The fake character's credibility began to unravel when a security researcher questioned the credentials of the self-proclaimed security professional. Had the other people who had contact with the fictitious security expert verified her credentials, they might not have fallen victim to this experiment.

In another case, an attacker compromised the email account of a former U.S. vice-presidential candidate. The attacker simply used a search engine to find the answers to the password-recovery questions, which included date of birth, ZIP code, and where she met her spouse, and reset the password. The attacker then read through her email and posted it to a public forum [Zetter 2008].

Organizations should train their employees about the risks of disclosing information online, especially personal information. Disclosing one seemingly harmless piece of information could

lead a potential attacker down a bread-crumb trail of information, enabling the attacker to compromise personal or even corporate accounts and infrastructure.

7.4 Quick Wins and High-Impact Solutions

7.4.1 All Organizations

- ☐ Establish a social media policy that defines acceptable uses of social media and information that should not be discussed online.
- ☐ Include social media awareness training as part of the organization's security awareness training program.
- ☐ Encourage users to report suspicious emails or phone calls to the information security team, who can track these emails to identify any patterns and issue alerts to users.

7.4.2 Large Organizations

- ☐ Consider monitoring the use of social media across the organization, limited to looking in a manner approved by legal counsel for postings by employees, contractors, and business partners.

7.5 Mapping to Standards

- NIST: AT-2, AT-3, PS-1, PS-3
- NITTF: C-1-2
- Minimum Standards: E-1, G-1-a
- CERT-RMM:
  - Monitoring

Practice 8: Structure management and tasks to minimize insider stress and mistakes.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	✓

Organizations must understand the psychology of their workforce and the demands placed upon them by their leadership. Once these are understood, it behooves the organization to create a work environment conducive to positive outcomes.

Human behavior offers many opportunities for mistakes to be made, especially by those rushing to complete multiple tasks in high-stress environments. Beyond mistakes, high levels of stress in the workplace will create ill will and greater potential for malicious activity. This drive for productivity comes at a cost of both efficiency and security. When insiders are rushed they will make more mistakes, feel as if their concerns are not being considered, and potentially develop negative attitudes toward their management and organization. Mistakes can include unintentional disregard or missing of telltale signs of social engineering, overlooking a key security control, or simply speaking before thinking through the repercussions of the information being shared.

8.1 Protective Measures

To reduce the likelihood of malicious and unintentional insider threats, organizations may choose to consider means by which the stress level of employees can be reduced. These may include focusing less on top-line productivity, and more on achieving productive outcomes, instituting policies and practices that provide employees more time to achieve mission oriented objectives, responsive human oriented rather than project-oriented management, and including time in work schedules to focus on planning out tasks or coming up with new ideas of how to do things that benefit the organization.

8.2 Challenges

1. balancing stress level with productivity—Organizations may find it challenging to determine an appropriate level of stress for employees to prevent data leakage while encouraging employees to achieve desired outcomes.
2. baselining employee productivity—Different employees will achieve at varying levels, achieving stressful points at various times and under alternating conditions. It could be difficult for an organization to measure the stress of its entire staff at one time to determine who is overworked, skipping steps, and multi-tasking in an attempt to get the necessary job done.
3. getting a return on investment—Organizations need to weigh the costs and risks of reducing stress and its effect on productivity with the cost of data exfiltration and other forms of malicious insider threat.

8.3 Case Studies

In one of the costliest (and oldest) cases in our corpus, the Chairman of Military Affairs Committee during World War II disclosed confidential military information in a press conference. This information dealt with the depths of Japanese and U.S. subs and attack/evasion strategies. The information was disseminated and publicly disclosed. At the end of the war, the Admiral in charge of submarine operations in that theater of war attributed this disclosure to the loss of 800 servicemen.

In one case, a bank teller fell asleep on the keyboard and accidentally transferred millions of dollars. The teller noted that he had not slept in a long time, and had been overworked.

In another case, a congressional liaison for an oversight entity accidentally emailed a copy of the minutes from a policy meeting to congressional staffers and trade lobbyists. The liaison had been trying to get the minutes out quickly, and did not realize the incorrect e-mail addresses were included in the e-mail.

In a third case, a file cabinet that was sent to a correctional facility for repair contained highly classified documents that were not removed prior to transport. When an inmate was repairing the cabinet, he found the two dozen pages of classified material. It was noted that the cases were never reviewed by anyone before being sent out, as it was a priority simply to get them repaired.

In a fourth case, a high-ranking member of Congress tweeted real-time updates about his location while traveling in a secret congressional convoy in a war zone. It was said that this information was considered confidential. The member of Congress noted that he was simply informing his constituents of his activities.

During a magazine promotion, there was a “coding error” that exposed the personal data of about 12,000 people, including the credit card information of about 50 people. The information of some of these individuals was used by attackers for identity theft. The coders had been rushed to get the coding done to launch the promotion.

In terms of malicious threats induced by stress, two cases paint the picture clearly:

In the first, the insider was employed as a director by the victim organization, a local government entity. The insider had a continually escalating stressful conflict with a government official, resulting in the insider shredding documents from the official's human resources (HR) files. The following day, the insider was caught deleting e-mails from the computer of a subordinate, who observed and reported the previous day’s shredding. Roughly two weeks later, the insider began deleting work-related e-mails and spreadsheets. The insider was terminated some time shortly after the incident and was not prosecuted.

In the second, the insider was employed as a computer engineer by a trusted business partner (TBP) organization, an IT company that managed computer systems for a foreign government, the victim organization. One month prior to the incident, the insider resigned from the TBP. In his resignation letter, the insider expressed that he felt “isolated and stressed due to his physical segregation from the rest of his team.” The insider also stated that he felt he was inappropriately disciplined for the team’s mistakes because he was new to the team. The incident occurred after the insider’s fiancée broke off their engagement and the insider proceeded to get intoxicated. At

the time, the insider was living with a former colleague, who was still employed by the TBP organization. The insider used his colleague's work computer and credentials to open a VPN connection. The insider crashed multiple government servers and deleted 11,000 accounts for government employees at those victim organizations. The incident-related impact was over $1 million. The insider was arrested, convicted, and sentenced to three years' imprisonment. The insider claimed he was trying to expose security vulnerabilities in the government's IT systems.

In all of these cases, what is clear is that the people involved were either stressed, careless, or did not know important operating processes or rules. Many believed that there was a limited timeframe in which to operate. Their actions were induced by high intensity, causing them not to check every action against the simply question of "Should I do this?" Lowering the stress level at organizations, lowering the workload for overburdened employees, and encouraging quality outcomes could have limited, if not eliminated, all of these cases.

8.4 Quick Wins and High-Impact Solutions

8.4.1 All Organizations

- ☐ Establish a work culture that measures success based on appropriate metrics for the work environment. For instance, knowledge workers might measure their success based on outcomes and efficiency instead of metrics that are better suited for a production line.
- ☐ Encourage employees to think through projects, actions, and statements before committing to them.
- ☐ Create an environment that encourages focusing upon one thing at a time, rather than multi-tasking.
- ☐ Offer employees who are under stress options to de-stress, such as massages, time off, games, or other social but non-project oriented activities.
- ☐ Routinely monitor employee workloads to make sure that they are commensurate with the employee's skills and available resources.

8.4.2 Large Organizations

The recommendations in this section apply to all organizations.

8.5 Mapping to Standards

- NIST: AC-5, AC 16-22, CM 1-7, CM 8-10, MP 1-2, PE 2-5, SC-4
- NITTF: C-1-3
- Minimum Standards: G-2, G-4, I-1, I-2, I-3

Practice 9: Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	

Without broad understanding and buy-in from the organization, technical or managerial controls will be short lived. Periodic security training that includes malicious and unintentional insider threat awareness supports a stable culture of security in the organization.

9.1 Protective Measures

All employees need to understand that insider crimes do occur and have severe consequences. In addition, it is important for them to understand that malicious insiders do not fit a particular profile. Their technical abilities have ranged from minimal to advanced, and their ages have ranged from late teens to retirement age. No standard profile exists that can be used to identify a malicious insider. The CERT Insider Threat Center's collection of insider threat cases reveals a wide range of people who have committed crimes, from low-wage earners to executives, and new hires to seasoned company veterans. There is no way to use demographic information to easily identify a potentially malicious insider. However, there are ways to identify higher risk employees and implement mitigation strategies to reduce their impact on the organization should they choose to attack.

The same can be said of the unintentional insider threat. Cases reveal that those who cause harm without malicious intent also fail to fit a particular profile. Their behaviors and technical skills vary drastically.

Security awareness training should encourage employees to identify malicious insiders not by stereotypical characteristics but by their behavior, including

- threatening the organization or bragging about the damage the insider could do to the organization or coworkers
- downloading sensitive or proprietary data within 30 days of resignation
- using the organization's resources for a side business or discussing starting a competing business with co-workers
- attempting to gain employees' passwords or to obtain access through trickery or exploitation of a trusted relationship (often called "social engineering")

Awareness training for the unintentional insider threat should encourage employees to identify potential actions or ways of thinking that could lead to an unintentional event, including

- level of risk tolerance—someone willing to take more risks than the norm
- attempts at multi-tasking—individuals who multi-task may be more likely to make mistakes
- large amounts of personal or proprietary information shared on social media

- lack of attention to detail

Managers and employees should be trained to recognize social networking in which an insider engages other employees to join his or her schemes, particularly to steal or modify information for financial gain. Alerting employees of this possibility and its consequences may make them more aware of such manipulation and may be more likely to report it to management.

Social engineering is often associated with attempts to gain physical or electronic access to an organization's system via accounts and passwords. For example, an attacker who has gained remote access to a system may need to use another employee's account to access a server containing sensitive information. In addition, some cases in the CERT insider threat database reveal that social engineering is sometimes an intermediary step to malicious access or an attempt to obfuscate the malicious insider's activities. Organizations should train their employees to be wary of unusual requests, even ones that do not concern accounts and passwords. This includes social engineering by outsiders in order to gain access to an insider's credentials.

Training programs should create a security culture appropriate for the organization and include all personnel. The training program should be offered at least once a year. In the United States, the month of October is recognized as National Cyber Security Awareness Month [DHS 2011]. The name implies an IT focus, but the CERT Insider Threat Center's studies of insider threat have indicated that vulnerabilities in an organization's business processes are at least as important to cybersecurity as technical vulnerabilities. All of an organization's departments should conduct refresher training that may or may not directly relate to cyber threats. The following are insider threat topics that organizations should consider for inclusion in training:

- Human Resources: Review insider threat policies and the processes that address them, across the organization. This is also a good time to remind employees of the organizations resources available to employees, such as an employee assistance program (EAP).
- Legal: Review insider threat policies and discuss any issues that arose in the past year and how to avoid them in the future.
- Physical Security: Review policies and procedures for access to company facilities by employees, contractors, and trusted business partners. In addition, review any policies on prohibited devices (USB devices, cameras, etc.). This also provides the organization an opportunity to discuss proper handling of the organization's physical assets as well as evacuation or emergency procedures that may arise in the event of an emergency.
- Data Owners: Discuss projects that may have heightened risk of insider threat, for example, strategic research projects that will involve creation of new trade secrets. This topic should show the value of an organization's IP and the potential damage associated with an insider attack. When applicable, insider trading should be thoroughly covered.
- Information Technology: IT can educate employees on procedures for recognizing viruses and other malicious code. This is another opportunity to discuss which devices are prohibited or permitted for authorized use on the various information systems within the organization. IT can coordinate with cybersecurity to conduct phishing campaigns that are designed to educate employees about real phishing attacks.
- Software Engineering: The software engineering team could review the importance of auditing of configuration management logs to detect insertion of malicious code.

To increase the effectiveness and longevity of measures used to secure an organization against insider threats, such measures must be tied to the organization's mission, values, and critical assets, as determined by an enterprise-wide risk assessment. For example, if an organization places a high value on customer service quality, it may view customer information as its most critical asset and focus security on protection of that data. Training on reducing risks to customer service processes would focus on

- protecting computer accounts used in these processes (see Practice 10)
- auditing access to customer records (see Practice 12)
- ensuring consistent enforcement of defined security policies and controls (see Practice 3)
- implementing proper system administration safeguards for critical servers (see Practices 11, 12, 13, and 20)
- using secure backup and recovery methods to ensure availability of customer service data (see Practice 18)

No matter what assets an organization focuses on, it should still train its members to be vigilant against a broad range of unintentional and malicious employee actions, which are covered by a number of key practices:

- detecting and reporting disruptive behavior of employees (see Practice 2)
- monitoring adherence to organizational policies and controls (see Practice 3)
- monitoring and controlling changes to organizational systems (e.g., to prevent the installation of malicious code) (see Practices 14 and 17)
- requiring separation of duties between employees who modify customer accounts and those who approve modifications or issue payments (see Practice 15)
- detecting and reporting violations of the security of the organization's facilities and physical assets (see Practice 3)
- planning for potential incident response proactively (see Practice 2)

The organization should base its security training on documented policy, including a confidential means of reporting security issues. Confidential reporting allows employees to report suspicious events without fear of repercussion, circumventing the cultural barrier against whistle blowing. Employees need to understand that the organization uses established policies and procedures, not arbitrary and personal judgment, and that managers will respond to security issues fairly and promptly.

An organization must notify its employees that it is monitoring system activity, especially system administration and privileged activity. All employees should be trained in their personal security responsibilities, such as protecting their own passwords and work products. Finally, the training should communicate IT acceptable-use policies. Organizations should ensure yearly acknowledgment of the acceptable-use policy or rules of behavior, which can be accomplished at training events.

Employees must be taught that they are responsible for protecting the information the organization has entrusted to them. Malicious individuals, who can be from within the organization or outside of it, may try to take advantage of employees' access. The organization

should regularly remind employees of procedures for anonymously reporting suspicious co-worker behavior or recruitment attempts by individuals inside or outside the organization.

Organizations must educate employees about the confidentiality and integrity of the company's information and that compromises to the information will be dealt with harshly. Sometimes insiders incorrectly believe the information they are responsible for, such as customer information developed by a salesperson or software developed by a programmer, is their own property rather than the company's.

Organizations should consider implementing an information classification system that includes categories of information and defines what protections must be afforded the information. For example, the U.S. government utilizes a classification system that includes Unclassified, Confidential, Secret, and Top Secret information. The government has defined each of these categories and developed procedures for properly handling classified information. Organizations may consider a similar classification system, which could include categories such as Company Public, Company Confidential, and so on. The SANS Institute provides sample policy design guidance at https://www.sans.org/security-resources/policies/. If an organization uses an information classification system, it must train its employees how to use it correctly.

In some insider threat cases, technical employees sold their organization's IP because they were dissatisfied with their pay, or they gave such information to reporters and lawyers because they were dissatisfied with their organization's practices. In cases like these, signs of disgruntlement often appear well before the actual compromise. For this particular threat, clarity about salary expectations and opportunities for career enhancement through training and extra project opportunities can benefit both employee and employer and reduce disgruntlement. Staff trained to recognize warning signs can help mitigate insider threats, possibly preventing malicious acts and stopping or reducing harm to the organization and/or fellow coworkers.

9.2 Challenges

1. managing the training program—Organizations may find it challenging to keep their staff engaged after several iterations of training. Organizations will need to determine how often to train individuals and how to measure the training's effectiveness. It may be difficult to discuss prior incidents without revealing sensitive information.
2. classifying information—Implementing an information classification program will require a lot of time and employee buy-in. Employees must be trained to correctly classify and handle marked documents. Documents will need to be reviewed and marked appropriately, and additional access control protections must be placed on the information.
3. Organizational culture—If the organization has a culture that does not value intellectual property or information security, employees may resist training on malicious or unintentional insider threats. Organizations can work through this by obtaining buy-in from employees, focusing on the employee protection aspect of the program, and considering alternative titles to "Insider Threat Program" such as "Insider Risk Program." Another approach to help employees learn about cybersecurity is to use case studies of past security incidents involving the organization. This can address an employee's attitude or belief that an attack would not occur at the organization and increase one's appreciation for cybersecurity.

9.3 Case Studies

A tax office employed the insider as a manager. The insider had detailed knowledge of the organization's computer systems and helped design the organization's newly implemented computer system. The insider convinced management that her department's activities should be processed outside of this new system. All records for the insider's department were maintained manually, on paper, and were easily manipulated. Over 18 years, the insider issued more than 200 fraudulent checks, totaling millions of dollars. The insider had at least nine accomplices, insiders and outsiders, with unspecified roles in the scheme. One of the insider's external accomplices, her niece, deposited checks into the bank accounts of the fake companies and then distributed the funds to various members of the conspiracy. The incident was detected when a bank teller reported a suspicious check for more than $400,000. The insider was arrested, convicted, and ordered to pay $48 million in restitution, $12 million in federal taxes, and $3.2 million in state taxes. She was also sentenced to 17.5 months of imprisonment. One of the insider's motivations was that she enjoyed acting as a benefactor, giving co-workers money for things like private school tuition, funerals, and clothing. The insider avoided suspicion by telling her co-workers that she had received a substantial family inheritance. The generous insider also spent a substantial amount of money on multiple homes, each valued at several million dollars, luxury cars, designer clothing and accessories, jewelry, and other lavish items. At the time of her arrest, the insider had $8 million in her bank account. The insider apparently endured a traumatic childhood, leading her to abuse drugs and alcohol and develop a substantial gambling habit.

If the organization had provided training on suspicious activities that indicate insider activity, this incident might have been detected earlier. The insider in this case made purchases that were out of reach for others in her position. In addition, the insider abused drugs and alcohol and had a gambling habit. With proper training, the combination of these risk factors might have recognized and reported by an employee, resulting in the organization investigating and identifying the crime.

In another case, a disgruntled employee placed a hardware keystroke logger on a computer at work to capture confidential company information. After the organization fired the insider unexpectedly, the now former employee tried to coerce a nontechnical employee still at the company into recovering the device for him. Although the employee did not know the device was a keystroke logger, she was smart enough to recognize the risk of providing it to him and notified management instead. Forensics revealed that he had removed the device and transferred the keystrokes file to his computer at work at least once before being fired. In this case the employee was wary, correctly, of an unusual request regarding network systems and accounts, including physical access, so the keystroke logger was found. This case shows a great example of the benefits organizations realize when their employees are trained to recognize and be cautious of social engineering.

9.4 Quick Wins and High-Impact Solutions

9.4.1 All Organizations

- ☐ Develop and implement an enterprise-wide training program that discusses various topics related to insider threat. The training program must have the support of senior management to be effective. Management must be seen participating in the course and must not be exempt

from it, which other employees could see as a lack of support and an unequal enforcement of policies.

- ☐ Train all new employees and contractors in security awareness, including insider threat, before giving them access to any computer system. Make sure to include training for employees who may not need to access computer systems daily, such as janitorial and maintenance staff. These users may require a special training program that covers security scenarios they may encounter, such as social engineering, active shooter, and sensitive documents left out in the open.
- ☐ Train employees continuously. However, training does not always need to be classroom instruction. Posters, newsletters, alert emails, and brown-bag lunch programs are all effective training methods. Your organization should consider implementing one or more of these programs to increase security awareness.
- ☐ Establish an anonymous or confidential mechanism for reporting security incidents. Encourage employees to report security issues and consider incentives to reporting by rewarding those who do.

9.4.2 Large Organizations

- ☐ The information security team can conduct periodic inspections by walking through areas of your organization, including workspaces, and identifying security concerns. Your organization should bring security issues to the employee's attention in a calm, nonthreatening manner and in private. Employees spotted doing something good for security, like stopping a person without a badge, should be rewarded. Even a certificate or other item of minimal value goes a long way to improving employee morale and increasing security awareness. Where possible, these rewards should be presented before a group of the employee's peers. This type of program does not have to be administered by the security team but could be delegated to the employee's peer team members or first-level management.

9.5 Mapping to Standards

- NIST: AT-1 (Security Awareness and Training Policy and Procedures), AT-2 (Security Awareness Training), AT-3 (Role-Based Security Training)
- NITTF: C-1-3
- Minimum Standards: I
- CERT-RMM:
  - Organizational Training and Awareness
    - Although the CERT-RMM focuses on resilience, it includes training in areas such as vulnerability management.
- ISO 27002:
  - 8.2.2 Information security awareness, education, and training

Practice 10: Implement strict password and account management policies and practices.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓		✓	✓	

Strict password and account management policies and practices can prevent malicious insiders from compromising an organization's user accounts to circumvent manual and automated control mechanisms.

