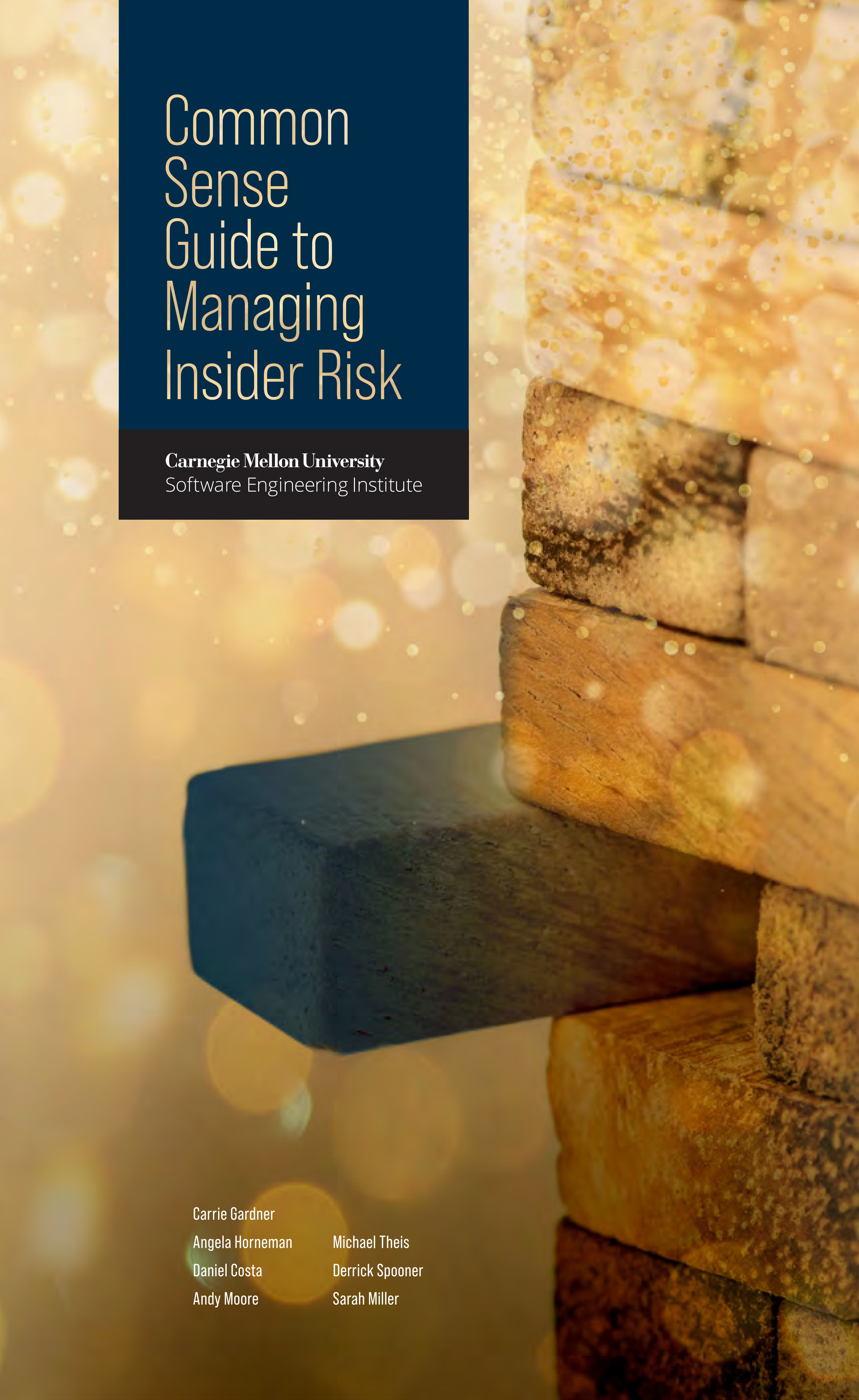


Common Sense Guide to Managing Insider Risk

Carnegie Mellon University
Software Engineering Institute

Carrie Gardner
Angela Horneman
Daniel Costa
Andy Moore
Michael Theis
Derrick Spooner
Sarah Miller

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 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/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM21-0782

Table of Contents

List of Figures

List of Tables

Acknowledgments

Since 2001, members of the technical staff at Carnegie Mellon University's (CMU's) Software Engineering Institute (SEI) have been studying the hard problems of mitigating insider threats and managing insider risk. The work has evolved from a single study sponsored by the United States (U.S.) Secret Service (the *Insider Threat Study* [Conway 2005]) to a collection of over 3,000 insider incidents, more than 150 publications, hundreds of blog posts and presentations, and dozens of fundamental and applied research projects across public and private organizations.