10.1 Protective Measures

No matter how vigilant an organization is against insider threat, if the organization's user accounts can be compromised, insiders have an opportunity to circumvent attack prevention mechanisms. User account and password management policies and practices are critical to impeding an insider's ability to use the organization's systems for illicit purposes. Fine-grained access control combined with proper computer account management will ensure that access to all of the organization's critical electronic assets is attributed to individual employees.

The following methods are just some of the ways malicious insiders have compromised accounts:

- obtaining passwords through social engineering or because employees openly shared passwords
- obtaining passwords stored by employees in clear-text files on their computer or in email
- obtaining passwords left on sticky notes or paper left in plain sight or easily accessible places (under keyboard, phone, or mouse pad; in an address book; etc.)
- using an unattended computer whose user is still logged in
- using password crackers
- using keystroke loggers
- watching while a user types in his or her password, also known as "shoulder surfing"

Password policies and procedures should ensure that all passwords are strong,[17] employees do not share their passwords with anyone, employees change their passwords regularly, employees lock their console before stepping away from it, and all computers automatically execute password-protected screen savers after a fixed period of inactivity. Additionally, security training should instruct users to block visual access to their screens as they type their passcodes.

Organizations should use shared accounts only when absolutely necessary. Often, organizations use these accounts out of administrative convenience, rather than out of necessity. Simple shared accounts abrogate definitive attribution of actions, which is required in some cases by regulations and important for investigations. To minimize risks and improve regulatory compliance,

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

organizations should consider using shared account password management (SAPM) tools that automate processes and enforce controls for remaining shared accounts. Combined, these steps reduce the likelihood of a malicious insider performing an attack in a non-attributable way. In addition, employees should report all attempts or suspected attempts of unauthorized account access to the organization's help desk or information security team.

Some insiders have created backdoor accounts that provide them with system administrator or privileged access following termination. Other insiders found that shared accounts were overlooked in the termination process and were still available to them after they were terminated. They commonly used system administrator accounts and database administrator accounts. Some insiders have used other types of shared accounts, including those set up for access by external partners such as contractors and vendors. One insider also used training accounts that the organization used repeatedly without changing the password. Systems used by non-employees should be isolated from other organizational systems, and accounts should not be replicated across these systems. In addition, organizations should carefully consider the risks of issuing guest accounts to visitors.

Periodic account audits combined with technical controls allow organizations to identify

- backdoor accounts that could be used later for malicious insider actions, whether those accounts were specifically set up by the insider or left over from a previous employee
- shared accounts whose password was known by the insider and not changed upon the insider's termination or reassignment to another position within the company
- accounts created for external partners, such as contractors and vendors, whose passwords were known to certain insiders and not changed upon any of those insiders' termination or reassignment
- password resets performed in excess by administrators or for infrequently used accounts

Account management policies that include strict documentation of all access privileges for all users enable a straightforward termination procedure that reduces the risk of attack by terminated employees. Organizations should periodically re-evaluate the need for every account and retain only those that are absolutely necessary. Strict procedures and technical controls should be implemented that enable auditors or investigators to trace all online activity on those accounts to an individual user. These limits, procedures, and controls diminish an insider's ability to conduct malicious activity without being identified. Organizations using centralized account management systems, such as the Lightweight Directory Access Protocol (LDAP) Directory Services, for authentication may reduce the risk of overlooking an account during termination or during a periodic audit.

An organization's password and account management policies must also apply to all contractors, subcontractors, and vendors who have access to the organization's information systems or networks. These policies should be written into contracting agreements and require the same level of access accountability as for the organization's own employees. Every account must be attributable to an individual. Contractors, subcontractors, and vendors should not be granted shared accounts for access to organizational information systems. They should not be permitted to share passwords, and when they terminate employees, they must notify the contracting organization in advance so it can change account passwords or close the account. The contract should require notification within a reasonable timeframe if advance notification is not possible.

Finally, the contracting organization must include contractor, subcontractor, and vendor accounts in its regularly scheduled password change process.

10.2 Challenges

1. balancing risk and business processes—Finer grained access controls, account management, and other account security measures may incur tradeoffs and costs associated with business inefficiencies.
2. managing accounts—Organizations with large numbers of distributed user workstations may find it challenging to manage local accounts.

10.3 Case Studies

The insider, a contractor, was formerly employed as a software developer and tester by the victim organization. The organization terminated the insider for poor performance but failed to change a shared account password upon his departure. The insider used the company laptop assigned to him by his subsequent employer, a noncompeting organization, to remotely access 24 of the victim organization's user accounts. The insider ignored banner warnings indicating that unauthorized access or attempted access was a criminal violation, the computer system was subject to audit, and federal laws provided penalties for unauthorized use. An employee at the victim organization discovered that her user name had been used to log on to her computer just a few hours earlier when in fact she had not logged on, prompting a cooperative investigation by both the insider's current and previous employers. Security personnel at the insider's current employer traced the intrusions to the insider's laptop and confronted him. The insider made several claims, including that he had logged on only to check on a program he wrote; that he had not been fired from the victim organization, but rather he had not had his contract renewed; that a former co-worker had asked him to log on to help with a problem; and that he had been playing a break-in game with his former co-workers to find flaws in the victim organization's network. The insider was arrested, convicted, and sentenced to two concurrent two-year terms of probation, as well as unspecified fines and penalties. The insider exploited 13 systems storing trade secrets valued at approximately $1.3 million.

Many other cases in our corpus involve insiders who log into systems using shared passwords that were not changed upon the insiders' termination. Organizations should have proper account management practices and identify all shared accounts. Whenever an individual leaves an organization, the organization should use this record to identify the accounts the individual could access and to change the passwords.

A third example is an e-commerce company that employed an insider as a chief project engineer. The organization removed the insider from a major project and subsequently terminated his employment. Afterward, the insider's accomplice, an employee of the victim organization, allegedly gave the insider the password to the server storing the project he had worked on. According to some sources, the insider wanted to delete the project file for revenge. Other sources claim that the insider wanted to hide the file during a presentation so that his accomplice could recover the file, appear to be a hero, and avoid being fired. The insider did delete the file, but the organization was able to recover the lost data. The project was valued at $2.6 million. The insider and his accomplice were arrested. The insider was found not guilty.

In a fourth case, an accomplice shared an account password with a former employee, who used it to access and delete company data. An organization's password policy should state that account information is not to be shared with anyone outside of the organization and should outline consequences for violations. In this case example, such a policy may have deterred the activities of the insider and his accomplice.

10.4 Quick Wins and High-Impact Solutions

10.4.1 All Organizations

- ☐ Establish account management policies and procedures for all accounts created on all information systems. These policies should address how accounts are created, reviewed, and terminated. In addition, the policy should address who authorizes the account and what data they can access.
- ☐ Perform audits of account creation and password changes by system administrators. The account management process should include creation of a trouble ticket by the help desk. (Help desk staff should not be able to create accounts.) Your organization could confirm the legitimacy of requests to reset passwords or create accounts by correlating such requests with help desk logs.
- ☐ Define password requirements and train users on creating strong passwords. Some systems may tolerate long passwords. Encourage users to use passphrases that include proper punctuation and capitalization, thereby increasing passphrase strength and making it more memorable to the user.
- ☐ Security training should include instruction to block visual access to others as users type their passcodes.
- ☐ Ensure all shared accounts are absolutely necessary and are addressed in a risk management decision.

10.4.2 Large Organizations

- ☐ Review systems and risk to determine the feasibility of centrally managing user accounts.
- ☐ If using a central account management system, add contractors to groups linked to projects, organizations, or other logical groups. This allows administrators to quickly identify contractors and change access permissions. Accounts themselves might contain contractor status tipoffs, for example, putting "CONT" in the account name or description.

10.5 Mapping to Standards

- NIST: AC-2 (Account Management), IA-2 (Identification and Authentication (Organizational Users)
- NITTF: B-7, C-1-4
- Minimum Standards: G-1-b
- CERT-RMM:
  - Identity/Access Management
- ISO 27002:
  - 11.2.3 User password management

- 11.2.4 Review of user access rights

Practice 11: Institute stringent access controls and monitoring policies on privileged users.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓			✓	✓

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

11.1 Protective Measures

According to the CERT Insider Threat Center's research, a majority of the insiders who committed sabotage and more than half of those who stole confidential or proprietary information held technical positions at the victim organizations. Technically sophisticated methods of carrying out and concealing malicious activity have included

- writing or downloading scripts or programs (including logic bombs)
- creating backdoor accounts
- installing remote system administration tools
- modifying system logs
- planting viruses
- using password crackers

However, of the 50 cases studied for the recent CERT Insider Threat Center report *An Analysis of Technical Observations in Insider Theft of Intellectual Property*, only six contained clear information about the insider's concealment methods [Hanley et al. 2011a]. Stringent access controls and monitoring policies on privileged users might have detected concealment methods, but they might also have prevented the attacks or reduced the damage they caused.

By definition, system administrators and privileged users[18] have greater access to systems, networks, or applications than other users. Privileged users pose an increased risk because they

- have the technical ability and access to perform actions that ordinary users cannot
- can usually conceal their actions by using their privileged access to log in as other users, modify system log files, or falsify audit logs and monitoring reports
- typically have oversight of and approval responsibility for change requests to applications or systems, even when their organizations enforce technical separation of duties

Organizations can configure systems and networks to facilitate nonrepudiation by using certain policies, practices, and technologies. Should malicious insider activity occur, nonrepudiation

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

techniques allow each and every online activity to be attributed to a single employee, no matter the employee's level of access? However, those measures are designed, created, and implemented by system administrators and other privileged users. To prevent any one privileged user from building in ways to circumvent nonrepudiation measures, multiple privileged users should create, implement, and enforce network, system, and application security designs. In addition, the organization's information security team should regularly review privileged activity.

Organizations should consider having privileged users sign a privileged user agreement or rules of behavior[19] outlining what is required of them, including what they are and are not permitted to do with accounts they can access. Such agreements help instill the responsibilities of elevated access in privileged users. Monitoring technologies and policies must be lawful, and organizations should consult legal counsel before implementing them.

Though user activity monitoring tools have advanced significantly since the last publication of the *Common Sense Guide*, organizations must learn about and fully understand the limitations of the tools. While the practices discussed above facilitate identification of users following detection of suspicious activity, organizations must take additional steps to defend against malicious actions before they occur. For instance, system administrators and privileged users have access to all computer files within their domains. Users can encrypt files with private keys and passwords to prevent unauthorized access by privileged administrators who do not need to access the data. However, access to encryption tools also poses a risk: a malicious insider could encrypt company information and refuse to provide the key. Organizations should evaluate encryption solutions, and how they might impact user activity monitoring, before allowing their use.

Policies, procedures, and technical controls should enforce separation of duties and require actions by multiple users to release any modifications to critical systems, networks, applications, and data. In a software development scenario, no single user should be permitted or be technically able to release changes to the production environment without action by at least one other user. For example, a developer should have a peer review her code before giving it to someone else for deployment.

To enforce separation of duties for system administration functions, the organization must employ at least two system administrators. Small organizations that cannot afford to employ more than one system administrator must recognize their increased risk. Several cases cited in this guide involve an organization victimized by its sole system administrator. In organizations that can only afford one system administrator, some methods can be used to separate the auditing role out from the single administrator. For example, organizations can make log information available to non-technical managers, independent audit reviews, or investigations. To achieve effective separation of duties, any such method must assure that the system administrator has no control over the auditing function. For more on separation of duties, see Practice 15: "Enforce separation of duties and least privilege."

Finally, many of the insiders in the CERT insider threat database, especially those who engaged in IT sabotage, were former employees of the victim organizations. Organizations must be especially

[19] A good example of privileged user rules of behavior is available at http://trainingcenter.nih.gov/pdf/lms/OPM_Rules_of_Behavior_form.pdf

careful to disable system access to former system administrators and technical or privileged users. Thoroughly documented procedures for disabling access can help ensure that an organization does not overlook stray access points. In addition, organizations should consider implementing the two-person rule (which requires two people to participate in a task in order for it to be executed successfully) for the critical functions performed by these users, to reduce the risk of extortion after they leave the organization.[20]

11.2 Challenges

1. justifying payroll costs—It may be difficult for organizations to justify the cost of additional staff needed to implement separation of duties and access control restrictions.
2. engendering trust—The organization must ensure that system administrators and other privileged users feel trusted by the organization.

11.3 Case Studies

The victim organization, which was responsible for managing prescription benefit plans, employed the insider as a computer systems administrator. Following the victim organization's spin-off from its parent company, its staff, including the insider, circulated emails discussing the anticipated layoffs of the victim organization's computer systems administrators. The insider, fearing he would be laid off, created a logic bomb by modifying existing computer code and inserting new code into the victim organization's servers. Even after the layoffs occurred and the insider retained his employment, he did not remove the logic bomb. When the logic bomb failed to detonate on the intended day, the insider modified the logic bomb to correct the error. Another computer systems administrator discovered the logic bomb while investigating a system error. IT security personnel subsequently neutralized the destructive code. The logic bomb would have destroyed information on more than 70 servers, including a critical database of patient-specific drug interaction conflicts; applications relating to clients' clinical analyses, rebate applications, billing, and managed care processing; new prescription call-ins from doctors; coverage determination applications; and numerous internal applications, including corporate financials, pharmacy maintenance tracking, web and pharmacy statistics reporting, and employee payroll input. The incident spanned a year and two months from the creation of the logic bomb to its detection. The insider was arrested, convicted, ordered to pay over $75,000 in restitution, and sentenced to 30 months of imprisonment.

In another case, an IT company employed the insider as an IT administrator. The insider was dating another employee, who was fired. The insider sent threatening messages to management demanding they rehire the employee. The organization fired the insider for this behavior. Before the organization revoked the insider's access, he created another user account. During this time, the insider also deleted a customer's files. After terminating the insider, the IT company refused to help him with an unemployment compensation claim. The insider, using the backdoor account he had previously created, accessed one of the organization's servers several times, sometimes using his home network and sometimes using public networks. The insider deleted the data of two customers and made it difficult for one of the customers to access the company's server. The IT

[20] See Practice 15, "Enforce separation of duties and least privilege."

company contacted a government agency to help with its investigation, which identified the insider by the user account and logs. The insider was arrested and pleaded guilty to computer intrusion.

In both of these cases, the insiders were able to make changes to the system without verification. In the first case, the insider planted a logic bomb in a production system. In the second case, the insider was able to create an account without permission or verification. Had appropriate monitoring and access controls been in place, the insiders' activities may have been stopped or detected earlier.

Such controls would also have been effective in another case, this one against a foreign investment trader who manipulated source code. This insider had a degree in computer science, so the victim organization gave him access to its trading system's source code. He used that access to build in a back door that enabled him to hide trading losses, without detection, totaling nearly $700 million over several years.

11.4 Quick Wins and High-Impact Solutions

11.4.1 All Organizations

☐ Conduct periodic account reviews to avoid privilege creep. Employees should have sufficient access rights to perform their everyday duties. When an employee changes roles, the organization should review the employee's account and rescind permissions that the employee no longer needs.

11.4.2 Large Organizations

☐ Implement separation of duties for all roles that affect the production system. Require at least two people to perform any action that may alter the system.

☐ Use multifactor authentication for privileged user or system administrator accounts.[21] Requiring multifactor authentication will reduce the risk of a user abusing privileged access after an administrator leaves your organization, and the increased accountability of multifactor authentication may inhibit some currently employed, privileged users from committing acts of malfeasance. Assuming that the former employee's multifactor authentication mechanisms have been recovered, the account(s) will be unusable.

11.5 Mapping to Standards

- NIST: AC-2, AC-6, AC-17, AU-2, AU-3, AU-6, AU-9, CM-5, IA-2, MA-5, PL-4, SA-5
- NITTF: C-1-1
- Minimum Standards: H-1
- CERT-RMM:
  - Identity/Access Management
  - Monitoring

[21] NIST Special Publication 800-53, AC-6 (Access Control) requires multifactor authentication for moderate- to high-risk systems.

- ISO 27002:
  - 10.10.4 Administrator and operator logs
  - 10.10.2 Monitoring system use

Practice 12: Deploy solutions for monitoring employee actions and correlating information from multiple data sources.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	

Effective insider threat programs collect and analyze information from many different sources across their organizations. Simply logging all network activity is not sufficient to protect an organization from malicious insider activity. As the number of data sources used for insider threat analysis increases, so too does an organization's ability to produce more relevant alerts and make better informed decisions regarding potential insider activity. The volume of data that must be collected, aggregated, correlated, and analyzed drives the need for tools that can fuse data from disparate sources into an environment where alerts can be developed that identify actions indicative of potential insider activity. Solutions for monitoring employee actions should be implemented using a risk-based approach and focusing first on the organization's critical assets.

12.1 Protective Measures

User activity can be monitored at two levels: at the network and at the host. Many actions performed on computers involve network communications, often allowing network-based analysis to provide a sufficient view into user activity. The volume of information necessary for network-based monitoring is often much less than is required for collecting host-based logs and other information from every system on the network. Insider-threat-related activity identifiable through network analysis can include authentication, access to sensitive files, unauthorized software installations, web browsing activity, email/chat, printing, and many others. However, there are some actions the organization may be interested in monitoring that do not leave any traces on the network. These can include copying local files to removable media, local privilege escalation attempts, and many others. These actions can be monitored through host-based log collection as well as through host-based monitoring systems.

One of the most powerful tools an organization can use to perform event correlation is a security information and event management (SIEM) solution. SIEM tools are designed to provide a centralized view of a wide array of logs from sources including databases, applications, networks, and servers. SIEM tools provide the ability to write queries or generate alerts that pull together data from previously disparate data sources, enhancing potential analytic capabilities for insider threat prevention, detection, and response.

A SIEM system allows an organization to continuously monitor employee actions. This further allows the organization to establish a baseline level of normal activity as well as detect irregular events. Organizations can use a SIEM system to conduct more granular monitoring of privileged accounts. The SIEM system should be able to highlight events related to any actions a normal user cannot perform, such as installing software or disabling security software. Increasing the auditing level for certain events will create additional audit records that must be reviewed. The SIEM

system will facilitate sorting through these events by highlighting those that need further review and discarding background noise.

Organizations can also use a SIEM system for enhanced monitoring. This is especially important for employees who are leaving the organization or who have violated or are suspected of violating organizational policy. Based on the CERT Insider Threat Center's research and feedback from industry, malicious insiders often conduct illicit activities within 90 days of their termination. When an employee submits his or her resignation, the HR team should notify the insider threat program who should then notify the information assurance (IA) team so that its staff may review the employee's actions over at least the past 90 days and going forward to detect potential insider activity. HR should also alert IA if an employee is reprimanded or counseled for violating a work policy. Ideally, the communication between HR and IA should take place between representatives from each division working in the insider threat program. The insider threat program provides a way to quickly and seamlessly respond to insider incidents by including representation from all key stakeholders within an organization.

SIEM tools are not limited to information security events. Physical security events should also be sent to the SIEM system for analysis, creating a more complete set of events to detect insider activity. For example, if an organization sends employee badge access records to a SIEM system, it would be possible to detect unauthorized account usage by checking to see if an employee who is logged into a workstation locally is physically present within the facility. This same method could also be used to detect unauthorized remote access if an employee is physically in the facility. It would also be possible to detect after-hours physical access and correlate it with logical access logs. It should be noted that many alerts, triggers, and indicators will be organization specific. Successful insider threat indicator development depends on an understanding of the organization's culture and behavioral norms.

Successful implementation of an analytic capability for insider threat depends on knowing what data to collect. There are numerous data sources found in many organizations that are recommended for consideration into an insider threat analytic capability. Table 4 provides a listing of these data sources, and a brief description of each data source and the types of analysis that each data source supports.

Table 4: Description of Data Sources for Insider Threat Analysis

Data Source Name	Description
Account Creation Logs	Account creation logs can be correlated with information from human resources systems and help desk ticket system logs to identify suspicious or unauthorized account creation events.
Active Directory Logs	Active Directory logs can assist with entity resolution by being used to identify multiple accounts that are associated with the same user.
Antivirus Logs	Logs from host-based antivirus can be used to detect unauthorized or malicious software on users' workstations and attempts to circumvent host-based controls.
Application Logs	Applications produce logs that can provide insight into user behavior and information access.
Authentication Logs	Login/logout logs can provide information on user activity, and invalid login attempts can point to users attempting to access information that is out of scope for their job roles or attempts to masquerade as another user.

Data Source Name	Description
Chat Logs	Analyzing communication between coworkers can help identify potentially malicious activity and provide insight into employees' concerning personality traits.
Configuration Change Logs	Logs of changes to network devices and other resources should be analyzed and correlated with other data sources to identify unauthorized configuration changes.
Data Loss Prevention Logs	DLP systems can identify when critical information traverses the network.
DNS Logs	DNS can be used to efficiently analyze what services and websites employees are accessing on the Internet.
Email Logs	Email logs can be used to identify concerning communication, particularly with competitors. They can also identify data exfiltration, and can be used to provide insight into employees' concerning personality traits.
File Access Logs	File Access information can be used to identify unusual or concerning access to critical information.
Firewall Logs	Firewall logs can be used to analyze network traffic and identify when employees are attempting to access unauthorized resources on the network or the Internet.
Help Desk Ticket System Logs	Help desk ticket system logs can be used alongside application logs and configuration change monitoring logs to identify unauthorized activity performed by system administrators.
HTTP/SSL Proxy Logs	Analysis of web activity can be used to identify users visiting concerning websites and aid in the detection of data exfiltration via web-based services such as webmail or cloud-based file upload sites.
Intrusion Dection / Prevention Logs	IDS/IPS may detect malicious insider activity, as many of the technical actions are the same as the external actions these systems are designed to detect.
Mobile Device Manager Logs	Logs from mobile device managers can be used to identify users attempting to circumvent security controls and using their mobile devices to exfiltrate data.
Network Monitoring Logs	Malicious insider activity can often be observable in unusual network traffic, such as abnormal traffic spikes or other anomalous network traffic.
Network Packet Tags	Tagging network packets can allow analysts to quickly identify important information about the source of traffic, and can be used to identify traffic originating from unauthorized devices or software.
Permission Change Monitor Logs	Unexplained permission changes to accounts can be indicative of an insider attempting to access information or resources outside of need-to-know.
Printer / Copier / Scanner / Fax Logs	These common exfiltation methods should be monitored for unusual activity, and can be correlated against several other listed data sources that can provide context for a given action.
Removable Media Manager Logs	Removable media is a common exfiltration method, and logs should be monitored for copying of sensitive information and violations of policy.
Telephone Logs	Telephone logs can be used to identify suspicious communication with foreign parties or competitors.
User Activity Monitoring Logs	Alerts from UAM tools can be supplemented with contextual information from many other listed data sources to more efficiently identify false positives and better inform next steps in the analysis process.
VPN Logs	VPN logs can be analyzed to identify unusual access and can be correlated with other sources such as physical access logs to identify suspicious network access.

Data Source Name	Description
Wireless Spectrum Monitor Logs	Rogue wireless access points are a common method for circumventing normal network border controls to access and exfiltrate data from the internal network, and can be detected through regular monitoring of the wireless spectrum.
Anonymous Reporting	Leads from anonymous reporting should be followed up on, as it is a useful way to identify potentially malicious insiders based on observed suspicious behavior.
Asset Management Logs	Movement of critical assets should be reviewed and analyzed for suspicious activity.
AUP Violation Records	Violations of acceptable use policies could be part of malicious activity or point to rule-breakers who may be more likely to commit malicious actions.
Background Investigations	Background investigation results can provide useful context about an employee to help the insider threat team gain a “whole-person” perspective.
Conflict of Interest Reporting	A user’s conflict of interest reports can be correlated against their communication activity and resource access activity to identify unreported conflicts of interest.
Corporate Credit Card Records	This data is useful in anomaly detection as well as allegation resolution. This data may also reveal unreported or unauthorized travel.
Disciplinary Records	Disciplinary records can help the insider threat team identify problem employees who may merit enhanced monitoring.
Foreign Contacts Reporting	Lists of foreign contacts can be correlated against a user’s communication activity to identify potentially unreported foreign contacts.
IP Policy Violation Records	Violations of IP policies could be part of malicious activity or point to rule-breakers who may be more likely to commit malicious actions.
Performance Evaluations	Performance evaluations can provide useful context about an employee to help the insider threat team gain a “whole-person” perspective. This data source can also be used to identify significant changes in employee performance.
Personnel Records	Personnel records including information on employee’s job titles, supervisors, promotions, and discpline history
Physical Access Records	This data can be correlated with other sources for anomaly detection, and can be used to identify unusual work hours.
Physical Security Violation Reports	Violations of physical security policies could be part of malicious activity or point to rule-breakers who may be more likely to commit malicious actions.
Security Clearance Records	Security clearance records can provide useful context about an employee to help the insider threat team gain a “whole-person” perspective.
Travel Reporting	Travel information can be correlated with other data sources to identify anomolous or suspicious behavior.

This list of data sources is not comprehensive enough to completely prevent or detect all insider threats in all organizations. Some organizations may not collect all the listed data, and some organizations have different data sources available that provide additional information on employees and critical assets. Incorporating all of the listed data sources into an analytic capability is a significant technical challenge, even with the assistance of SIEM tools. In the face of limited resources, organizations must know their critical assets (see Best Practice 1: “Know and protect your critical assets”), understand what types of actions those critical assets are susceptible to, and prioritize the incorporation of data sources based on each source’s applicability to analysis that predicts or detects those actions. Figure 5 provides a consolidated view of the list of

recommended data sources for inclusion in an analytic capability for insider threat detection, prevention, and response.

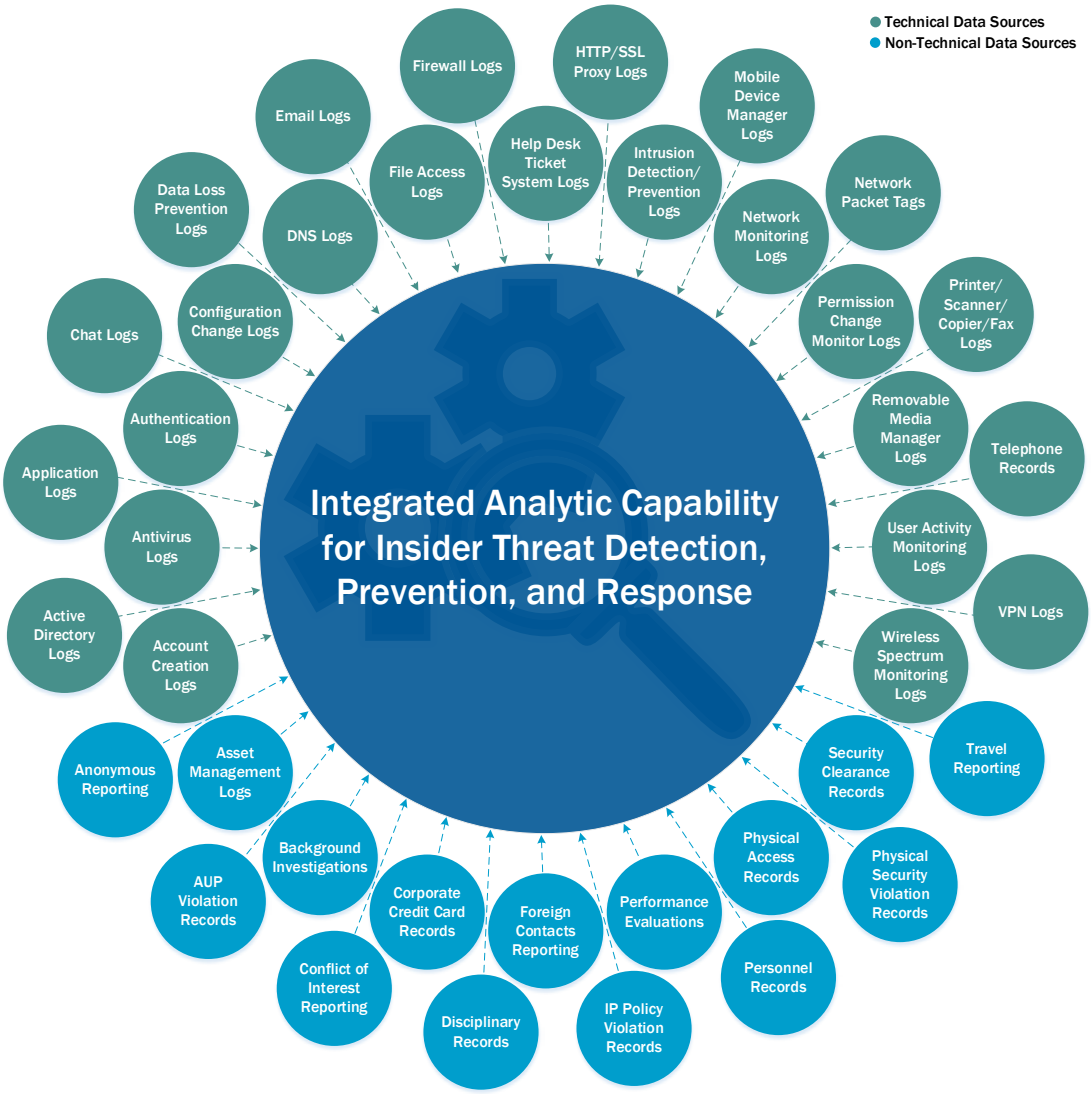

Figure 5: An Integrated Analytic Capability for Insider Threat Detection, Prevention, and Response

Organizations should create monitoring policies and procedures before institutionalizing any monitoring program. Employees should be informed that their use of any information system is monitored. This is typically done through logon banners and security awareness training provided to users before using a system and through annual refreshers. Organizations should consult legal counsel before implementing any monitoring program to ensure they meet all legal requirements and disclosures.

12.2 Challenges

1. false positives—Organizations should tune their SIEM system to reduce the number of false positives. Organizations may find it best to tune the individual devices sending events to the SIEM system.

2. establishing a baseline—The organization should determine normal user behavior in addition to distinguishing anomalies from true threats.
3. accessing information—Various departments from across the organization must work together to determine what information will be collected and who has permission to review the alerts.

12.3 Case Studies

In one case, a help desk technician at a large telecommunications firm installed hacking tools in his company-assigned computer, stole other employees' credentials, and passed those credentials on to an external conspirator who used them to gain unauthorized access to the company's website, which he defaced. This caused significant damage to the organization's reputation and subsequent loss of customers and market share. The organization discovered the insider's installation of hacking tools in his system, demoted him, and imposed policy restrictions that forbade him from accessing the Internet from his office. However, the company did not implement these restrictions at a technical level, allowing him to continue to access the Internet and email using an expired customer account. The insider used instant messaging to threaten a co-worker who was cooperating with the investigation. Moreover, the company failed to correlate the many events pointing to the insider's malfeasance because it lacked a log correlation or SIEM capability. Access logs eventually connected the insider and outsider to the incident.

In another case, an insider disabled the antivirus application in his organization's system, installed malware, used that malware to gain unauthorized access to his supervisor's system, and planted a logic bomb in a critical server. In this case, if the organization had implemented proper auditing and utilized an IDS/IPS system, various security events should have triggered alerts: disabling the antivirus application, anomalous traffic passing through an IDS sensor, and installing a logic bomb. As it was, the organization did not consider these isolated security events worthy of further inspection and failed to respond to any of them. Correlating these events would have painted a far more sinister picture of this insider's activities, and a SIEM system would have been able to generate a high-priority alert that would have demanded immediate attention.

12.4 Quick Wins and High-Impact Solutions

12.4.1 All Organizations

- ☐ Implement rules within the SIEM system, to automate alerts.
- ☐ Create log management policy and procedures. Ensure they address log retention (consult legal counsel for specific requirements), what logs to collect, and who manages the logging systems.

12.4.2 Large Organizations

- ☐ Ensure that someone regularly monitors the SIEM system. Depending on the environment, this may involve multiple personnel who monitor employee activity full-time.

12.5 Mapping to Standards

- NIST: AU-1, AU-2, AU-6, AU-7, AU-8, AU-12

- NITTF: C-1-1, C-1-2, C-1-4
- Minimum Standards: H-1
- CERT-RMM:
  - Monitoring

Practice 13: Monitor and control remote access from all end points, including mobile devices.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
			✓	✓	

Remote access provides a tempting opportunity for insiders to attack with less perceived risk. Organizations have been moving toward a mobile workforce, enabling employees essentially to work from anywhere a data connection exists. This has also allowed more users to telecommute and use additional technologies, such as smartphones and tablet computers, to remotely access corporate information systems. Organizations must be aware of the remote access technologies used by their employees and what potential threats they pose to organizational systems and data.

Mobile devices are not new to organizations, which have relied on them for quick access to corporate email or sensitive company information while on the go. However, the CERT Insider Threat Center sees mobile devices as an emerging attack platform for malicious insiders. Traditionally, organizations have restricted, or simply have chosen not to adopt, mobile devices in the enterprise. However, with more employees demanding to use a device of their choosing [Hamblen 2011], the risk of malicious insider activity may increase. The CERT Insider Threat Center will continue to monitor insider threat cases that involve mobile devices, and organizations should consider the risks these devices pose and include them as part of an enterprise risk assessment.

13.1 Protective Measures

Insiders often attack organizations remotely, either while employed or after termination, using legitimate access provided by the organization. While remote access can greatly enhance employee productivity, remote access to critical data, processes, or information systems must be given with caution. Insiders have admitted that it is easier to conduct malicious activities from home because it eliminates the concern of a co-worker physically observing the malicious acts.

The inherent vulnerabilities in remote access suggest that organizations should build multiple layers of defense against remote attack. Organizations may provide remote access to email and noncritical data, but they should strongly consider limiting remote access to the most critical data and functions and permitting remote access only from devices that are administered by the organization. As much as possible, access to data or functions that could inflict major damage to the company should be limited to employees physically located inside the workplace. Remote system administrator access should be limited to the smallest group practicable, if not prohibited altogether. Organizations that are unable to furnish organizationally owned equipment to teleworkers should consider restricting access to company systems by using an application gateway. These devices act as a launching pad into the corporate network, often through a secured terminal service or remote desktop session.

Smartphones and other mobile devices now have the ability to place many of the same functions of a desktop computer into the palm of your hand. Whether the organization or the employee owns these devices, organizations should be aware of their capabilities and how they are used in the enterprise. The organization should include mobile devices in their risk assessment and consider some specific features:

- cameras
- microphones
- remote access
- applications
- wireless capabilities (Wi-Fi, Bluetooth, cellular, WiMax, etc.)
- mass storage capabilities

Mobile devices can be used to exfiltrate data. Many phones today have integrated cameras and microphones that could be used to capture sensitive company information, such as architectural drawings, trade secrets, or confidential discussions. Pictures can either be stored on the phone or immediately sent from the device via email or Multimedia Messaging Service (MMS). These devices can also sync their data immediately to cloud storage, social media services, or personal computers outside administrative control of the organization.[22] These devices also allow for remote management of organizational assets with applications available that allow for remote management of servers, workstations, and network infrastructure devices. Some applications allow remote access to the user's desktop. To allow this usage, the organization should have a justifiable business need, usage policies and procedures, and careful monitoring practices. Legal counsel should review any monitoring policies before a monitoring program is implemented.

Organizations should be aware of who has these types of applications installed and who can access the device and the associated services. When an employee leaves the organization, the organization must disable the employee's access to these applications. If the organization's data is on an employee's phone (such as e-mail), the organization should set up an agreement to require employees to give the organization the capability to remotely erase the device in the case it is lost, stolen, or upon termination.

Organizations also need to carefully weigh the risks of allowing personally owned devices to connect to the enterprise network. Company-owned equipment allows the organization to control how the device is used and managed, often through a mobile device management server. Organizations must be aware of the applications installed on the device and how they may introduce vulnerabilities into the organization. As Hurlburt, Voas, and Miller put it [Hurlburt et al. 2011],

> *Is mobile app software general-purpose, or could it lead to loss of life or financial problems? The answer is both. Software of any level of criticality or any type of functionality can be developed for handhelds. Direct access to hardware on these devices—such as cameras and microphones—add to the diversity of potential apps but can also add security risks. Moreover, access to the Internet and remote GPS satellites further add to the variety of*

[22] Note that data spillage and incident response become more challenging due to the multitude of possible synchronized storage locations, which is beyond the scope of this document.

features and potential for threat exploitation available on mobile devices. There's no question that the concept of trust should become more central in the mobile apps world.

For example, a malicious insider could use applications designed for penetration testing to compromise the security of an information system. Organizations should investigate enterprise-controlled "app stores" or other commercially available mobile device configuration management technologies that offer the ability to control device configurations, including applications that are approved for installation.

Some smartphones can "tether," or use the cellular phone network to access the Internet or allow VPN access to the corporate network via a laptop or other device. These functions allow telecommuters to access information on the go; however, they are entry points into the corporate network that need to be monitored and controlled. If users can use tethering to bridge their trusted, corporate connection with an untrusted, tethered connection, then they could completely bypass all enterprise network security by directing their illicit activity through the unmonitored connection. Furthermore, these devices may create back doors into the system by introducing an unknown network connection to a computer. Insiders may be able to take otherwise air-gapped computers online via tethering. In one case example, an insider left a rogue modem attached to company equipment in order to dial in and perform administrative tasks. Using current technology, it is conceivable that a tethered smartphone could be used to accomplish the same objective.

Insiders could use mobile devices, including smartphones and netbooks, to exfiltrate video or photographs of data via a non-organization ISP connection such as a public cellular network. Technology such as IDSs and IPSs, firewalls, and network logs cannot detect this type of exfiltration because such networks are not connected to the organization's IT system in any way. Video of scrolling source code could capture millions of lines of code and millions of dollars' worth of work.

Finally, organizations must treat mobile devices with mass storage as removable media and have appropriate protections to mitigate any risks associated with them.[23]

When an organization deems that remote access to critical data, processes, and information systems is necessary, it should offset the added risk with closer logging and frequent auditing of remote transactions. Allowing remote access only from company devices will enhance the organization's ability to control access to its information and networks as well as monitor the activity of remote employees. Information such as account logins, date and time connected and disconnected, and IP address should be logged for all remote logins. It is also useful to monitor failed remote logins, including the reason the login failed. Organizations can make such monitoring more manageable and effective by keeping authorization for remote access to critical data to a minimum.

Disabling remote access is an often-overlooked but critical part of the employee termination process. Employee termination procedures must include the following actions:

- retrieve any company-owned equipment

[23] See Practice 19, "Close the doors to unauthorized data exfiltration" (p. 90).

- disable remote access accounts (such as VPN and dial-in accounts)
- disable firewall access
- disable all remote management capabilities
- change the passwords of all shared accounts (including system administrator, database administrator (DBA), and other privileged shared accounts)
- close all open connections
- if previously agreed upon, remotely erase any devices associated with the employee if they contain company information

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

13.2 Challenges

1. managing remote devices—The demand for organizations to permit personally owned devices is growing, and the associated management and privacy issues may be challenging.
2. getting a return on investment—Organizations may have difficulty prohibiting personally owned devices and should conduct a risk–benefit analysis to support their decision.

13.3 Case Studies

In one case, two engineers worked for an international tire manufacturing company that supplied equipment to other manufacturers. The two insiders had been contracted by an overseas company to design a particular piece of equipment. The insiders knew that another company, a previous client of the tire manufacturer, had its own trade secret version of the equipment the two insiders were contracted to design. They visited the previous client's plant under the pretense of inspecting equipment that the tire manufacturer had previously supplied them. The victim organization's plant restricted access to parts of its facility behind several secure doors, and it had posted signs stating that cameras were prohibited. Visitors were required to sign in and out and be escorted at all times. The victim organization also asked visitors to sign a nondisclosure agreement (NDA), but the insiders falsely stated that they had already signed one the previous year. While one insider kept a lookout, the other insider took several pictures of the trade secret equipment with the camera on his cellphone. After the insiders left the victim's facility, one insider downloaded the images from his camera and emailed them from his personal account to his work email. Later, he sent the images from his work account to the tire manufacturer's plant to produce its version of the trade secret equipment.

The type of attack in this case poses a challenge for many organizations. Organizations' security policy and staff often overlook cameras on mobile devices, allowing attackers to circumvent technical protections on sensitive company information. However, this case crosses into the physical realm. The equipment the insiders photographed was a trade secret. While doors and warning signs were in place to deter photographing equipment, little was done to ensure people were following policy. Areas that contain sensitive trade secrets need to have additional controls

in place to prevent unauthorized photography. For example, an organization could place metal detectors and guards at the entrance to these sensitive areas to ensure no one is taking a mobile device into the restricted area. In addition, nondisclosure agreements and other legal documents should be verified long before a visitor arrives on company property. In this case, the visitors stated they had signed an NDA in the past. Organizations should require employees to reaffirm their agreement on a regular basis. Had the victim organization determined whether an NDA was on file, escorted the visitors at all times, and required that all mobile devices be left outside the secure area, this incident may not have occurred.