We, as authors of this guide and members of the technical staff at the SEI who are studying this subject area, wish to acknowledge and thank the authors of previous versions of this guide for the tremendous foundation of knowledge we continue to build on. We also want to acknowledge our countless collaborators, both internal and external to CMU and the SEI, who continue to provide the multidisciplinary subject matter expertise that is vital to the continued progress of this research.

For this updated guide, we especially acknowledge the hard work of Isabel Gardner, Harrison Leinweber, and Hui-Chen Betty Liu. Thank you all for your continued support.

David Biber, Mike Duda, Kurt Hess, Sandy Shrum, Barbara White, and Tracey Kelly: Thank you all so much for helping us get this guide out. We cannot thank you enough.

Executive Summary

This seventh edition of the *Common Sense Guide to Managing Insider Risk* (i.e., *Common Sense Guide*) provides our most current recommendations for mitigating ***insider threats*** and managing ***insider risk***. These evidence-based recommendations are based on our empirical research and analysis of 3,000 cases of insider threat.

Insider risk management is a multi-million-dollar problem for many organizations, impacting organizations of all sizes and across all sectors.[1] Although the methods of attack can vary, the primary types of incidents we identified—theft of ***intellectual property (IP)***, sabotage, fraud, espionage, unintentional incidents, and misuse—continue to be the archetypes of insider threat events.

As we share our guidance and best practices for insider threat mitigation and insider risk management, here are a few common definitions that we use throughout this guide:

- **Insider Threat**—The potential for an individual who has or had authorized access to an organization's ***critical assets*** to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization [Costa 2017] (This definition has been updated to include both intentional and unintentional insider threats as well as workplace violence.)
- **Insider Risk**—The impact and likelihood associated with the realization of an insider threat
- ***Insider Risk Management Program (IRMP)***[2]—A designated set of capabilities and resources purposefully allocated to mitigate insider threat and manage insider risk

In our work with public and private sectors, we continue to find that insider threats are influenced by a combination of technical, behavioral, and organizational factors. We recommend that organizations consider implementing policies, procedures, and practices across the organization to mitigate insider threats and manage insider risk.

Our guidance and recommendations are tailored to build and sustain high-impact IRMPs in partnership with key stakeholders across various groups throughout an organization:

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

[1] Sixty percent of organizations surveyed by the Ponemon Institute in 2019 had at least twenty insider threat incidents per year. On average, a ***malicious insider*** can cost an organization $756,760 per incident [Ponemon 2020].

[2] Previously, we referred to ***insider risk management programs (IRMPs)*** as insider threat programs (InTPs). With this edition of the *Common Sense Guide*, we are adjusting the language we use to align with our approach to this topic—insider threat mitigation is an exercise in risk management.