In a not-yet-adjudicated case, a worker at a charity allegedly took many photos of donors' check and credit card data with her smartphone, and then sent the photos off-site via her smartphone's cellular service connection. Donors of that charity were allegedly victims of fraud related to that exfiltrated data. Regardless of whether this individual is found guilty, it is clear that modern mobile devices have the ability to exfiltrate PII without detection by an organization's IT security system. Metal detectors and rules against bringing mobile devices into sensitive areas might have prevented this case's financial losses.

13.4 Quick Wins and High-Impact Solutions

13.4.1 All Organizations

- ☐ Disable remote access to the organization's systems when an employee or contractor separates from the organization. Be sure to disable access to VPN service, application servers, email, network infrastructure devices, and remote management software. Be sure to close all open sessions as well. In addition, collect all company-owned equipment, including multifactor authentication tokens, such as RSA SecurID tokens or smart cards.
- ☐ Include mobile devices, with a listing of their features, as part of the enterprise risk assessment.
- ☐ Prohibit or limit the use of personally owned devices.
- ☐ Prohibit devices with cameras in sensitive areas.

13.4.2 Large Organizations

- ☐ Implement a central management system for mobile devices.
- ☐ Monitor and control remote access to the corporate infrastructure. VPN tunnels should terminate at the furthest perimeter device and in front of an IDS and firewall. This allows for packet inspection and network access control. In addition, IP traffic-flow capture and analysis devices placed behind the VPN concentrator will allow collection of network traffic statistics to help discover anomalies. If personally owned equipment, such as a laptop or home computer, is permitted to access the corporate network, it should only be allowed to do so through an application gateway. This will limit the applications available to an untrusted connection.

13.5 Mapping to Standards

- NIST: AC-2, AC-17, AC-19
- NITTF: C-1-1

- Minimum Standards: E-1
- CERT-RMM:
  - Technology Management
    - SG2.SP2 Establish and Implement Controls
- ISO 27002:
  - 11.4.2 User authentication for external connections
  - 11.7.1 Mobile computing and communications

Practice 14: Establish a baseline of normal behavior for both networks and employees.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
			✓	✓	

This practice builds on Practice 12. Once an organization identifies and fuses the most information-rich data streams related to its critical assets, the organization can then begin to perform analysis on the data.

Every organization has a unique network topology whose characteristics, such as bandwidth utilization, usage patterns, and protocols, can be monitored for security events and anomalies. Similarly, all employees within organizations have their own unique characteristics, including typical working hours, resource usage patterns, and resource access patterns. Deviations from normal network and employee behavior can signal possible security incidents, including insider threats. To be able to identify deviations from normal behavior, organizations must first establish what characterizes normal network and employee behavior.

14.1 Protective Measures

To create a baseline of normal activity, organizations must identify the data points to collect, how long data points will be collected to establish a baseline, and what tools it will use to collect and store the data. Various tools are available for baselining normal network activity and identifying anomalies, and specialized tools for baselining normal employee behavior and identifying anomalous activity have emerged in recent years.

Organizations must ensure that they collect data for a sufficient period of time when establishing baselines of normal behavior to account for natural periods of variation in activity. For example, temporary increases in network activity due to events such as database backups or sales increases could artificially inflate baselines if the monitoring window is small. Organizations must account for normal activity spikes as part of the baseline so that it accurately reflects the organization's operations. Collecting baseline data for too long, however, increases the likelihood that abnormal or malicious behavior will become part of the baseline and may render the information inaccurate.

Computers on any given network typically need to communicate to a relatively small number of devices. For example, a workstation may only need access to a domain controller, file server, email server, and print server. If this workstation communicates with any other device, it may simply be misconfigured, or someone may be using it for suspicious activity. Host-based firewalls can be configured to allow communications between authorized devices only, preventing malicious insiders from accessing unauthorized network resources. VPN usage should be carefully monitored because it allows users to access organizational resources from nearly any place that has an Internet connection. Organizations may have policies defining permissible times for network access. For example, they may permit some staff VPN access only between business hours, while others may have access at any time. Monitoring access times or enforcing access

policies will help an organization detect insider activity. Organizations that do not require VPN connections from many foreign countries should consider permitting (via white listing) VPN connections only from countries where a business need exists. Organizations should implement further VPN access controls, such as limiting access to file shares on a server, to control how data can leave the organization. To enforce stricter security controls, organizations should also consider limiting access to organizationally owned assets only. When this is not possible, an application gateway can restrict which resources are remotely accessible. In addition, organizations should monitor VPN connections for any abnormal behavior, such as a sudden download of data that exceeds normal usage.

An organization's networks typically use a known set of ports and protocols. Devices that stray from this known set should be flagged for review. For example, organizations typically have a central email server, so a workstation exhibiting SMTP traffic may be cause for concern. Similarly, use of protocols with a nonstandard port should be flagged for review, for example, using the SSH protocol on port 80, instead of the usual port 22.

Organizations should review firewall and IDS logs to determine normal activity levels. A SIEM tool will help security staff sift through the event logs and establish a baseline of normal firewall and IDS behavior. Sudden changes in the number of alerts may indicate abnormal behavior and should be further investigated. For example, a sudden surge in port 21 (FTP) firewall denials caused by a workstation may indicate that someone is trying to directly contact an FTP server to upload or download information.

Employees tend to develop patterns in the files, folders, and applications they access, and when and where they access company resources and facilities. Deviations from an employee's normal access patterns may be indicative of that employee accessing information outside of their need-to-know, violating company policies such as acceptable use policies and intellectual property policies, or attempting to conceal malicious behavior. Identifying anomalous employee activity relative to an employee's peers (which may include groups such as employees with the same job title, employees that work in the same department, or employees that work in the same office) may also identify employees whose actions are not in line with their roles and responsibilities within the organization.

14.2 Challenges

1. establishing a trusted baseline—Organizations may find it challenging to establish a trusted baseline, which may incorporate ongoing and unrecognized malicious activity, including insider attacks.
2. ensuring privacy—Organizations may find it challenging to maintain employee privacy while collecting data to establish a baseline.
3. scaling—Larger organizations may benefit from establishing baselines for individual subunits of the organization. A single, all-encompassing baseline may conceal concerning behavior if some details go undetected. The organization may have to experiment to decide what best suits its needs.

14.3 Case Studies

The victim organization, a financial institution, employed the insider as a senior financial analyst. Every Sunday, the insider came to the organization's offices and downloaded 20,000 mortgage applicant records to a USB flash drive. Over a two-year period, the insider downloaded and sold more than two million records that contained PII. The organization noticed that the insider had been coming to work outside of normal working hours, but it believed the insider was merely hard working. The insider sometimes downloaded the records during normal working hours. The organization had a policy prohibiting flash drives or other storage devices from being used on its computers. The organization had also disabled flash drive access on nearly all its computers, but the insider located the one computer that lacked this security feature. To conceal his activity, the insider emailed most of the records from public computers, but he occasionally emailed them from his personal computer. The insider and his accomplice, an outsider with a lengthy criminal history, sold batches of 20,000 records for $500 each. The insider made $50,000 to $70,000 and stored the proceeds in a bank account created under his name and that of a fictional consulting company. At least 19,000 mortgage applicants became victims of identity theft. Dozens of class-action lawsuits have been filed against the victim organization, which was experiencing financial difficulties and was bought out one year after the incident began.

In another case, the insider was a contractor temporarily working as a customer service representative for the victim organization, a commercial online service. The victim organization's system administrator detected suspicious after-hours network traffic, which was traced back to the insider's workstation using the IP address. A manager at the victim organization conducted an investigation and discovered that the insider had entered the facility after hours, and that at least one customer's credit card information had been disclosed on the Internet. Additionally, the insider had copied and transferred the organization's proprietary, copyrighted files via the Internet. Despite a warning from management, the insider continued his activity until his employment was terminated. The insider was arrested, and convicted.

In both of these instances, the insiders' behavior deviated significantly from baseline network behavior. One insider accessed and downloaded large volumes of information, beyond the normal usage of average users, while the other accessed the system outside of normal working hours. Organizations need to establish a normal baseline of activity and be watchful for any activity that exceeds that baseline. To avoid any appearance of discrimination or wrongdoing, organizations must carefully document and adhere to policies and procedures for monitoring any employee activity. They should also get legal advice as the policies and procedures are developed, finalized, and implemented.

14.4 Quick Wins and High-Impact Solutions

14.4.1 All Organizations

- ☐ Use monitoring tools to monitor network and employee activity for a period of time to establish a baseline of normal behaviors and trends.

- ☐ Deny VPN access to foreign countries where a genuine business need does not exist. White list only countries where a genuine business need exists.[24]
- ☐ Establish which ports and protocols are needed for normal network activity, and configure devices to use only these services.
- ☐ Determine which firewall and IDS alerts are normal. Either correct what causes these alerts or document normal ranges and include them in the network baseline documentation.

14.4.2 Large Organizations

- ☐ Establish network activity baselines for individual subunits of the organization.
- ☐ Determine which devices on a network need to communicate with others and implement access control lists (ACLs), host-based firewall rules, and other technologies to limit communications.
- ☐ Understand VPN user requirements. Limit access to certain hours and monitor bandwidth consumption. Establish which resources will be accessible via VPN and from what remote IP addresses. Alert on anything that is outside normal activity.

14.5 Mapping to Standards

- NIST: AC-17, AU 5-6, CM-7, RA-3, SC-7
- NITTF: C-1-2
- Minimum Standards: E-1
- CERT-RMM:
  - Monitoring

[24] Regional Internet Registries maintain IP address assignments. Registries include AfriNIC, ARIN, APNIC, LACNIC, and RIPE NCC. Other companies maintain IP data that is available under various licenses, such as http://www.maxmind.com/app/geoip_country and http://www.countryipblocks.net/. Regional Internet registry data will be more accurate.

Practice 15: Enforce separation of duties and least privilege.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	✓

Though this practice was discussed in relation to privileged users, the organization should work toward separation of duties for all employees involved in all business processes. This practice limits the damage that malicious insiders can inflict on critical business processes, systems, and information.

15.1 Protective Measures

Separation of duties requires dividing functions among multiple people to limit the possibility that one employee could steal information or commit fraud or sabotage without the cooperation of others. Many organizations use the *two-person rule*, which requires two people to participate in a task for it to be executed successfully. Organizations can use technical or nontechnical controls to enforce separation of duties. Examples include requiring two bank officials to sign large cashier's checks or requiring verification and validation of source code before the code is released. In general, employees are less likely to engage in malicious acts if they must collaborate with another employee.

Typically, organizations define roles that characterize the responsibilities of each job and the level of access to organizational resources required to fulfill those responsibilities. Organizations can mitigate insider risk by defining and separating roles responsible for key business processes and functions. For example, organizations could

- require online management authorization for critical data-entry transactions
- implement configuration management processes that allow for a developer, a reviewer, and a tester to independently review changes to code
- use configuration management processes and technology to control software distributions and system modifications
- require two different individuals to perform backup and restore functions
- design auditing procedures to prevent collusion among auditors

Effective separation of duties requires implementation of *least privilege*, or authorizing people to use only the resources needed to do their jobs. Least privilege also reduces an organization's risk of insider theft of confidential or proprietary information because access to it is limited to only those employees who need it to do their jobs. For instance, some cases of theft of IP involved salespeople who had unnecessary access to strategic products under development.

Organizations must manage least privilege as an ongoing process, particularly when employees move throughout the organization in promotions, transfers, relocations, and demotions. As employees change jobs, organizations tend not to review their required access to information and information systems. All too often, organizations give employees access to new systems or information required for their new job without revoking their access to information and systems required for their previous job. Unless a transitioned employee retains responsibility for tasks from his or her previous job, the

organization should disable the employee's access to previously required information and information systems.

Organizations can use physical, administrative, and technical controls to enforce least privilege. Gaps in access control have often facilitated insider crimes. Employees can easily circumvent separation of duties if they are enforced by policy rather than by technical controls. Ideally, organizations should include separation of duties in the design of their business processes and enforce them through technical and nontechnical means.

Access control based on separation of duties and least privilege is crucial to mitigating the risk of insider attack. These principles have implications in both the physical and virtual worlds. In the physical world, organizations need to prevent employees from gaining physical access to resources not required by their work roles. For example, researchers need access to their laboratory space but not to Human Resources' file cabinets. There is a direct analogy in the virtual world: Organizations must prevent employees from gaining online access to information or services that are not required for their job. This kind of control is often called *role-based access control*. Prohibiting access by personnel in one role from the functions permitted for another role limits the damage they could inflict.

15.2 Challenges

1. separating duties and enforcing least privilege—Smaller organizations will find it more difficult to implement separation of duties and least privilege security models because the organization may not be staffed to accommodate the practice. Implementing these practices at a granular level may interfere with business processes.
2. balancing security and the organization's mission—Most organizations will find it challenging to strike a balance between implementing these recommendations and accomplishing the organization's mission.

15.3 Case Studies

The insider, a resident alien, was employed as a clerk by the victim organization, a department of motor vehicles (DMV). For over five years, the insider and three accomplices issued over 1,000 fraudulent driver's licenses to immigrants in exchange for $800-$1,600 per license. Applicants would exchange payment with an insider in the parking lot, and then be sent inside the victim organization for processing by another insider. When a fraudulent license request was made, the insiders would falsify department records so it would appear that the immigrants had surrendered an out-of-state license in exchange for a new license. The primary insider also committed Social Security fraud by misusing valid SSNs for the benefit of other applicants. The insiders were captured after surveillance of the insider's office allowed law enforcement and department investigators to observe the transactions. The insider was arrested, convicted, ordered to pay a $200,000 fine, and sentenced to over three years' imprisonment.

In another case the insider was hired by the victim organization and eventually promoted to executive director. In this management role, the insider had access to the victim organization's various bank accounts and accounting system. The insider would issue checks to himself and modify the payee names in the accounting system. He would name vendors that the organization commonly did business with as the payees in order to conceal the fraud. The insider also modified

bank statements to match the fictitious invoices created. The fake invoices were then stapled to the altered bank statements and then filed away. The insider was arrested, convicted, ordered to pay $400,000 restitution, and sentenced to over two years' imprisonment followed by five years of supervised release.

These individuals were both able to modify critical business data without requiring someone else to verify the changes. In addition to sometimes being malicious insiders, executives are common targets for social engineering attacks, so a best practice is to restrict their level of access. If an individual requires additional access, organizations should consider creating a separate account with more granular control and additional logging and auditing.

15.4 Quick Wins and High-Impact Solutions

15.4.1 All Organizations

- ☐ Carefully audit user access permissions when an employee changes roles within the organization to avoid privilege creep. In addition, routinely audit user access permissions at least annually. Remove permissions that are no longer needed.
- ☐ Establish account management policies and procedures. Audit account maintenance operations regularly. Account activity should reconcile with help desk documentation.
- ☐ Require privileged users to have both an administrative account with the minimum necessary privileges to perform their duties and a standard account that is used for every day, non-privileged activities.

15.4.2 Large Organizations

- ☐ Review positions in the organization that handle sensitive information or perform critical functions. Ensure these employees cannot perform these critical functions without oversight and approval. The backup and restore tasks are often overlooked. One person should not be permitted to perform both backup and restore functions. Your organization should separate these roles and regularly test the backup and recovery processes (including the media and equipment). In addition, someone other than the backup and restore employees should transport backup tapes off-site.

15.5 Mapping to Standards

- NIST: AC-5 (Separation of Duties), AC-6 (Least Privilege)
- NITTF: B-2
- Minimum Standards: G-1-a, G-1-b
- CERT-RMM:
  - Access Management
- ISO 27002:
  - 10.1.3 Segregation of duties
  - 11.2.2 Privilege management

–

Practice 16: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
	✓		✓	✓	

Organizations should include provisions for data access control and monitoring in any agreements with cloud service providers.

Cloud computing allows organizations to quickly stand up various infrastructure devices and services while keeping costs low. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [Mell and Grance 2011].

A recent study by Ponemon Institute found a "majority of cloud providers believe it is their customer's responsibility to secure the cloud and not their responsibility. They also say their systems and applications are not always evaluated for security threats prior to deployment to customers" [Ponemon 2011]. Organizations should not assume that cloud service providers take responsibility for securing the organization's information.

16.1 Protective Measures

Four types of cloud services are currently available to organizations [GAO 2010]:

1. private cloud—operated solely for one organization
2. community cloud—shared by several organizations
3. public cloud—available to any customer
4. hybrid cloud—two or more clouds (private, community, or public) that are connected

Private clouds are operated by the organization itself or by another entity on behalf of the organization. Community clouds typically consist of several organizations that have the same needs. Public clouds are open to any customers, who often have diverse needs [GAO 2010].

In each of these models, the cloud service provider—a trusted business partner—provides data and infrastructure services to the organization. This relationship extends the organization's network perimeter and greatly increases the organization's reliance on the service provider's practices. It may also offer new attack opportunities for malicious insiders. The same protections that the organization uses to secure its data and infrastructure should extend to the service provider. Organizations must often accept the service provider's attestation that its policies and procedures afford the organization the required levels of protection. Organizations may wish to work with the service provider to obtain independent audit reports or conduct an audit themselves.

Before using a cloud service, an organization must thoroughly understand, document, and assess the service's physical and logical access and security controls. Appropriate measures to protect the confidentially, integrity, and availability of data at rest, in motion, and in use must be in place. For example, encryption can protect data at rest and in motion. Organizations must fully understand who has access to their data and infrastructure as well as what measures are in place to mitigate any risks.

To understand the cloud environment effectively, sufficient auditing and monitoring of the environment must regularly occur. Depending on the capabilities of the cloud service provider and the service agreement, the service provider may offer certain monitoring capabilities on behalf of the customer. To effectively manage the environment and ensure contractual obligations are being met, the organization's operations and security personnel should have access to auditing and monitoring information as needed. The auditing and monitoring capabilities must meet any rules, laws, and regulations that bind the organization. Either the service provider or the organization must supplement any capabilities that are found to be lacking. Agreements with the service provider must define these capabilities. Organizations should consider methods for secure authorization and access control specific to clouds [Shin et al. 2011, 2012].

The cloud's control plane refers to the underlying hardware, hypervisors, administrative interfaces and management tools that are used to run the cloud itself. Generally, access to the control plane gives users almost total control of any applications running in that cloud. Many of the control technologies are complex and relatively new, providing many opportunities for security vulnerabilities including those due to misconfigurations. To help protect the control plane, an organization could perform near-real-time auditing of access, internal events, and the external communication between its components to help distinguish anomalies from normal behavior.

Organizations should consider each of their potential insider threats related to cloud services and determine if service level agreements (SLAs) and the provider's insurance cover identified risks. A cloud insider could be a rogue administrator of a service provider, an insider who exploits a cloud-related vulnerability to gain unauthorized access to organization systems and/or steal data from a cloud system, or an insider who uses cloud systems to carry out an attack on an employer's local resources. Organizations should consider the different types of potential rogue administrators: hosting-company administrators, virtual-image administrators, system administrators, and application administrators. Differences in security policies or access control models between cloud-based and local systems could enable insiders to exploit vulnerabilities that might not otherwise be exposed. Attacks could exploit the increased latency between servers in a cloud architecture or, to cause more damage during an attack, use any delays due to problems validating the organization's identity to the cloud provider [Claycomb and Nicoll 2012]. Even insiders attacking data, non-cloud data or systems could use cloud parallel processing to crack password files, a distributed cloud platform to launch a DDoS attack, or the use of cloud storage to exfiltrate data from an employer. SLAs should identify any known risks that the provider has identified in its enterprise risk assessment, and the cloud consumer should ensure the cloud service provider's insurance would cover losses in case of a provider's business failure.

The Cloud Security Alliance recommends the following practices to help protect against rogue administrators [CSA 2010]:

- Specify HR requirements as part of legal contracts.

- Strictly enforce supply chain management and assess suppliers.
- Determine processes for security breach notification.
- Ensure transparency in overall information security and management practices.

To protect against insiders who exploit cloud-related vulnerabilities and to ensure a timely response to attacks in progress, organizations should create an incident response plan that includes offline credential verification. System administrators within the organization should be familiar with configuration tools for their cloud-based systems, including procedures for disabling cloud-based services if necessary. Organizations should use data loss prevention (DLP) tools and techniques to detect sensitive data being sent to cloud-based storage. Network- or host-based controls may also prevent employees from accessing particular external cloud resources.

To improve data access latencies around the world as well as resiliency to localized Internet problems, cloud providers often have data centers in multiple countries. However, each country has particular laws, cultural norms, and legal standards, enforced with varying stringency, regarding contracts, security, background checks, and corruption. Employees of cloud service providers have ultimate control over the hardware, and thus over an organization's cloud-based data. They can typically reset passwords, copy disks, sniff the network, or physically alter the hardware or operating system, including the virtualization hypervisor.[25] Organizations should consider particular risks related to countries their data could go to, and whether contracts with the cloud service provider offer adequate assurance of data security.

Organizations commonly hire outside consultants to help them migrate data or services to a cloud service provider. The migration process often involves exceptions to normal IT system processes. The consultant has expert knowledge of the migration process and is given knowledge of the organization's IT systems, so the consultant has an insider's means to cause the organization a great deal of harm. Vetting and background checks on any outside consultants for this process should be particularly rigorous, and oversight of these insider workers is important.

Cloud infrastructure audits should periodically evaluate cloud security, including auditing virtual machines to ensure they meet security configuration requirements. Continuous monitoring of the distributed infrastructure's behavior and use should be done in near-real-time if possible. Audit logs should be reviewed according to policy, and diagnostic data aggregation and management should be performed. New devices and services should be identified, as well as security reconfigurations and any deviations from a predetermined baseline.

16.2 Challenges

1. working with cloud service providers—Organizations may find it challenging to establish contracts with cloud service providers due to the provider's business model. It may be a challenge to find a service provider that meets the organization's expectations of both physical and logical security. Some providers may leave security up to the customer [Ponemon 2011].

[25] Department of Homeland Security. *Cloud Computing Security*. U.S. Department of Homeland Security, Federal Network Security Branch.

2. accepting risk—Organizations should consider cloud services as they would any other contractual service. The chosen cloud service provider should meet or exceed the organization's own levels of security, and senior management must formally accept the risk of using these services. Organizations should keep in mind that they are ultimately entrusting the organization's data and outsourced services to a third party. A failure by the trusted business partner, whether security related or otherwise, may expose the organization to negative publicity or legal action.
3. lacking standards for mitigating insider threats in a cloud computing model

16.3 Case Studies

A retail organization that used USB virtual private network (VPN) tokens for remote access fired a network engineer. Before his termination, the insider created a token in the name of a fake employee. A month after termination, the insider contacted the IT department, using the fictional name he had created, and convinced them to activate the VPN token. Several months later, the insider used the VPN token to access the network 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.

In another case, the senior management of a pharmaceutical company had a dispute with an IT employee. The insider resigned, but the insider's supervisor and close friend convinced the company to keep the insider on as a contractor. A few months later, the insider left the company completely. The insider used his home network to install a piece of software on the victim organization's server. Then, using a restaurant's Internet connection and a compromised user password to access the server, the insider used the previously installed software to delete virtual machines that hosted the organization's email, order tracking, and financial management systems. This attack halted the organization's operations for several days. The insider's connection to the attack was discovered via his purchases in the restaurant near the time of the attack. The insider was arrested and pleaded guilty.

In these two cases, the organizations utilized their own private clouds, on which the insiders had administrative remote access to virtual machines hosting critical processes. Organizations need to be aware of what remote access to their systems exists and the risks associated with it. Virtual machines can be quickly deployed, but they can also be destroyed just as quickly. Organizations should carefully monitor and log the virtual environment to quickly respond to issues. They must also carefully control or prohibit remote access to tools that allow for the modification of virtual services.

16.4 Quick Wins and High-Impact Solutions

16.4.1 All Organizations

The considerations below apply to any organization utilizing cloud services. Such services not owned and operated by the organization deserve further scrutiny.

☐ Conduct a risk assessment of the data and services that your organization plans to outsource to a cloud service provider before entering into any agreement. Your organization must ensure that the service provider poses an acceptable level of risk and has implemented

mitigating controls to reduce any residual risks. Your organization must carefully examine all aspects of the cloud service provider to ensure the service provider meets or exceeds your organization's own security practices.

- ☐ Verify the cloud service provider's hiring practices to ensure it conducts thorough background security investigations on any personnel (operations staff, technical staff, janitorial staff, etc.) before they are hired. In addition, the service provider should conduct periodic credit checks and reinvestigations to ensure that changes in an employee's life situation have not caused any additional unacceptable risks.
- ☐ Control or eliminate remote administrative access to hosts providing cloud or virtual services.
- ☐ Understand how the cloud service provider protects data and other organizational assets before entering into any agreement. Verify the party responsible for restricting logical and physical access to your organization's cloud assets.

16.5 Mapping to Standards

- NIST: Access Control Family (AC), Audit Family (AU), Risk Assessment Family (RA), Secure Communications Family (SC)- sans SC-9 (withdrawn), Services and Acquisitions Family (SA)
- NITTF: N/A
- Minimum Standards: H-1
- CERT-RMM:
  - External Dependencies Management

Practice 17: Institutionalize system change controls.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
			✓	✓	✓

Organizations must control changes to systems and applications to prevent insertion of back doors, keystroke loggers, logic bombs, and other malicious code or programs. Change controls should be thoroughly implemented and continue over time and all stages of projects.

17.1 Protective Measures

Security controls are defined in NIST 800-53 Rev. 4 as "the safeguards/countermeasures prescribed for information systems or organizations that are designed to: (i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (ii) satisfy a set of defined security requirements." [NIST 2015]. *Change controls* are security controls that ensure the accuracy, integrity, authorization, and documentation of all changes made to computer and network systems.[26] The wide variety of insider compromises that relied on unauthorized modifications to the victim organizations' systems suggests the need for stronger change controls. To develop stronger change controls, organizations should identify baseline software and hardware configurations. An organization may have several baseline configurations, given the different computing and information needs of different users (e.g., accountant, manager, programmer, and receptionist). As an organization identifies different configurations, it should characterize its hardware and software components.

Baseline documentation can be a basic catalog of information, such as disk utilization, hardware devices, and versions of installed software. However, such basic information can be easily manipulated, so strong baseline documentation often requires more comprehensive records. Baseline documentation should consist of

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

Once an organization captures this information, it can validate computers implementing each configuration by comparing them against the baseline copy. The organization can then investigate discrepancies to determine if they are benign or malicious. Changes to system files or the addition of malicious code should be flagged for investigation. Some tools designed to check file integrity partially automate this process and allow scheduled sweeps through computer systems.[27]

[26] See Information Technology Controls, the Institute of Internal Auditors, http://www.theiia.org/download.cfm?file=70284.

[27] See http://www.sans.org/resources/idfaq/integrity_checker.php for a discussion of file integrity checkers.

Depending on the computing environment, configurations may not remain unchanged for long. An organization's change management process should include characterization and validation. The organization should define different roles within this process and assign them to different individuals so that no one person can make a change unnoticed by others within the organization. For example, someone other than the person who made configuration changes should validate the configuration so that there is an opportunity to detect and correct malicious changes (including planting of logic bombs). Some commercial software products will monitor the system to detect configuration changes.

Organizations must protect change logs and backups so they can detect unauthorized changes and, if necessary, roll back the system to a previous valid state. In addition, some insiders have modified change logs to conceal their activity or implicate someone else for their actions. Other insiders have sabotaged backups to further amplify the impact of their attack.

Malicious code placement and other insider malicious IT actions may defeat common defensive measures, such as firewalls and IDSs. While these defenses are useful against external compromises, they are less useful against attacks by malicious insiders as they primarily monitor and analyze data communications, including code spread through networking interfaces, rather than code installed directly on a computer. Antivirus software installed on workstations, servers, and Internet gateways may reduce the likelihood of a successful compromise. However, antivirus software must have the latest malicious code detection signatures updated regularly to be able to detect the malicious code. Zero-day exploits, exploits that have never been seen before, as well as logic bombs such as maliciously configured or scheduled ordinary processes (e.g., incomplete backups) are likely to be missed by signature-based antivirus solutions. Change controls help address the limitations of these defenses.

Just as organizations can implement tools for detecting and controlling system changes, they should also implement configuration management tools for detecting and controlling changes to source code and other application files. As described in Practice 15: "Enforce separation of duties and least privileges," some insiders have attacked by modifying source code during the maintenance phase of the software development lifecycle, not during initial implementation. Some organizations institute much more stringent configuration management controls during the initial development of a new system, including code reviews and use of a configuration management system. However, once the system is in production and development stabilizes, some organizations relax the controls, leaving a vulnerability open for exploitation by technical insiders.

17.2 Challenges

1. managing the project—Change controls may increase the turnaround time for system changes.
2. monitoring—Changing the information system may entail adjustments to monitoring mechanisms, so IT staff may need to coordinate with those responsible for monitoring and auditing alerts.

3. managing the baseline—While baseline management helps reduce the number of diverse systems with unique configurations that require special management and patching procedures, it also introduces a certain level of risk. Having many baselines with similar software or configurations may allow an attacker to exploit a single vulnerability on a large scale.

17.3 Case Studies

The victim organization, an investment bank, employed the insider as a computer specialist. The insider created a risk assessment program to help bond traders decide which bonds to buy and sell. Later, the insider was employed by the same organization as a securities trader. For unknown reasons, the insider became angry with management. He may have been displeased with his bonus, even though he made more than $125,000 a year. Motivated by revenge, the insider inserted a logic bomb into the risk assessment program he had created as a computer specialist. The logic bomb increased the risks of deals in tiny increments so that traders would not realize their deals were getting riskier and would take more and more precarious deals. The insider planned for the organization and its customers to lose $1 million over the course of a year. A programmer trying to modify the program's code realized that someone had tampered with the program and subsequently discovered the logic bomb. The organization was able to prevent any major damage from occurring, but it spent $50,000 repairing the damage. The insider later claimed that he had created the program for personal use, but he contradicted this claim when he revealed that a trader had made a large profit using the insider's program. The insider was terminated, arrested, and convicted, but sentencing details are unknown.

In another case, a financial services firm employed the insider as a systems administrator. The insider had heard that bonuses would be half of what they normally were and had complained to his supervisor. When the organization announced the cut to employee bonuses, the insider responded by building and distributing a logic bomb on the organization's UNIX-based network. The logic bomb took down nearly 2,000 servers in the head office and 370 servers at branch offices around the country. Prior to the logic bomb's detonation, the insider purchased put options on the company, expecting the subsequent detonation of the logic bomb to drive down the firm's stock price. The insider quit when the organization became suspicious of him. Although the firm's stock price did not drop, the logic bomb cost the victim organization $3.1 million in repairs and caused mass chaos from which the firm never fully recovered. A forensics investigation connected the insider to the incident through VPN access and copies of the logic bomb source code found on his home computers. The insider was arrested, convicted, and sentenced to 97 months of imprisonment.

In both of these cases, the insiders were able to manipulate critical production systems by placing malicious code onto them. The insiders caused the victim organizations and their customers or shareholders to suffer losses. A change management process, along with separation of duties, could have reduced the likelihood of these attacks succeeding. In addition, if the organizations had regularly used a tool to compare system baselines or file hashes, the changes to the system would have been detected and the attack mitigated or neutralized before causing substantial harm.

17.4 Quick Wins and High-Impact Solutions

17.4.1 All Organizations

☐ Periodically review configuration baselines against actual production systems and determine if any discrepancies were approved. If the changes were not approved, verify a business need for the change.

17.4.2 Large Organizations

☐ Implement a change management program within the organization. Ensure that a change control board vets all changes to systems, networks, or hardware configurations. All changes must be documented and include a business reason. Proposed changes must be reviewed by information security teams, system owners, data owners, users, and other stakeholders.

☐ The configuration manager must review and submit to the change control board any software developed in-house as well as any planned changes.

17.5 Mapping to Standards

- NIST: CM 1-11, CA-2
- NITTF: N/A
- Minimum Standards: N/A
- CERT-RMM: Technology Management
  - Technology Management
    - SG4.SP3: Perform Change Control and Management
- ISO 27002:
  - 10.1.2 Change Management

Practice 18: Implement secure backup and recovery processes.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
			✓	✓	

Despite all of an organization's precautions, it is still possible that an insider will carry out a successful attack. Organizations must prepare for that possibility and enhance organizational resiliency by implementing and periodically testing secure backup and recovery processes.

18.1 Protective Measures

Prevention is the first line of defense against insider attacks. However, determined insiders may still find ways to compromise a system. Organizations must run effective backup and recovery processes so they can sustain business operations with minimal interruption if a system compromise occurs. Case studies show that effective backup and recovery mechanisms can

- reduce from days to hours the downtime needed to restore systems from backups
- avoid weeks of manual data entry when current backups are not available
- reduce from years to months the time needed to reconstruct information for which no backup copies exist

Backup and recovery strategies should include

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

In addition, organizations should legally and contractually require accountability and full disclosure of any third-party vendors responsible for providing backup services, including off-site storage of backup media. SLAs should clearly state the required recovery period, who has access to physical media while it is being transported off-site, and who has access to the media while in storage. Case examples throughout this guide have demonstrated the threat presented by employees of trusted business partners. Organizations should apply the mitigation strategies for those threats to backup service providers also.

Organizations should encrypt backup media, and they should verify and record cryptographic checksums, such as MD5 or SHA-1 checksums, before the media leaves the organization. This will ensure the confidentiality and integrity of the data while it is in transport and in storage. Organizations should manage encryption keys to ensure the data is available when needed.

When possible, an organization should have multiple copies of backups and store redundant copies in a secure, off-site facility. Different people should be responsible for the safekeeping of

each copy so that multiple individuals would have to cooperate to compromise the backups. An additional level of protection for the backups should include encryption, particularly when the redundant copies are managed by a third-party vendor at the secure, off-site facility. Encryption does come with additional risk, however, such as lost or damaged keys. To maintain control of the decryption process if the employees responsible for backing up the information resign or are terminated, the organization should always follow the two-person rule when managing the encryption keys.

System administrators should ensure that the physical media where backups are stored are also protected from insider corruption or destruction. Cases in the CERT insider threat database describe attackers who deleted backups, stole backup media (including off-site backups in one case), and performed actions whose consequences could not be undone due to faulty backup systems. Some system administrators neglected to perform backups in the first place, while other insiders sabotaged established backup mechanisms. Such actions can amplify the negative impact of an attack on an organization by eliminating the only means of recovery. Organizations should take the following actions related to backup and recovery processes, in order to guard against insider attack:

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

Unfortunately, some attacks against networks may interfere with common methods of communication, increasing the uncertainty and disruption in organizational activities, including recovery from the attack. This is especially true of insider attacks because insiders are familiar with organizational communication methods. Separate trusted communication paths outside of the network, with sufficient capacity to ensure critical operations in the event of a network outage, are often substantial investments for an organization. A risk assessment will help determine if the investment is worthwhile. However, this kind of protection would reduce the impact of attacks on an organization's communication capability, making it a less attractive target for malicious insiders.

Organizations must regularly test their backup and recovery processes. Most importantly, organizations must test their backup media. A regular exercise, conducted as part of a disaster recovery or continuity-of-operations exercises, should actually test the organization's ability to restore data from backup. A tabletop exercise is not sufficient. A good test might be to rebuild or restore the backed-up system to a separate piece of hardware without any previously installed software or operating system (also called a "bare metal restore"), to recover a critical server asset. Ordering that the test should restore to a random date from past archives, with no notice of that date until during the restore test, will help test for and prevent bad backups, while simultaneously avoiding test process tampering by malicious backup administrators. For example, a malicious backup administrator who knows of an impending exercise could configure the backup and recovery mechanisms to function properly so as to conceal any ongoing malicious activity. If the organization has separated the backup and recovery roles, this (restore by a recovery administrator

who is given a random date to restore from) will also be a good test to verify that company policies and procedures are working.

18.2 Challenges

1. justifying operational costs—Justifying additional costs for implementing more sophisticated and resilient backup and recovery processes, separation of duties, and off-site storage facilities may be an obstacle for some organizations.
2. managing keys—Organizations may need to purchase additional hardware or software to properly manage encryption keys to ensure backup and recovery processes will succeed.

18.3 Case Studies

An insider was reading the classified ads of a newspaper when she came across an ad for an administrative assistant position that sounded very similar to her own current position. The ad included the contact information for the insider's manager. On the Friday before the incident, the insider called in sick. The insider contacted the business owner's wife about the ad that was placed on Saturday. The victim's wife attempted to convince the insider that the ad was for a job at a company his wife owned and not the insider's job. On Sunday, around 11 p.m., the insider entered the company's premise and proceeded to delete the company's data before leaving at around 3 a.m. The owner arrived at the business office Monday to discover the data had been erased with no backups available. He contacted police and stated he suspected his administrative assistant. Police went to the insider's house where she was questioned and arrested. The insider was convicted, ordered to pay $3,000 restitution, sentenced to five years' probation with 100 hours of community service and court-ordered anger management classes, mental health evaluation, and treatment.

In this case, the insider was able to delete the company's data by simply showing up on-site during off-work hours. This case illustrates the need for multiple backups and off-site storage. If the organization implemented off-site storage of backup data, it would have been able get the business up and running within a reasonable amount of time. The following case highlights an example of backups helping to mitigate the damage from an insider incident.

In a second case, the insider was employed as a programmer by the victim organization, a financial institution. The insider was responsible for managing the organization's specialized financial software computer network. The insider had administrative level access to and familiarity with the company's computer systems, including the database server. The insider was advised of adverse employment issues and subsequently placed on a performance improvement plan. Shortly after this, the insider planted a logic bomb on the organization's network. The insider was terminated when he failed to show up at work without providing prior notice. At the time of the insider's termination, the organization was not aware of the logic bomb. The logic bomb detonated, causing the deletion and modification of 50,000 financial records and disrupting the computer network. All points of access to the logic bomb were through the insider's account. Backup tapes showed that the insider authored the logic bomb. There was also evidence that the insider deleted computer records containing his command history of access to the logic bomb. The insider was arrested, convicted, and sentenced to 12 months of imprisonment followed by six months of electronic monitoring and home confinement and three years of supervised release.

In this case, the insider attempted to cause significant damage to the victim organization by detonating a logic bomb. Backups were able to restore the deleted and modified financial records, while also providing evidence of the insider's attack despite the insider's attempts to delete those logs. This case illustrates the importance of backup and recovery process for both resuming business operation and identifying the perpetrator.

18.4 Quick Wins and High-Impact Solutions

18.4.1 All Organizations

- ☐ Store backup media off-site. Ensure media is protected from unauthorized access and can only be retrieved by a small number of individuals. Utilize a professional off-site storage facility; do not simply send backup media home with employees. Encrypt the backup media and manage the encryption keys to ensure backup and recovery are possible.
- ☐ Ensure that configurations of network infrastructure devices (e.g., routers, switches, and firewalls) are part of your organization's backup and recovery plan as well as the configuration management plan.

18.4.2 Large Organizations

- ☐ Implement a backup and recovery process that involves at least two people: a backup administrator and a restore administrator. Both people should able to perform either role.
- ☐ Regularly test both backup and recovery processes. Ensure that your organization can reconstitute all critical data as defined by the business continuity plan and/or disaster recovery plan. Ensure that this process does not rely on any single person to be successful.

18.5 Mapping to Standards

- NIST: CP 2-4, CP-6, CP-9, CP-10,
- NITTF: N/A
- Minimum Standards: N/A
- CERT-RMM:
  - Knowledge and Information Management
    - SG6.SP1: Perform Information Duplication and Retention
- ISO 27002:
  - 10.5.1 Back-up

Practice 19: Close the doors to unauthorized data exfiltration.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
		✓	✓	✓	

Organizations must understand where their information systems are vulnerable to data exfiltration and implement mitigation strategies.

Information systems offer many ways to share information, from USB flash drives and other removable media to printers and email. Each type of device presents unique challenges for preventing data exfiltration. To reduce the risk of an insider compromising sensitive information, organizations must understand where and how data can leave their systems.

19.1 Protective Measures

To mitigate the risk of insiders maliciously (or unintentionally) removing (or exposing) data, the organization must first understand where and how it can be removed. Because many types of technologies and services could become exit points for data, an organization must be able to account for all devices that connect to its system, as well as all physical and wireless connections to its systems, such as

- Bluetooth
  - wireless file transfers
- loss of a device
  - laptop
  - CD
  - hard drive
  - mobile device
- removable media
  - USB flash drives
  - CD-RW and/or DVD-RW
  - phones with storage
  - media cards (compact flash, SD cards, etc.)
  - projectors with data storage
  - cameras and video recorders
  - USB drives (non-flash)
  - microphones
  - web cameras
- enclave exit points
  - Internet connections

  - interconnections with trusted business partners
- Internet services
  - FTP, SFTP, SSH
  - instant messaging and Internet chat (GChat, Facebook Chat, etc.)
  - cloud services (online storage, email, etc.)
- printers, fax machines, copiers, and scanners

Removable media is prevalent in every organization, and many employees have a justifiable business need for it. However, there are ways to properly control and audit various types of media without impeding the organization's mission.