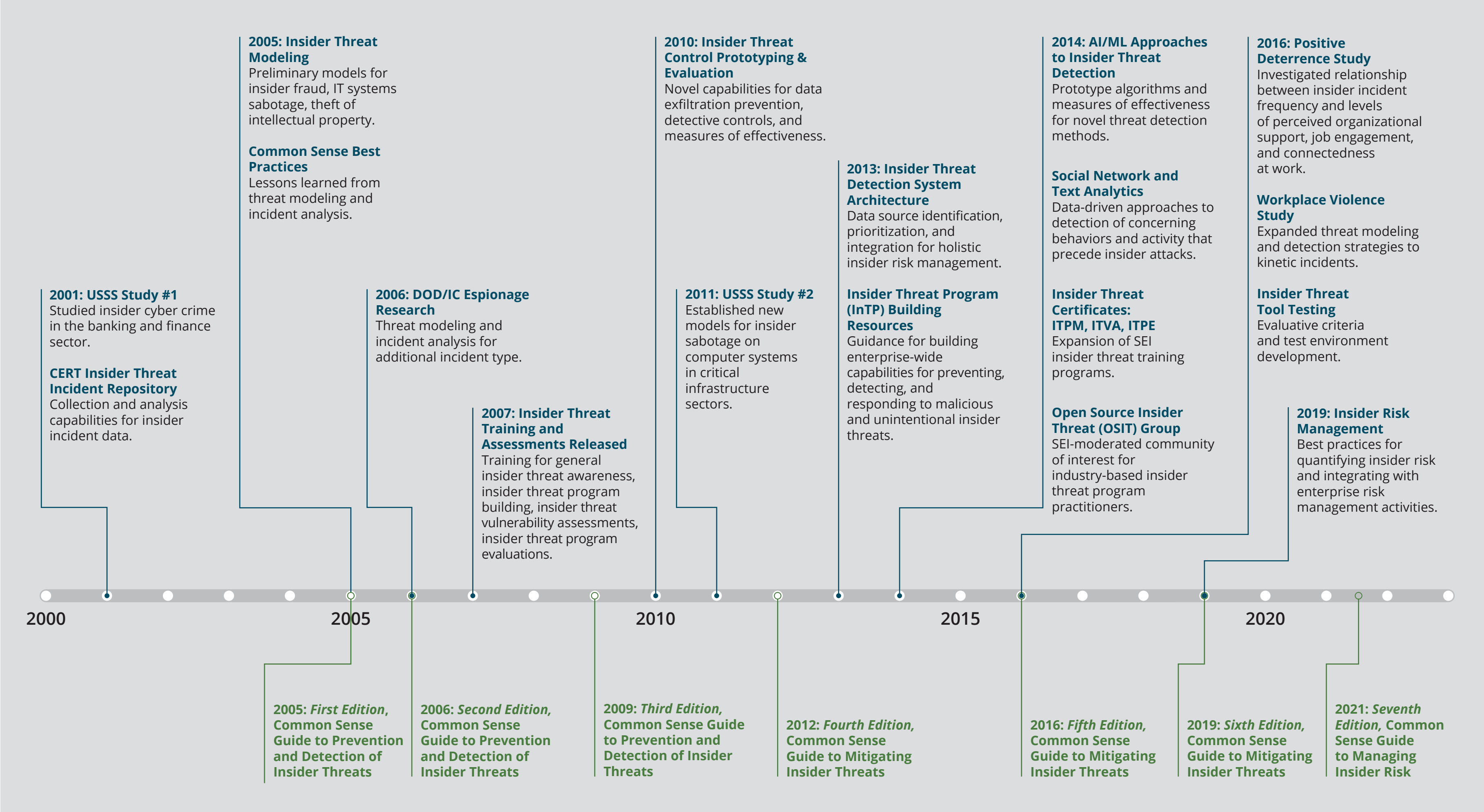
The recommendations in this guide are designed for decision makers and stakeholders to work together to effectively prevent, detect, and respond to insider threats.

This seventh edition of the guide describes 22 actionable best practices that organizations can leverage to manage insider risk. Each best practice includes strategies and tactics for quick wins and high-impact solutions, mitigations to minimize implementation challenges and roadblocks, and mappings to notable and relevant security and privacy standards.

Each best practice also provides resources for relevant stakeholders. The appendices include a glossary of relevant terms and a list of acronyms.

The History of the *Common Sense Guide*

This update to the *Common Sense Guide* contains and updated introduction, our latest statistics, updated mappings, and a new best practice, **Best Practice 22, Learn From Past Insider Incidents**.



2001: USSS Study #1
Studied insider cyber crime in the banking and finance sector.

CERT Insider Threat Incident Repository
Collection and analysis capabilities for insider incident data.

2005: Insider Threat Modeling
Preliminary models for insider fraud, IT systems sabotage, theft of intellectual property.

Common Sense Best Practices
Lessons learned from threat modeling and incident analysis.

2006: DOD/IC Espionage Research
Threat modeling and incident analysis for additional incident type.

2007: Insider Threat Training and Assessments Released
Training for general insider threat awareness, insider threat program building, insider threat vulnerability assessments, insider threat program evaluations.

2010: Insider Threat Control Prototyping & Evaluation
Novel capabilities for data exfiltration prevention, detective controls, and measures of effectiveness.

2011: USSS Study #2
Established new models for insider sabotage on computer systems in critical infrastructure sectors.

2013: Insider Threat Detection System Architecture
Data source identification, prioritization, and integration for holistic insider risk management.

Insider Threat Program (InTP) Building Resources
Guidance for building enterprise-wide capabilities for preventing, detecting, and responding to malicious and unintentional insider threats.

2014: AI/ML Approaches to Insider Threat Detection
Prototype algorithms and measures of effectiveness for novel threat detection methods.

Social Network and Text Analytics
Data-driven approaches to detection of concerning behaviors and activity that precede insider attacks.

Insider Threat Certificates: ITPM, ITVA, ITPE
Expansion of SEI insider threat training programs.

Open Source Insider Threat (OSIT) Group
SEI-moderated community of interest for industry-based insider threat program practitioners.

2016: Positive Deterrence Study
Investigated relationship between insider incident frequency and levels of perceived organizational support, job engagement, and connectedness at work.