Group policies[28] for Microsoft-Windows-based environments can control which types of devices may be installed on a client system. Other commercial solutions allow a finer grained approach to controlling USB devices and offer additional features such as shadow copying of files, which makes a snapshot copy of any file that is moved to removable storage. This allows an organization to see who copied the files and what the files contained. A simple log containing just the name of a copied file does not provide definitive details of file contents. In addition, some commercial products require the removable file or media to be encrypted before a file is moved to it. To better control authorized devices for storing company data, organizations should have a policy requiring that employees use only company-owned media devices for transferring files.

Organizations whose risk assessment has identified USB devices as a threat should consider adopting policies and procedures that restrict their use to a trusted agent, or at least a second person (using the two-person rule [Infosecurity 2010]) who reviews, approves, and conducts the copy. For example, an organization could implement the following policy:

> *The data transfer process typically begins when a user identifies files that need to be copied from the system for a justified business reason. The user completes a data transfer form that lists the filenames, location of the files, reason for the transfer, whom the data is intended for, sensitivity of the data, and the requestor's signature. Once this form is completed, the requestor's manager should review the request and contents of the files and approve or deny the transfer. Next, the data owner reviews the request and either approves or denies the transfer. If everyone has approved, the request is taken to the business unit's trusted agent, who completes the request by transferring the files to removable media. This process eliminates the need for access to USB flash drives by multiple individuals and establishes a way to audit data that has been removed from the system.*

However, users could email data out of the organization to bypass the approved data transfer process. Therefore, an email or data loss prevention (DLP) program is needed to filter data and take appropriate actions at this exit point. DLP programs can help prevent data exfiltration via USB devices as well.

Software development organizations, especially, can benefit from having a separate, disconnected network for source code and other software-related IP. This development network should not

[28] http://msdn.microsoft.com/en-us/library/bb530324.aspx

connect to any other organizational network, have Internet access, or allow unrestricted access to removable media capabilities. This eliminates the possibility of emailing sensitive data from the development network and forces users to use the data transfer process, if established, for moving data between systems.

Organizations must also understand and define all network connections to their organization, also called a network enclave, which Gezelter defines as "an information system environment that is end-to-end under the control of a single authority and has a uniform security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave" [Gezelter 2002].

Connections to an Internet service provider or a trusted business partner are outside of the organization's enclave and are potential exit points for sensitive company information.[29] Data passing through them requires further scrutiny. Organizations should consider capturing full packet content at the perimeter or, at a minimum, capturing network flow data and alerting on anomalies at these exit points. Anomalies may include large amounts of data being sent out from a particular device. A better alternative is to proxy all traffic entering and exiting the enterprise, which allows inspection of unencrypted communications. When possible, encrypted web sessions should be decrypted and inspected. There are commercial products that allow decryption and inspection of SSL-encrypted traffic. Organizations must consider implementing a web-filtering solution that blocks access to certain websites. Typical block lists may include competitors' sites[30] and known malicious domains. Malicious insiders have been known to send sensitive company information to a personal email account or use a free webmail service to exfiltrate data. Many commercial and open source solutions can filter on a variety of effects. Any solution that is implemented within an organization should be able to filter not only on domain names, but also on IP addresses and ranges.

If certain employees need access to SSH, FTP, or SFTP, a limited access terminal, or "jump box," should be used. A typical jump box is a computer configured to allow only certain users, often those with a justifiable business need, to have access to administrative tools, and logging of jump boxes is verbose. In addition, devices administered by a jump box use certain ports and protocols to allow only that box to connect. Some commercial solutions allow for complete video capture of the user's session. This would allow management or security personnel to review what commands were executed and by whom on a particular system. Session video capture has the added benefit of clarifying what changes were made to a system should it malfunction.

Organizations also need to be aware of cloud-based services, or software as a service (SaaS). These services, such as email, online storage, or online office productivity suites, present another opportunity for data exfiltration. Generally, these types of offerings are outside of the organization's enclave, so they may offer little control of where data is stored or transmitted. Malicious insiders could use these services, especially cloud storage and email services, to

[29] Organizations should notify employees through an acceptable-use policy that their Internet use and use of private email on employer resources will be scrutinized.

[30] There are legitimate reasons for browsing a competitor's website. However, for OPSEC, the organization should consider doing so from a computer that cannot be attributed to that organization.

exfiltrate data. Organizations should carefully monitor and restrict access to these services, such as by proxying all network traffic and implementing block lists as previously discussed.

Finally, malicious insiders have exfiltrated information by using other devices within the organization, such as printers, scanners, copiers, and fax machines. For example, if an organization rarely monitors printers and copiers, attackers can simply print or copy large volumes of information and carry it out the door. Insiders have used fax machines to transmit data to a remote fax machine without detection. Scanners can be used to scan hard copies of documents for exfiltration. Organizations must carefully control and monitor these devices. Where possible, organizations should use print servers to facilitate logging. These logs may be helpful in detecting anomalous behavior, such as a large amount of sensitive documents being printed or documents being printed after normal work hours.

19.2 Challenges

1. balancing security with productivity—Organizations may find it challenging to determine an appropriate level of security to prevent data leakage while enabling employees to telecommute and freely collaborate with other organizations.
2. getting a return on investment—Organizations need to weigh the costs and risks of data exfiltration against the costs of protection mechanisms and their effects on productivity.

19.3 Case Studies

In one case, a top executive of a beverage manufacturer employed the insider as an executive administrative assistant. The insider's proximity to the executive granted her access to the organization's trade secret information, including confidential and proprietary documents as well as product samples that had not been publicly released. Video surveillance captured the insider placing trade secret documents and a product sample into her bag. The insider copied some documents and physically stole others. The insider also printed copies of an executive's email regarding one of the victim organization's secret projects. Two co-conspirators, both outsiders with criminal records, aided the insider. The primary co-conspirator contacted a competitor organization via letter and offered to sell the victim organization's trade secrets. The primary co-conspirator faxed additional information to the competitor organization, including a copy of the sensitive email regarding the victim organization's secret project and information regarding a bank account belonging to a beneficiary organization that was owned by the co-conspirators. Fortunately, the competitor notified authorities, and the individuals responsible were arrested after the FBI conducted an undercover investigation.

This case illustrates several methods an insider may use to exfiltrate data. Organizations need to be aware of all data exfiltration points within the organization and include them as part of an enterprise risk assessment. Organizations can then implement mitigation strategies to reduce the identified risks.

In another case, a chemical manufacturing company employed the insider, a resident alien, as a senior research scientist. The insider was working on a multimillion-dollar project related to chemicals used in the production of a new electronic technology. In the month after the insider announced his resignation, the insider emailed a Microsoft Word document detailing the chemical procedure to his email account at the beneficiary organization. At the victim organization, the

insider repeatedly inquired about transferring the data from his company laptop to the victim organization's foreign branch. The organization consistently responded that the transfer would require approval. The insider attempted to force the transfer by asking the IT department how to perform the transfer, falsely stating that it had been approved. Before the insider's departure, the victim organization performed a forensic examination on the insider's computer, which was standard procedure for transferring employees. The day after the organization returned the insider's laptop, while on-site and during early morning hours, the insider downloaded more than 500 documents from the laptop to an external storage device. A few days later, the victim organization confronted the insider about downloading confidential documents and his connection to the beneficiary organization. The insider initially confessed that he had downloaded documents to an external drive, but he denied any additional actions or connections to the beneficiary organization. The insider considered the documents to be reference materials. A subsequent investigation revealed that the insider had copied the documents to his personal computer, and there was evidence that the insider had transferred information to his personal online email account. The incident was detected before the information could be shared with the beneficiary organization.

In a third case, a tax preparation service employed an insider as a tax preparer. While on-site and during work hours, the insider printed PII on at least 30 customers. The insider used this information to submit fraudulent tax returns with false aliases and the correct SSNs. The refunds, totaling $290,000, were deposited into 17 bank accounts.

These three cases highlight several methods insiders use to remove data from a system. Organizations must implement safeguards to prevent unauthorized data removal or transfers. Technologies exist that allow organizations to define policies that control how data is moved to removable devices or how the material may be printed. Organizations should consider these options after carefully performing an enterprise-wide risk assessment that includes the scenarios mentioned in this guide.

19.4 Quick Wins and High-Impact Solutions

19.4.1 All Organizations

- ☐ Establish a cloud computing policy. Organizations must be aware of cloud computing services and how employees may use them to exfiltrate data. Restrict and/or monitor what employees put into the cloud.
- ☐ Monitor the use of printers, copiers, scanners, and fax machines. Where possible, review audit logs from these devices to discover and address any anomalies.
- ☐ Create a data transfer policy and procedure to allow sensitive company information to be removed from organizational systems only in a controlled way.
- ☐ Establish a removable media policy and implement technologies to enforce it.
- ☐ Restrict data transfer protocols, such as FTP, SFTP, or SCP, to employees with a justifiable business need, and carefully monitor their use.

19.4.2 Large Organizations

- ☐ Inventory all connections to the organization's enclave. Ensure that SLAs and/or memoranda of agreement (MOAs) are in place. Verify that these connections are still in use and have a justified business need. Implement protection measures, such as firewalls, devices that capture and analyze IP traffic flow, and IDSs at these ingress and egress points so that data can be monitored and scrutinized.
- ☐ Isolate development networks and disable interconnections to other systems or the Internet.

19.5 Mapping to Standards

- NIST: AC-20, AT-2, CA-3, CM-7, CM 10-11, MP-2, MP-3, MP-5, PE 5-6, SC-7
- NITTF: C-1-1
- Minimum Standards: G-1-a, G-1-b
- CERT-RMM:
  - Technology Management
    - SG2 Protect Technology Assets
- ISO 27002:
  - 12.5.4 Information leakage

Practice 20: Develop a comprehensive employee termination procedure.

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	

Organizations need a termination procedure that reduces the risk of damage from former employees. Termination procedures should ensure that the former employee's accounts are closed, his or her equipment is collected, and the remaining personnel are notified. Proper account and inventory management processes can help an organization reduce the insider threat risk when an employee separates from the company.

20.1 Protective Measures

To prepare for an employee's departure, organizations must address a number of areas before the employee's last day. Organizations must develop policies and procedures that encompass all aspects of the termination process. A termination checklist can help organizations track the various steps an employee needs to complete. At a minimum, a termination checklist should include the task, who should complete the task, who should verify task completion, when the task needs to be completed by, and a signature line for the initials of the person completing the task. The completed checklist should be returned to HR before the employee leaves the organization. Below is a list of areas that organizations should address during a termination and include on a termination checklist:

- Manager
  - Ensure an exit interview is scheduled and completed by the next higher level of management or HR.
  - Provide final performance appraisal feedback.
  - Collect final timesheets.
  - Determine where final paycheck is to be mailed.
- Finance department
  - Ensure employee returns company credit cards, calling cards, purchasing cards, and so on.
  - Close the accounts.
- IT Security department or information systems security officer (ISSO)
  - Notify systems administrators of account suspension and archiving. The system or network administrator should do the following:
    - Terminate all accounts (VPN, email, network logins, cloud services, specialized applications, company-owned social media site accounts, backup accounts).
    - For departing privileged users, change all shared account passwords, service accounts, network devices (routers, switches, etc.), test accounts, jump boxes, and so on.

  - Collect remote access tokens (two-factor authentication devices).
  - Update access lists to sensitive areas (server rooms, data centers, backup media access, etc.).
  - Remove employee from all distribution lists and automated alerts.
- Configuration manager
  - Ensure employee returns all equipment, such as software, laptop, tablet, netbook, and smartphone.
  - Verify returned equipment against inventory.
- Records department
  - Ensure employee returns any company-owned or controlled documents.
- Physical Security department
  - Collect identification badge, keys, access cards, parking pass, and so on.
  - Provide security debriefing.
- HR department
  - Obtain forwarding mailing address.
  - Complete separation paperwork.
  - Notify organization of separation.
  - Reaffirm any IP and nondisclosure agreements.
- Facilities
  - Collect desk phone.
  - Clear work area.

The CERT insider threat database includes cases that involved unreturned company-owned property. As part of the separation process, the organization must collect its physical property, including badges, access cards, keys, two-factor authentication tokens, mobile devices, and laptops. Any of these items, if not returned, may enable the former employee to attack the organization. Collecting these items cannot completely prevent such attacks, but it does mitigate the risk. A physical inventory system that tracks all equipment issued to employees allows an organization to understand who has what property at any given time.

Another step in the separation process is to reaffirm with the departing employee any agreements about IP and nondisclosure. This is an opportunity to remind the employee about his or her obligations to the company even after separation.

Finally, organizations should conduct a review of the departing employee's online actions around the time of the employee's termination. CERT's findings, along with feedback from those who run insider threat programs, suggest that at least 30 days of an employee's activity prior to and after termination should be reviewed, but the organization should review 90 days of activity if the data is available [Hanley and Montelibano 2011b]. This review should include email activity to ensure that the employee has not emailed sensitive company data outside the organization, such as to a personal email account or a competitor. If the organization allows employees to access cloud-based, personal email services, the organization should maintain access logs, such as proxy server logs, to these services and network flow data so that it can detect unusual traffic flow.

Furthermore, the organization should carefully monitor or block personal, cloud-based storage solutions to ensure that employees are not storing sensitive company information in the cloud.

Once an employee has left the organization, HR should notify all employees of the separation. HR may be reluctant to do this because of privacy concerns, but it does not need to say how or why the employee left the organization. A simple message, such as "Joe Smith no longer works for the company. Please do not disclose confidential information to Joe Smith" should suffice to notify employees. Informed employees will be able to alert management and security if they observe a former employee in the organization's facility. If employees do not know about terminations, they may unintentionally disclose sensitive information to former co-workers, open themselves to social engineering attacks, let the former colleague back into the facility, or unknowingly participate in a malicious act.

20.2 Challenges

1. disclosing information—Organizations may have legal concerns regarding how much information to release about a recently terminated employee.
2. completing exit procedures—Each department within an organization may need its own termination checklist tailored to that department's needs.

20.3 Case Studies

In one case, the victim organization terminated the insider from his position as the director of information technology. About a month later, the insider used his old administrative account and password, which the organization had not removed, to remotely access the company's web server hosted by a third party in another state. He deleted approximately 1,000 files from the web server to avenge his termination.

In another case, a systems administrator for a unified messaging service discovered a security vulnerability in the organization's email service. The insider reported the vulnerability to management, but the organization did nothing to fix it. The insider eventually resigned from the company and went to work for another company. Six months after leaving the victim organization, the insider used a valid email account, which the victim organization had not disabled, to email 5,600 of the organization's customers. The emails disclosed the email security flaw and directed customers to the insider's personal website for instructions on how to secure their accounts. The emails crashed the victim organization's servers and caused irreparable damage to its reputation, forcing the organization to go out of business shortly afterward.

The CERT insider threat database contains many cases of organizations failing to delete or block all the accounts associated with a former employee. Well-defined termination procedures coupled with solid account management processes should increase an organization's confidence that former employees can no longer access its systems.

20.4 Quick Wins and High-Impact Solutions

20.4.1 All Organizations

☐ Develop an enterprise-wide checklist to use when someone separates from the organization.

- ☐ Establish a process for tracking all accounts assigned to each employee.
- ☐ Reaffirm all nondisclosure and IP agreements as part of the termination process.
- ☐ Notify all employees about any employee's departure, where permissible and appropriate.
- ☐ Archive and block access to all accounts associated with a departed employee.
- ☐ Collect all of a departing employee's company-owned equipment before the employee leaves the organization.

20.4.2 Large Organizations

- ☐ Establish a physical-inventory system that tracks all assets issued to an employee.
- ☐ Conduct an inventory of all information systems and audit the accounts on those systems.

20.5 Mapping to Standards

- NIST: PS-4, PS-5, PS-7
- NITTF:N/A
- Minimum Standards: G-1-c
- CERT-RMM:
  - Human Resources Management
- ISO 27002:
  - 8.3.1 Termination responsibilities
  - 8.3.2 Return of assets
  - 8.3.3 Removal of access rights

Appendix A: Acronyms

AC	Access Control Family
ACL	access control lists
AT	Awareness and Training Family
AU	Audit Family
CA	Security Assessment and Authorization Family
CD-RW	rewritable compact disk
CEO	chief executive officer
CFO	chief financial officer
CIO	chief information officer
CISO	chief information security officer
CM	Configuration Management Family
COO	chief operating officer
COTR	Contracting Officer's Technical Representative
CP	Contingency Planning Family
CSIRT	Computer Security Incident Response Team
DBA	database administrator
DDoS	distributed denial of service
DHS	Department of Homeland Security
DISC	Disclosure
DLP	data loss prevention
DoS	denial of service
DVD-RW	rewritable digital versatile disk
EAP	employee assistance program
EEOC	Equal Employment Opportunity Commission
EPS	events per second
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FNR	Federal Network Resilience
FTP	File Transfer Protocol
GAO	Government Accountability Office
HR	human resources
HVAC	heating, ventilation, and air conditioning
IA	Identification and Authentication Family
IA	information assurance
IDS	intrusion detection system

IEC	International Electrotechnical Commission
IP	intellectual property
IP	Internet protocol
IPS	intrusion prevention system
IR	Incident Response Family
ISO	International Organization for Standardization
ISSO	information systems security officer
IT	information technology
LDAP	Lightweight Directory Access Protocol
MA	Maintenance Family
MB	megabyte
MMS	Multimedia Messaging Service
MOA	memorandum of agreement
MP	Media Protection Family
NDA	nondisclosure agreement
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPSEC	operations security
OSHA	Occupational Safety and Health Act
PDF	Portable Document Format
PE	Physical and Environmental Protection Family
PGP	pretty good privacy
PHYS	Physical Document
PII	personally identifiable information
PL	Planning Family
PM	Program Management Family
PORT	Portable Device
PS	Personnel Security Family
RA	Risk Assessment Family
SA	Services and Acquisitions Family
SaaS	software as a service
SAN	storage area network
SAPM	shared account password management
SC	Secure Communications Family
SCP	Secure Copy Protocol
SD	secure digital
SI	System and Information Integrity Family
SIEM	security information and event management

SLA	Service level agreement
SMTP	Simple Mail Transfer Protocol
SOC	Security Operations Center
SSH	Secure Shell
SSN	Social Security number
UIT	Unintentional Insider Threat
USB	universal serial bus
USDA	United States Department of Agriculture
VP	vice president
VPN	virtual private network

Appendix B: Sources of Best Practices

Appendix B lists additional sources for best practices that were not included in this guide.

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

British Standards Institute. http://www.bsigroup.com/ (2015).

Corporate Information Security Working Group (CISWG). Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. *Report of the Best Practices and Metrics Teams*," 2005. https://net.educause.edu/ir/library/pdf/CSD3661.pdf

Department of Homeland Security, National Cyber Security Division. *Build Security In*. 2015. https://buildsecurityin.us-cert.gov/daisy/bsi/home.html

Federal Financial Institutions Examination Council. *FFIEC Information Technology Examination Handbook.* http://ithandbook.ffiec.gov/ (2015).

Information Security Forum. *The Standard of Good Practice*. https://www.securityforum.org/ (2015)

Information Systems Audit and Control Association. http://www.isaca.org (2015).

International Organization for Standardization. *Information Technology – Security Techniques – Information Security Management Systems – Requirements* (ISO/IEC 27001:2005). 2013. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103

International Organization for Standardization. *Information Technology – Security Techniques – Code of Practice for Information Security Management* (ISO/IEC 27002). 2013. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50297

MasterCard Worldwide. *The MasterCard SDP Program (Site Data Protection)*. http://www.mastercard.com/sdp (2015).

National Institute of Standards and Technology. *Special Publications (800 Series).* 2015. http://csrc.nist.gov/publications/PubsSPs.html

Payment Card Industry (PCI) *Data Security Standard*. 2015 https://www.pcisecuritystandards.org/

Software Engineering Institute. *Survivability and Information Assurance Curriculum* (SIA). CERT Division, Software Engineering Institute, Carnegie Mellon University. http://www.cert.org/sia (2015).

Software Engineering Institute. *Virtual Training Environment* (VTE). Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9079

AXELOS, Information Technology Infrastructure Library. https://www.axelos.com/best-practice-solutions/itil/what-is-itil (2015).