Workplace Violence Study
Expanded threat modeling and detection strategies to kinetic incidents.

Insider Threat Tool Testing
Evaluative criteria and test environment development.

2019: Insider Risk Management
Best practices for quantifying insider risk and integrating with enterprise risk management activities.

2005: *First Edition*, Common Sense Guide to Prevention and Detection of Insider Threats

2006: *Second Edition*, Common Sense Guide to Prevention and Detection of Insider Threats

2009: *Third Edition*, Common Sense Guide to Prevention and Detection of Insider Threats

2012: *Fourth Edition*, Common Sense Guide to Mitigating Insider Threats

2016: *Fifth Edition*, Common Sense Guide to Mitigating Insider Threats

2019: *Sixth Edition*, Common Sense Guide to Mitigating Insider Threats

2021: *Seventh Edition*, Common Sense Guide to Managing Insider Risk

Figure 1: Historical Timeline of the Common Sense Guide

INTRODUCTION

Introduction

What Are Insider Threat and Insider Risk?

As the field of insider threat mitigation and insider risk management has matured, so has the terminology. Our definitions of ***insider threat***[3] and ***insider risk*** extend terminology found in the *CERT Resilience Management Model* (*CERT-RMM*) [Caralli 2016]:

- **Insider Threat**—The potential for an individual who has or had authorized access to an organization's critical assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization
- **Insider Risk**—The impact and likelihood associated with the realization of an insider threat

With this perspective, an ***insider threat actor*** (or simply, an ***insider***) is an individual who has or had authorized access to an organization's ***critical assets***.[4] The distinct patterns of how an insider threat actor can negatively affect the organization are referred to as ***insider threat scenarios***.[5] Each insider threat scenario has impact potential (typically measured in dollars as direct and indirect loss, or as a qualitative low to high anticipated magnitude)[6] and likelihood potential (typically measured as a probability or percentage, or as a qualitative low to high anticipated probability of occurrence).[7]

The primary insider threat scenarios derived from our incident repository include the following:

- Intellectual Property (IP) Theft
- Information Technology (IT) Sabotage
- Fraud
- Misuse of Authorized Access
- Unintentional Incidents
- National Security Espionage
- Workplace Violence

Each insider threat scenario is distinguished by a unique fact pattern or set of circumstances. Organizations should consider their operational context and critical assets for additional or derivative insider threat scenarios.

As an organization identifies applicable insider threat scenarios, the associated impact and likelihood of each scenario contributes to describing the relative risk. Using the impact and likelihood metrics, the organization's enterprise risk management (ERM) effort can catalog and prioritize these risks in a risk register, enabling more informed decisions on how to address each risk relative to the organization's risk appetite and resources.

[3] In the guide's Introduction and in each best practice, we highlight the first instance of each glossary term in ***bold italic***.

[4] ***Assets*** include people, information, technology, and facilities. See CERT-RMM, Asset Definition and Management (ADM) [Caralli 2016].

[5] ***Threat scenarios*** or ***threat*** events were formerly referred to as *case types*.

[6] ***Threat scenario impact*** measures direct and indirect costs associated with recovering from the potential loss and returning to the pre-incident posture.

[7] *Threat scenario likelihood* or *probability* measures the anticipated likelihood of the threat scenario occurring.

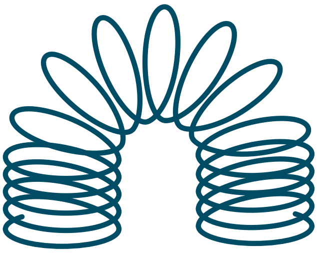
From Mitigating Insider Threats to Managing Insider Risk

The central theme of the seventh edition of the Common Sense Guide is approaching the problem of insider threat as a function of risk management. With this new approach, organizations prepare to accept risk by proactively addressing the underlying resource allocation problem:

> *There will never be enough funds to prevent all incidents or mitigate all vulnerabilities.*

Instead, decision makers must make the right strategic investments in the right defensive security portfolio to match their allowable risk appetite.

This approach *does* mitigate insider threats while embracing practical (i.e., financial, technological) constraints. Risk management also focuses priorities. If you know you have to accept some loss, what ***assets*** must you protect?[8] The answer to this question leads us to the premier priority for many executives—maintaining ***operational resilience*** in the face of an emergency.



Operational Resilience—The *ability* of an organization to continue to carry out its mission in the presence of operational *stress* and *disruption*

In the event of an insider event (intentional or unintentional, malicious or accidental), an organization must be able to rapidly pivot to the right incident containment and response plan to minimize disruption and maintain baseline operations.