Appendix C: Best Practices Mapped to Standards

Table 5: Best Practices Mapped to Standards

Practice Number	Best Practice	NIST Controls	NITTF	Minimum Standards	CERT-RMM	ISO 27002
1	Know and protect your assets.	CP -2, CM-2, CM-8, PM-5, PM-8, RA-2	• B-2	• G-1-b, G-1-c	• Asset Definition and Management • Enterprise Focus	• 7.1.1 Inventory of assets
2	Develop a formalized insider threat program.	AT-2, AU-6, IR-4, SI-4	• B	• G-1	• Incident Management and Control • Vulnerability Analysis and Resolution	• 6.1.2 Information security coordination • 15.1.5 Prevention of misuse of information processing facilities
3	Clearly document and consistently enforce policies and controls.	PL-1, PL-4, PS-8	• N/A	• N/A	• Compliance	• 15.2.1 Compliance with security policies and standards
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	PS-1, PS-2, PS-3, PS-8	• C-1-1, C-1-2	• H	• Monitoring • Human Resources	• 8.1.2 Screening
5	Anticipate and manage negative issues in the work environment.	PL-4, PS-1, PS-6, PS-8	• C-1-2	• E	• Human Resources • HRM:SG3.SP4 Establish Disciplinary Process	• 8.2.1 Management responsibilities • 8.2.3 Disciplinary process • 8.3.1 Termination responsibilities
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.	RA-1, RA-3, PM-9	• B-2, C-6	• E-1, G, J	• External Dependencies Management • Human Resources Management • Access Control and Management	• Identification of risks related to external parties • Addressing security when dealing with customers • 6.2.3 Addressing security in third party agreements
7	Be especially vigilant regarding social media.	AT-2, AT-3	• C-1-2	• E-1, G-1-a	• Monitoring	N/A

Practice Number	Best Practice	NIST Controls	NITTF	Minimum Standards	CERT-RMM	ISO 27002
8	Structure Management and Tasks to Minimize Insider Stress and Mistakes.	AC-5 AC 16-22 CM 1-7 CM 8-10 MP 1-2 PE 2-5 SC-4	• C-1-3	• G-2, G-4, I-1, I-2, I-3	• Risk Management	• N/A
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	AT-1, AT-2, AT-3	• C-1-3	• I	• Organizational Training and Awareness	• 8.2.2 Information security awareness, education, and training
10	Implement strict password and account management policies and practices.	AC-2, IA-2	• B-7, C-1-4	• G-1-b	• Identity/Access Management	• 11.2.3 User password management • 11.2.4 Review of user access rights
11	Institute stringent access controls and monitoring policies on privileged users.	AC-2, AC-6, AC-17, AU-2, AU-3, AU-6, AU-9, CM-5, IA-2, MA-5, PL-4, SA-5	• C-1-1	• H-1	• Identity/Access Management • Monitoring	• 10.10.4 Administrator and operator logs • 10.10.2 Monitoring system use
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.	AU-1, AU-2, AU-6, AU-7, AU-12	• C-1-1, C-1-2, C-1-4	• H-1	• Monitoring	• 10.10.1 Audit logging • 10.10.2 Monitoring system use
13	Monitor and control remote access from all end points, including mobile devices.	AC-2, AC-17, AC-19	• C-1-1	• E-1	• Technology Management • TM:SG2.SP2 Establish and Implement Controls	• 11.4.2 User authentication for external connections • 11.7.1 Mobile computing and communications
14	Establish a baseline of normal behavior for both networks and employees.	AC-17, CM-7, SC-7	• C-1-2	• E-1	• Monitoring	N/A
15	Enforce separation of duties and least privilege.	AC-5, AC-6	• B-2	• G-1-a, G-1-b	• Access Management	• 10.1.3 Segregation of duties • 11.2.2 Privilege management

Practice Number	Best Practice	NIST Controls	NITTF	Minimum Standards	CERT-RMM	ISO 27002
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.	AC-ALL, AU-ALL, RA-ALL, SC-ALL, SA-ALL	· N/A	· H-1	· External Dependencies Management	· Identification of risks related to external parties · Addressing security in third party agreements · 10.2.1 Service delivery · 10.2.2 Monitoring and review of third party services · 10.2.3 Managing changes to third party services
17	Institutionalize system change controls.	CM-1, CM-3, CM-4, CM-5, CM-6	· N/A	· N/A	· Technology Management · TM:SG4.SP3 Perform Change Control and Management	· 10.1.2 Change management
18	Implement secure backup and recovery processes.	CP-6, CP-9, CP-10	· N/A	· N/A	· Knowledge and Information Management · KIM:SG6.SP1 Perform Information Duplication and Retention	· 10.5.1 Information back-up
19	Close the doors to unauthorized data exfiltration.	AC-20, CA-3, CM-7, MP-2, MP-3, MP-5, PE-5, SC-7	· C-1-1	· G-1-a, G-1-b	· Technology Management · TM:SG2 Protect Technology Assets	· 12.5.4 Information leakage
20	Develop a comprehensive employee termination procedure.	PS-4, PS-5	· N/A	· G-1-c	· Human Resources	· 8.3.1 Termination responsibilities · 8.3.2 Return of assets · 8.3.3 Removal of access rights

Appendix D: Best Practices by Organizational Group

Table 6: Best Practices for All Organizational Groups

Practice		HR	Legal	Physical Security	Data Owners	IT	Software Engineering
1	Know and protect your critical assets.	✓	✓	✓	✓	✓	✓
2	Develop a formalized insider threat program.	✓	✓	✓	✓	✓	✓
3	Clearly document and consistently enforce policies and controls.	✓	✓	✓		✓	
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	✓	✓	✓	✓	✓	✓
5	Anticipate and manage negative issues in the work environment.	✓	✓	✓	✓	✓	
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.	✓	✓	✓	✓	✓	
7	Be especially vigilant regarding social media.	✓	✓	✓	✓	✓	
8	Structure management and tasks to minimize insider stress and mistakes.	✓	✓	✓	✓	✓	✓
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	✓	✓	✓	✓	✓	✓
10	Implement strict password and account management policies and practices.	✓	✓			✓	
11	Institute stringent access controls and monitoring policies on privileged users.	✓	✓			✓	✓
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.	✓	✓	✓	✓	✓	✓
13	Monitor and control remote access from all end points, including mobile devices.				✓	✓	
14	Establish a baseline of normal behavior for both networks and employees.				✓	✓	
15	Enforce separation of duties and least privilege.	✓	✓	✓	✓	✓	✓
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.		✓	✓	✓	✓	
17	Institutionalize system change controls.				✓	✓	✓
18	Implement secure backup and recovery processes.				✓	✓	
19	Close the doors to unauthorized data exfiltration.			✓	✓	✓	
20	Develop a comprehensive employee termination procedure.	✓	✓	✓	✓	✓	

Table 7: Human Resources Best Practices

Practice #	Practice
1	Know and protect your critical assets.
2	Develop a formalized insider threat program.
3	Clearly document and consistently enforce policies and controls.
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5	Anticipate and manage negative issues in the work environment.
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.
7	Be especially vigilant regarding social media.
8	Structure management and tasks to minimize insider stress and mistakes.
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.
10	Implement strict password and account management policies and practices.
11	Institute stringent access controls and monitoring policies on privileged users.
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
15	Enforce separation of duties and least privilege.
20	Develop a comprehensive employee termination procedure.

Table 8: Legal Best Practices

Practice #	Practice
1	Know and protect your critical assets.
2	Develop a formalized insider threat program.
3	Clearly document and consistently enforce policies and controls.
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5	Anticipate and manage negative issues in the work environment.
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.
7	Be especially vigilant regarding social media.
8	Structure management and tasks to minimize insider stress and mistakes.
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.
10	Implement strict password and account management policies and practices.
11	Institute stringent access controls and monitoring policies on privileged users.
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
15	Enforce separation of duties and least privilege.
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
20	Develop a comprehensive employee termination procedure.

Table 9: Physical Security Best Practices

Practice #	Practice
1	Know and protect your critical assets.
2	Develop a formalized insider threat program.
3	Clearly document and consistently enforce policies and controls.
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5	Anticipate and manage negative issues in the work environment.
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.
7	Be especially vigilant regarding social media.
8	Structure management and tasks to minimize insider stress and mistakes.
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
15	Enforce separation of duties and least privilege.
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
19	Close the doors to unauthorized data exfiltration.
20	Develop a comprehensive employee termination procedure.

Table 10: Data Owners Best Practices

Practice #	Practice
1	Know and protect your critical assets.
2	Develop a formalized insider threat program.
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5	Anticipate and manage negative issues in the work environment.
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.
7	Be especially vigilant regarding social media.
8	Structure management and tasks to minimize insider stress and mistakes.
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
13	Monitor and control remote access from all end points, including mobile devices.
14	Establish a baseline of normal behavior for both networks and employees.
15	Enforce separation of duties and least privilege.
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
17	Institutionalize system change controls.
18	Implement secure backup and recovery processes.
19	Close the doors to unauthorized data exfiltration.
20	Develop a comprehensive employee termination procedure.

Table 11: Information Technology Best Practices

Practice #	Practice
1	Know and protect your critical assets.
2	Develop a formalized insider threat program.
3	Clearly document and consistently enforce policies and controls.
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5	Anticipate and manage negative issues in the work environment.
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.
7	Be especially vigilant regarding social media.
8	Structure management and tasks to minimize insider stress and mistakes.
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.
10	Implement strict password and account management policies and practices.
11	Institute stringent access controls and monitoring policies on privileged users.
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
13	Monitor and control remote access from all end points, including mobile devices.
14	Establish a baseline of normal behavior for both networks and employees.
15	Enforce separation of duties and least privilege.
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
17	Institutionalize system change controls.
18	Implement secure backup and recovery processes.
19	Close the doors to unauthorized data exfiltration.
20	Develop a comprehensive employee termination procedure.

Table 12: Software Engineering Best Practices

Practice #	Practice
1	Know and protect your critical assets.
2	Develop a formalized insider threat program.
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
8	Structure management and tasks to minimize insider stress and mistakes.
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.
11	Institute stringent access controls and monitoring policies on privileged users.
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
15	Enforce separation of duties and least privilege.
17	Institutionalize system change controls.

Appendix E: Checklists of Quick Wins and High-Impact Solutions

This appendix compiles the checklists of "Quick Wins and High-Impact Solutions" from each best practice, for convenient reference.

1. Practice 1 - Know and protect your critical assets.

a. All Organizations

- ☐ Conduct a physical asset inventory. Identify asset owners' assets and functions; also identify the type of data on the system.
- ☐ Understand what data your organization processes by speaking with data owners and users from across your organization.
- ☐ Identify and document the software configurations of all assets.
- ☐ Prioritize assets and data to determine the high-value targets.

2. Practice 2 - Develop a formalized insider threat program.

a. All Organizations

- ☐ Ensure that legal counsel determines the legal framework the team will work in.
- ☐ Establish policies and procedures for addressing insider threats that include HR, Legal, Security, management, and IA.
- ☐ Consider establishing a contract with an outside consulting firm that is capable of providing incident response capabilities for all types of incidents, if the organization has not yet developed the expertise to conduct a legal, objective, and thorough inquiry.

b. Large Organizations

- ☐ Formalize an insider threat program (with a senior official of the organization appointed as the program manager) that can monitor for and respond to insider threats.
- ☐ Implement insider threat detection rules into SIEM systems. Review logs on a continuous basis and ensure watch lists are updated.

Ensure the insider threat team meets on a regular basis and maintains a readiness state.

3. Practice 3 - Clearly document and consistently enforce policies and controls.

a. All Organizations

The following considerations apply to organizations of all sizes. Some organizations may not have a department dedicated to security (physical security, IT security, etc.). However, the underlying theme of the practice still applies.

- ☐ Ensure that senior management advocates, enforces, and complies with all organizational policies. Policies that do not have management buy-in will fail and not be enforced equally. Management must also comply with policies. If management does not do so, subordinates will see this as a sign that the policies do not matter or they are being held to a different standard than management. Your organization should consider exceptions to policies in this light as well.
- ☐ Ensure that management briefs all employees on all policies and procedures. Employees, contractors, and trusted business partners should sign acceptable-use policies upon their hiring and once every year thereafter or when a significant change occurs. This is also an opportunity for your organization and employees, contractors, or trusted business partners to reaffirm any nondisclosure agreements.
- ☐ Ensure that management makes policies for all departments within your organization easily accessible to all employees. Posting policies on your organization's internal website can facilitate widespread dissemination of documents and ensure that everyone has the latest copy.
- ☐ Ensure that management makes annual refresher training for all employees mandatory. Refresher training needs to cover all facets of your organization, not just information security. Training should encompass the following topics: human resources, legal, physical security, and any others of interest. Training can include, but is not limited to, changes to policies, issues that have emerged over the past year, and information security trends.

Ensure that management enforces policies consistently to prevent the appearance of favoritism and injustice. The Human Resources department should have policies and procedures in place that specify the consequences of particular policy violations. This will facilitate clear and concise enforcement of policies.

4. Practice 4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

a. All Organizations

- ☐ Ensure that potential employees have undergone a thorough background investigation, which at a minimum should include a criminal background and credit check.
- ☐ Encourage employees to report suspicious behavior to appropriate personnel for further investigation.
- ☐ Investigate and document all issues of suspicious or disruptive behavior.

- ☐ Enforce policies and procedures consistently for all employees.
- ☐ Consider offering an EAP. These programs can help employees deal with many personal issues confidentially.

5. Practice 5 - Anticipate and manage negative issues in the work environment.

a. All Organizations

- ☐ Enhance monitoring of employees with an impending or ongoing personnel issue, in accordance with organizational policy and laws. Enable additional auditing and monitoring controls outlined in policies and procedures. Regularly review audit logs to detect activities outside of the employee's normal scope of work. Limit access to these log files to those with a need to know.
- ☐ All levels of management must regularly communicate organizational changes to all employees. This allows for a more transparent organization, and employees can better plan for their future.

6. Practice 6 - Consider threats from insiders and business partners in enterprise-wide risk assessments.

a. All Organizations

- ☐ Have all employees, contractors, and trusted business partners sign nondisclosure agreements (NDAs) upon hiring and termination of employment or contracts.
- ☐ Ensure each trusted business partner has performed background investigations on all of its employees who will have access to your organization's systems or information. These should be commensurate with your organization's own background investigations and required as a contractual obligation.
- ☐ If your organization is acquiring companies during a merger or acquisition, perform background investigations on all employees to be acquired, at a level commensurate with your organization's policies.
- ☐ Prevent sensitive documents from being printed if they are not required for business purposes. Insiders could take a printout of their own or someone else's sensitive document from a printer, desk, office, or from garbage. Electronic documents can be easier to track.
- ☐ Avoid direct connections with the information systems of trusted business partners if possible. Provide partners with task-related data without providing access to your organization's internal network.
- ☐ Restrict access to the system backup process to only administrators responsible for backup and restoration.

b. Large Organizations

- ☐ Prohibit personal items in secure areas because they may be used to conceal company property or to copy and store company data.
- ☐ Conduct a risk assessment of all systems to identify critical data, business processes, and mission-critical systems. (See NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems* for guidance [NIST 2002].) Be sure to include insiders and trusted business partners as part of the assessment. (See Section 3.2.1, "Threat-Source Identification," of NIST SP 800-30.)
- ☐ Implement data encryption solutions that encrypt data seamlessly and that restrict encryption tools to authorized users, as well as restrict decryption of organization-encrypted data to authorized users.
- ☐ Implement a clear separation of duties between regular administrators and those responsible for backup and restoration.
- ☐ Forbid regular administrators' access to system backup media or the electronic backup processes.

7. Practice 7 - Be especially vigilant regarding social media.

a. All Organizations

- ☐ Establish a social media policy that defines acceptable uses of social media and information that should not be discussed online.
- ☐ Include social media awareness training as part of the organization's security awareness training program.
- ☐ Encourage users to report suspicious emails or phone calls to the information security team, who can track these emails to identify any patterns and issue alerts to users.

b. Large Organizations

- ☐ Consider monitoring the use of social media across the organization, limited to looking in a manner approved by legal counsel for postings by employees, contractors, and business partners.

8. Practice 8 - Structure management and tasks to minimize insider stress and mistakes.

a. All Organizations

- ☐ Establish a work culture that measures success based on appropriate metrics for the work environment. For instance, knowledge workers might measure their success based on outcomes and efficiency instead of metrics that are better suited for a production line.
- ☐ Encourage employees to think through projects, actions, and statements before committing to them.

- ☐ Create an environment that encourages focusing upon one thing at a time, rather than multi-tasking.
- ☐ Offer employees who are under stress options to de-stress, such as massages, time off, games, or other social but non-project-oriented activities.
- ☐ Routinely monitor employee workloads to make sure that they are commensurate with the employee's skills and available resources.

b. Large Organizations

The recommendations in this section apply to all organizations.

9. Practice 9 - Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.

a. All Organizations

- ☐ Develop and implement an enterprise-wide training program that discusses various topics related to insider threat. The training program must have the support of senior management to be effective. Management must be seen participating in the course and must not be exempt from it, which other employees could see as a lack of support and an unequal enforcement of policies.
- ☐ Train all new employees and contractors in security awareness, including insider threat, before giving them access to any computer system. Make sure to include training for employees who may not need to access computer systems daily, such as janitorial and maintenance staff. These users may require a special training program that covers security scenarios they may encounter, such as social engineering, active shooter, and sensitive documents left out in the open.
- ☐ Train employees continuously. However, training does not always need to be classroom instruction. Posters, newsletters, alert emails, and brown-bag lunch programs are all effective training methods. Your organization should consider implementing one or more of these programs to increase security awareness.
- ☐ Establish an anonymous or confidential mechanism for reporting security incidents. Encourage employees to report security issues and consider incentives to reporting by rewarding those who do.

b. Large Organizations

- ☐ The information security team can conduct periodic inspections by walking through areas of your organization, including workspaces, and identifying security concerns. Your organization should bring security issues to the employee's attention in a calm, nonthreatening manner and in private. Employees spotted doing something good for security, like stopping a person without a badge, should be rewarded. Even a certificate or other item of minimal value goes a long way to improving employee morale and increasing security awareness. Where possible, these rewards should be presented before a group of the employee's peers. This type of program does not have to be administered by the security

team but could be delegated to the employee's peer team members or first-level management.

10. Practice 10 - Implement strict password and account management policies and practices.

a. All Organizations

- ☐ Establish account management policies and procedures for all accounts created on all information systems. These policies should address how accounts are created, reviewed, and terminated. In addition, the policy should address who authorizes the account and what data they can access.
- ☐ Perform audits of account creation and password changes by system administrators. The account management process should include creation of a trouble ticket by the help desk. (Help desk staff should not be able to create accounts.) Your organization could confirm the legitimacy of requests to reset passwords or create accounts by correlating such requests with help desk logs.
- ☐ Define password requirements and train users on creating strong passwords. Some systems may tolerate long passwords. Encourage users to use passphrases that include proper punctuation and capitalization, thereby increasing passphrase strength and making it more memorable to the user.
- ☐ Security training should include instruction to block visual access to others as users type their passcodes.
- ☐ Ensure all shared accounts are absolutely necessary and are addressed in a risk management decision.

b. Large Organizations

- ☐ Review systems and risk to determine the feasibility of centrally managing user accounts.
- ☐ If using a central account management system, add contractors to groups linked to projects, organizations, or other logical groups. This allows administrators to quickly identify contractors and change access permissions. Accounts themselves might contain contractor status tipoffs, for example, putting "CONT" in the account name or description.

11. Practice 11 - Institute stringent access controls and monitoring policies on privileged users.

a. All Organizations

- ☐ Conduct periodic account reviews to avoid privilege creep. Employees should have sufficient access rights to perform their everyday duties. When an employee changes roles, the organization should review the employee's account and rescind permissions that the employee no longer needs.

b. Large Organizations

- ☐ Implement separation of duties for all roles that affect the production system. Require at least two people to perform any action that may alter the system.
- ☐ Use multifactor authentication for privileged user or system administrator accounts.[31] Requiring multifactor authentication will reduce the risk of a user abusing privileged access after an administrator leaves your organization, and the increased accountability of multifactor authentication may inhibit some currently employed, privileged users from committing acts of malfeasance. Assuming that the former employee's multifactor authentication mechanisms have been recovered, the account(s) will be unusable.

[35] NIST Special Publication 800-53, AC-6 (Access Control) requires multifactor authentication for moderate- to high-risk systems.

12. Practice 12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources.

a. All Organizations

- ☐ Implement rules within the SIEM system, to automate alerts.
- ☐ Create log management policy and procedures. Ensure they address log retention (consult legal counsel for specific requirements), what logs to collect, and who manages the logging systems.

b. Large Organizations

- ☐ Ensure that someone regularly monitors the SIEM system. Depending on the environment, this may involve multiple personnel who monitor employee activity full-time.

13. Practice 13 - Monitor and control remote access from all end points, including mobile devices.

a. All Organizations

- ☐ Disable remote access to the organization's systems when an employee or contractor separates from the organization. Be sure to disable access to VPN service, application servers, email, network infrastructure devices, and remote management software. Be sure to close all open sessions as well. In addition, collect all company-owned equipment, including multifactor authentication tokens, such as RSA SecurID tokens or smart cards.
- ☐ Include mobile devices, with a listing of their features, as part of the enterprise risk assessment.
- ☐ Prohibit or limit the use of personally owned devices.
- ☐ Prohibit devices with cameras in sensitive areas.

b. Large Organizations

- ☐ Implement a central management system for mobile devices.
- ☐ Monitor and control remote access to the corporate infrastructure. VPN tunnels should terminate at the furthest perimeter device and in front of an IDS and firewall. This allows for packet inspection and network access control. In addition, IP traffic-flow capture and analysis devices placed behind the VPN concentrator will allow collection of network traffic statistics to help discover anomalies. If personally owned equipment, such as a laptop or home computer, is permitted to access the corporate network, it should only be allowed to do so through an application gateway. This will limit the applications available to an untrusted connection.

14. Practice 14 - Establish a baseline of normal behavior for both networks and employees.

a. All Organizations

- ☐ Use monitoring tools to monitor network and employee activity for a period of time to establish a baseline of normal behaviors and trends.
- ☐ Deny VPN access to foreign countries where a genuine business need does not exist. White list only countries where a genuine business need exists.[32]
- ☐ Establish which ports and protocols are needed for normal network activity, and configure devices to use only these services.
- ☐ Determine which firewall and IDS alerts are normal. Either correct what causes these alerts or document normal ranges and include them in the network baseline documentation.

b. Large Organizations

- ☐ Establish network activity baselines for individual subunits of the organization.
- ☐ Determine which devices on a network need to communicate with others and implement access control lists (ACLs), host-based firewall rules, and other technologies to limit communications.
- ☐ Understand VPN user requirements. Limit access to certain hours and monitor bandwidth consumption. Establish which resources will be accessible via VPN and from what remote IP addresses. Alert on anything that is outside normal activity.

15. Practice 15 - Enforce separation of duties and least privilege.

a. All Organizations

- ☐ Carefully audit user access permissions when an employee changes roles within the organization to avoid privilege creep. In addition, routinely audit user access permissions at least annually. Remove permissions that are no longer needed.
- ☐ Establish account management policies and procedures. Audit account maintenance operations regularly. Account activity should reconcile with help desk documentation.
- ☐ Require privileged users to have both an administrative account with the minimum necessary privileges to perform their duties and a standard account that is used for everyday, non-privileged activities.

b. Large Organizations

- ☐ Review positions in the organization that handle sensitive information or perform critical functions. Ensure these employees cannot perform these critical functions without oversight

[32] Regional Internet Registries maintain IP address assignments. Registries include AfriNIC, ARIN, APNIC, LACNIC, and RIPE NCC. Other companies maintain IP data that is available under various licenses, such as http://www.maxmind.com/app/geoip_country and http://www.countryipblocks.net/. Regional Internet registry data will be more accurate.

and approval. The backup and restore tasks are often overlooked. One person should not be permitted to perform both backup and restore functions. Your organization should separate these roles and regularly test the backup and recovery processes (including the media and equipment). In addition, someone other than the backup and restore employees should transport backup tapes off-site.

16. Practice 16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

a. All Organizations

The considerations below apply to any organization utilizing cloud services. Such services not owned and operated by the organization deserve further scrutiny.

- ☐ Conduct a risk assessment of the data and services that your organization plans to outsource to a cloud service provider before entering into any agreement. Your organization must ensure that the service provider poses an acceptable level of risk and has implemented mitigating controls to reduce any residual risks. Your organization must carefully examine all aspects of the cloud service provider to ensure the service provider meets or exceeds your organization's own security practices.
- ☐ Verify the cloud service provider's hiring practices to ensure it conducts thorough background security investigations on any personnel (operations staff, technical staff, janitorial staff, etc.) before they are hired. In addition, the service provider should conduct periodic credit checks and reinvestigations to ensure that changes in an employee's life situation have not caused any additional unacceptable risks.
- ☐ Control or eliminate remote administrative access to hosts providing cloud or virtual services.
- ☐ Understand how the cloud service provider protects data and other organizational assets before entering into any agreement. Verify the party responsible for restricting logical and physical access to your organization's cloud assets.

17. Practice 17 - Institutionalize system change controls.

a. All Organizations

- ☐ Periodically review configuration baselines against actual production systems and determine if any discrepancies were approved. If the changes were not approved, verify a business need for the change.

b. Large Organizations

- ☐ Implement a change management program within the organization. Ensure that a change control board vets all changes to systems, networks, or hardware configurations. All changes

must be documented and include a business reason. Proposed changes must be reviewed by information security teams, system owners, data owners, users, and other stakeholders.

- ☐ The configuration manager must review and submit to the change control board any software developed in-house as well as any planned changes.

18. Practice 18 - Implement secure backup and recovery processes.

a. All Organizations

- ☐ Store backup media off-site. Ensure media is protected from unauthorized access and can only be retrieved by a small number of individuals. Utilize a professional off-site storage facility; do not simply send backup media home with employees. Encrypt the backup media and manage the encryption keys to ensure backup and recovery are possible.
- ☐ Ensure that configurations of network infrastructure devices (e.g., routers, switches, and firewalls) are part of your organization's backup and recovery plan as well as the configuration management plan.

b. Large Organizations

- ☐ Implement a backup and recovery process that involves at least two people: a backup administrator and a restore administrator. Both people should able to perform either role.
- ☐ Regularly test both backup and recovery processes. Ensure that your organization can reconstitute all critical data as defined by the business continuity plan and/or disaster recovery plan. Ensure that this process does not rely on any single person to be successful.

19. Practice 19 - Close the doors to unauthorized data exfiltration.

a. All Organizations

- ☐ Establish a cloud computing policy. Organizations must be aware of cloud computing services and how employees may use them to exfiltrate data. Restrict and/or monitor what employees put into the cloud.
- ☐ Monitor the use of printers, copiers, scanners, and fax machines. Where possible, review audit logs from these devices to discover and address any anomalies.
- ☐ Create a data transfer policy and procedure to allow sensitive company information to be removed from organizational systems only in a controlled way.
- ☐ Establish a removable media policy and implement technologies to enforce it.
- ☐ Restrict data transfer protocols, such as FTP, SFTP, or SCP, to employees with a justifiable business need, and carefully monitor their use.

b. Large Organizations

- ☐ Inventory all connections to the organization's enclave. Ensure that SLAs and/or MOAs are in place. Verify that these connections are still in use and have a justified business need.

Implement protection measures, such as firewalls, devices that capture and analyze IP traffic flow, and IDSs at these ingress and egress points so that data can be monitored and scrutinized.

- ☐ Isolate development networks and disable interconnections to other systems or the Internet.

20. Practice 20 - Develop a comprehensive employee termination procedure.

a. All Organizations

- ☐ Develop an enterprise-wide checklist to use when someone separates from the organization.
- ☐ Establish a process for tracking all accounts assigned to each employee.
- ☐ Reaffirm all nondisclosure and IP agreements as part of the termination process.
- ☐ Notify all employees about any employee's departure, where permissible and appropriate.
- ☐ Archive and block access to all accounts associated with a departed employee.
- ☐ Collect all of a departing employee's company-owned equipment before the employee leaves the organization.

b. Large Organizations

- ☐ Establish a physical-inventory system that tracks all assets issued to an employee.
- ☐ Conduct an inventory of all information systems and audit the accounts on those systems.

Appendix F: Insider Threat Privacy Appendix

Building an effective insider threat program requires enterprise-wide participation, involving representation from senior management, Information Technology, Human Resources, Information Assurance, counterintelligence, law enforcement, contracting/procurement, and General Counsel (see best Practice 2, "Develop a Formalized Insider Threat Program"). It is essential that the concerns of each organization unit are considered when building the insider threat program structure, policy, implementation plan, and incident response capabilities. The goal of the insider threat program should be to protect the organization's critical assets from threats that originate from within the organization, both malicious and non-malicious, but in doing so, should not infringe upon the privacy rights and civil liberties of the individuals working for the organization.

Any well-rounded and properly implemented insider threat program must consider employee privacy. It is essential to maintain a culture that balances achieving the mission of the organization with the ability to support the individuals working at the organization. An organization must determine the appropriate level of trust necessary to give employees while, at the same time, respecting their privacy. Employees need to have clear expectations about what can be performed and expected to remain private while at work. Organizations should work with their legal counsel to define and differentiate between *expectation of privacy* and *right to privacy* and consider those definitions and distinctions when developing, implementing, and monitoring their insider threat program. In addition, consider the implications of both of those issues in relation to implementation inside the United States of America and countries outside of the U.S. Within the U.S., both state and federal law needs to be considered when designing insider threat controls that bear on employee privacy.

Bibliography

[Ariani 2013]
Ariani, Dorothea Wahyu. "The Relationship Between Employee Engagement, Organizational Citizenship Behavior, and Counterproductive Work Behavior." *International Journal of Business Administration 4,* 2 (2013).

[Boudreaux 2009]
Boudreaux, Chris. *Online Database of Social Media Policies.* http://socialmediagovernance.com/policies/ (2012).

[Butler 2009]
Butler, J. Michael. *Benchmarking Security Information Event Management (SIEM).* SANS, February 2009. http://www.sans.org/reading_room/analysts_program/eventMgt_Feb09.pdf

[Caralli et al. 2010]
Caralli, Richard A.; Allen, Julia H; & White David W. *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley Professional, 2010.

[CISCO 2012]
CISCO. *Supplier Information: Diversity Business Practices.* http://www.cisco.com/web/about/ac50/ac142/sdbd/index.html (2015).

[Claycomb and Nicoll 2012]
Claycomb, William R. & Nicoll, Alex. "Insider Threats to Cloud Computing: Directions for New Research Challenges," 387-394. *Proceedings of the 2012 IEEE Computer Software and Applications Conference (COMPSAC)*. Izmir, Turkey, July 16-20, 2012. IEEE, 2012.

[CSA 2010]
Cloud Security Alliance. *Top Threats to Cloud Computing, Version 1.0.* https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (2010).

[Deschenaux 2012]
Deschenaux, Joanne. *Maryland Enacts Country's First Social Media Password Law*. Society for Human Resource Management, 2012. http://www.shrm.org/legalissues/stateandlocalresources/pages/marylandenactscountrysfirst.aspx

[DHS 2011]
Department of Homeland Security. *National Cyber Security Awareness Month.* http://www.dhs.gov/files/programs/gc_1158611596104.shtm (2011).

[EEOC 2012]
U.S. Equal Employment Opportunity Commission. EEOC Enforcement Guidance 915.002. *Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964,* 2012. http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm

[Gallup 2013]
Gallup. “State of the American Workplace: Employee Engagement Insights for U.S. Business Leaders.” http://www.gallup.com/services/178514/state-american-workplace.aspx (2013).

[GAO 2010]
U.S. Government Accountability Office. *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing* (GAO-10-513). U.S. Government Accountability Office, 2010. http://www.gao.gov/new.items/d10513.pdf

[Gezelter 2002]
Gezelter, Robert. Ch. 10, “Mobile Code.” *Computer Security Handbook,* 4th ed. John Wiley & Sons, Inc., 2002.

[Hamblen 2011]
Hamblen, Matt. “Workers Want to Choose Their Mobile Devices, Survey Finds.” 2011. http://www.computerworld.com/article/2509600/mobile-apps/workers-want-to-choose-their-mobile-devices--survey-finds.html

[Hanley et al.2011a]
Hanley, Michael; Dean, Tyler; Schroeder, Will; Houy, Matt; Trzeciak, Randall F.; & Montelibano, Joji. *An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases* (CMU/SEI-2011-TN-006). Software Engineering Institute, Carnegie Mellon University, 2011. http://www.sei.cmu.edu/library/abstracts/reports/11tn006.cfm

[Hanley and Montelibano 2011b]
Hanley, Michael & Montelibano, Joji. *Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination* (CMU/SEI-2011-TN-024). Software Engineering Institute, Carnegie Mellon University, 2011. http://www.sei.cmu.edu/library/abstracts/reports/11tn024.cfm

[Hurlburt et al. 2011]
Hurlburt, G.; Voas, J.; & Miller, K. W. “Mobile-App Addiction: Threat to Security?” *IT Professional 13*, 6 (January-February 2011): 9-11. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6096589

[Infosecurity 2010]
Infosecurity. “Air Force’s Banning of Thumb Drives Temporary Solution to WikiLeaks,” *Infosecurity* (online, December 17, 2010). http://www.infosecurity-magazine.com/view/14762/air-forces-banning-of-thumb-drives-temporary-solution-to-wikileaks/

[INSA 2013]
INSA. *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector*, INSA, September 2013. http://www.insaonline.org/i/d/a/b/InsiderThreat_embed.aspx

[ISO/IEC 2013]
International Organization for Standardization. *ISO/IEC 27002:2013 Information technology -- Security techniques--Code of Practice for information security controls.* http://www.iso.org/iso/catalogue_detail?csnumber=54533

[Johnson et al. 2009]
Johnson, David J.; Takacs, Nicholas; & Hadley, Jennifer. Ch. 36.6, "Securing Stored Data." *Computer Security Handbook, 5th ed.* John Wiley & Sons, Inc., 2009.

[Lew 2011]
Lew, Jacob J. *Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems* (M-11-08). Executive Office of the President, Office of Management and Budget, 2011. http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-08.pdf

[Moore et al. 2015]
Moore, Andrew P.; Novak, William E.; Collins Matthew L.; Trzeciak, Randall F.; & Theis, Michael C. "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls." Software Engineering Institute, Carnegie Mellon University, 2015. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=446367

[Mell and Grance 2011]
Mell, Peter & Grance, Timothy. *The NIST Definition of Cloud Computing* (SP 800-145, Draft). National Institute of Standards and Technology, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[NCSL 2015]
Conference of State Legislators. *Access to Social Media Usernames and Passwords.* 2015. http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspxNational

[NIST 2002]
National Institute of Standards and Technology. *Risk Management Guide for Information Technology Systems* (NIST Special Publication 800-30). National Institute of Standards and Technology, 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[NIST 2010]
National Institute of Standards and Technology. *Guide for Applying the Risk Management Framework to Federal Information Systems* (NIST SP 800-37, Rev. 1). National Institute of Standards and Technology, 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[NIST 2012]
National Institute of Standards and Technology. *Risk Management Framework (RMF) Overview.* National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Center, 2012. http://csrc.nist.gov/groups/SMA/fisma/framework.html

[NIST 2015]
National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information System and Organizations* (NIST SP 800-53, Rev. 4). National Institute of Standards and Technology, 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[Obama 2011]
Obama, Barack. *Executive Order 13587 — Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. The White House, Office of the Press Secretary, 2011. http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

[OSHA 2015]
U.S. Department of Labor Occupational Safety and Health Administration. *OSHA Fact Sheet: Workplace Violence*. https://www.osha.gov/OshDoc/data_General_Facts/factsheet-workplace-violence.pdf

[Ponemon 2011]
Ponemon Institute, LLC. *Security of Cloud Computing Providers Study*. Ponemon Institute, LLC, 2011.

[Purcell 2012]
Purcell, Anne. *Report of the Acting General Counsel Concerning Social Media Cases* (OM 12-59). Office of the General Counsel, 2012. goo.gl/N1ClKE

[PRC 2015]
Privacy Rights Clearinghouse. *Chronology of Data Breaches*. 2015. https://www.privacyrights.org/data-breach

[PWC 2015]
Price Waterhouse Cooper; CSO Magazine; U.S. Secret Service; Deloitte; & Software Engineering Institute CERT Division at Carnegie Mellon University. *Key Findings from the U.S. State of Cybercrime Survey.* 2015. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf

[Raman et al.2009]
Raman, Karthik et al. Ch. 19, “Social Engineering and Low-Tech Attacks.” *Computer Security Handbook*, 5th ed. John Wiley & Sons, Inc., 2009.

[SEI 2007]
Software Engineering Institute, “Over-Confidence Is Pervasive Amongst Security Professionals.” Carnegie Mellon University, 2007. http://www.sei.cmu.edu/news/article.cfm?assetid=52340&article=254&year=2007

[SEI 2013]
Software Engineering Institute, CERT Insider Threat Team. *Insider Threat Science of Cybersecurity* (CMU/SEI-2013-TN-022). Software Engineering Institute, Carnegie Mellon University, 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=77455

[SEI 2014]
Software Engineering Institute, CERT Insider Threat Team. *Unintentional Insider Threats: Social Engineering* (CMU/SEI-2013-TN-024). Software Engineering Institute, Carnegie Mellon University, 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=77455

[Shin et al. 2011]
Shin, Dongwan; Akkan, Hakan; Claycomb, William; & Kim, Kwanjoong. "Toward Role-Based Provisioning and Access Control for Infrastructure as a Service (IaaS)." *Journal of Internet Services and Application 2*, 3 (Dec. 2011): 243-255.

[Shin et al. 2012]
Shin, Dongwan; Wang, Ying; & Claycomb, William. "A Policy-Based Decentralized Authorization Management Framework for Cloud Computing." *Proceedings of the 27th Annual ACM Symposium on Applied Computing*. Riva del Garda (Trento), Italy, March 2012. ACM, 2012.

[Strozer et al.2014]
Strozer, Jeremy R.; Collins, Matthew L; & Cassidy, Tracy. *Unintentional Insider Threats: A Review of Phishing and Malware Incidents by Economic Sector*. Software Engineering Institute, Carnegie Mellon University, 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=296268

[Sulea et al. 2012]
Sulea, Coralia; Virga, Delia; Maricutoiu, Laurentiu, P.; Schaufeli, Wilmar; Dumitru, Catalina Zaborila; & Sava, Florin A. 2012. "Work Engagement as Mediator between Job Characteristics and Positive and Negative Extra-Role Behaviors." *Career Development International 17*, (3): 188–207.

[Tillman 1987]
Tillman, Robert. *Prevalence and Incidence of Arrest Among Adult Males in California* (NCJ 105431). National Institute of Justice Reference Service, 1987. https://www.ncjrs.gov/App/publications/Abstract.aspx?id=105431

[Waterman 2010]
Waterman, Shaun. "Fictitious Femme Fatale Fooled Cybersecurity." *Washington Times*, July 18, 2010. http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity/?page=all

[Wikoff 2015]
Wikoff, Darrin. "How to effectively manage assets by criticality." ReliablePlant, Noria Corporation. January 4, 2004. http://www.reliableplant.com/Read/15166/manage-assets-criticality

[Zetter 2008]
Zetter, Kim. *Palin E-Mail Hacker Says It Was Easy. Wired*, September 18, 2008. http://www.wired.com/2008/09/palin-e-mail-ha/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	March 2016	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Common Sense Guide to Mitigating Insider Threats, Fifth Edition	FA8721-05-C-0003

6. AUTHOR(S)

The CERT Insider Threat Center

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2015-TR-010

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

This fifth edition of the *Common Sense Guide to Mitigating Insider Threats* provides the most current recommendations of the CERT® Division (part of Carnegie Mellon University's Software Engineering Institute), based on an expanded corpus of more than 1,000 insider threat cases and continued research and analysis. It introduces the topic of insider threats, explains its intended audience and how this guide differs from previous editions, defines insider threats, and outlines current patterns and trends. The guide then describes 20 practices that organizations should implement across the enterprise to prevent and detect insider threats, as well as case studies of organizations that failed to do so. Each practice includes features new to this edition: challenges to implementation, quick wins and high-impact solutions for small and large organizations, and relevant security standards. This edition also focuses on six groups within an organization—Human Resources, Legal, Physical Security, Data Owners, Information Technology, and Software Engineering—and maps the relevant groups to each practice. The appendices provide a revised list of information security best practices, a new mapping of the guide's practices to established security standards, a new breakdown of the practices by organizational group, a new look at considerations for employee privacy, and new checklists of activities for each practice.

14. SUBJECT TERMS	15. NUMBER OF PAGES
insider threat, common sense guide, CERT Insider Threat Center, Sabotage, Fraud, Theft of Intellectual Property, Espionage, Unintentional Insider Threat, Behavioral Analytics, Indicators, Data Analysis, Insider Threat Program, CSG	158

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