Tying together efforts to prevent, detect, and respond to insider threat incidents and efforts to proactively manage insider risk is the responsibility of an ***insider risk management program (IRMP)***.

An IRMP is a designated set of capabilities and resources purposefully allocated to mitigate insider threat and manage insider risk.[9] The strategies and tactics that IRMPs can deploy and lead are described throughout the *Common Sense Guide*.

Research on Insider Incidents

The ***threat*** of attack from insiders is real and substantial. Our research as well as research from the Ponemon Institute, Verizon, and Deloitte, consistently reveals that insider threats are a growing problem [Ponemon 2020, Verizon 2021, Deloitte 2021].

In the *2017 U.S. State of Cybercrime Survey*—conducted by Carnegie Mellon University's (CMU's) Software Engineering Institute (SEI), United States (U.S.) Secret Service, *CSO Magazine*, and sponsored by Forcepoint—found that 20% of electronic crime events were suspected or known to be caused by insiders. The survey also revealed that 30% 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 (in descending order): sensitive information was exposed, confidential records (e.g., trade secrets or IP) were compromised, customer records were compromised, and employee records were compromised [CSO Magazine 2017].

Since 2001, we have conducted a variety of research engagements, training, and assessments on the topic of insider threat. Our work revealed that insider attacks occur across organizations of all sizes and in all sectors, and these incidents can cause significant damage. 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
- workplace violence incidents that lead to loss of life and injuries

[8] For resources describing critical asset identification, see OCTAVE Forte [Tucker 2020].

[9] The formalization of an IRMP is described in **Best Practice 2**.

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

The foundation of our work is the incident repository we maintain—a collection of over 3,000 cases of insider incidents in which the perpetrator was charged and convicted or found liable of a criminal or civil action. These cases document publicly disclosed insider threat incidents, revealing fact patterns of insider acts that demonstrate some malfeasance, misfeasance, and nonfeasance[10] standard of action.

We map these failures to discharge obligations to either a malicious or unintentional motivation scale. The rationale for continuing data collection and analysis for twenty years is that this span of collection provides us with a set of data points for known and agreed-on insider attacks, and it allows us to provide evidence-based insights for how insider threat incidents unfold.

Conducting applied research to generate evidence-based insights is a known but difficult problem[11] in cybersecurity because of the lack of dependable data. This problem is amplified for insider threat research because of the personal nature of the data—traits and observables of actors who might (or might not) commit an attack.

Many techniques exist to collect data (e.g., surveys, synthetic generation, anonymized real-world data), but these approaches are typically constrained by sensitivity concerns or a validity criterion. We find incident collection to be one of the most reliable and accessible means of collecting dependable data.

[10] See **https://en.wikipedia.org/wiki/Misfeasance**.

[11] Refer to the Defense Advanced Research Projects Agency (DARPA) Grand Challenge [DARPA 2004].

Our Data

The charts on this page illustrate data captured within the CERT Insider Threat Incident Repository.

Insider Threat Incident Types

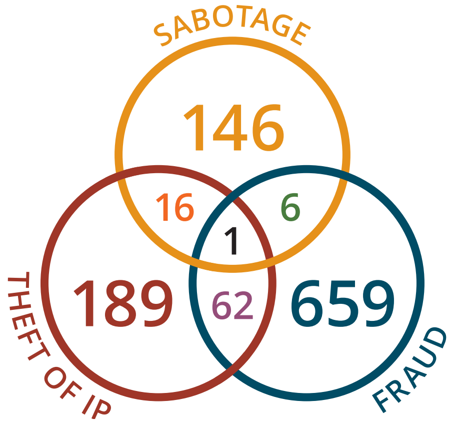


Figure 2: Insider Threat Incident Types (n=1314)

Estimated Financial Impact

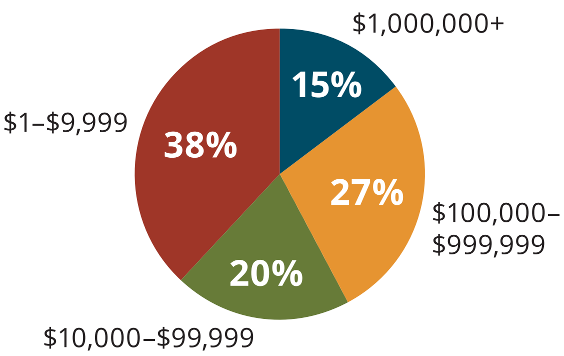


Figure 3: Estimated Financial Impact (n=1179)

Victim Organization Industry Type

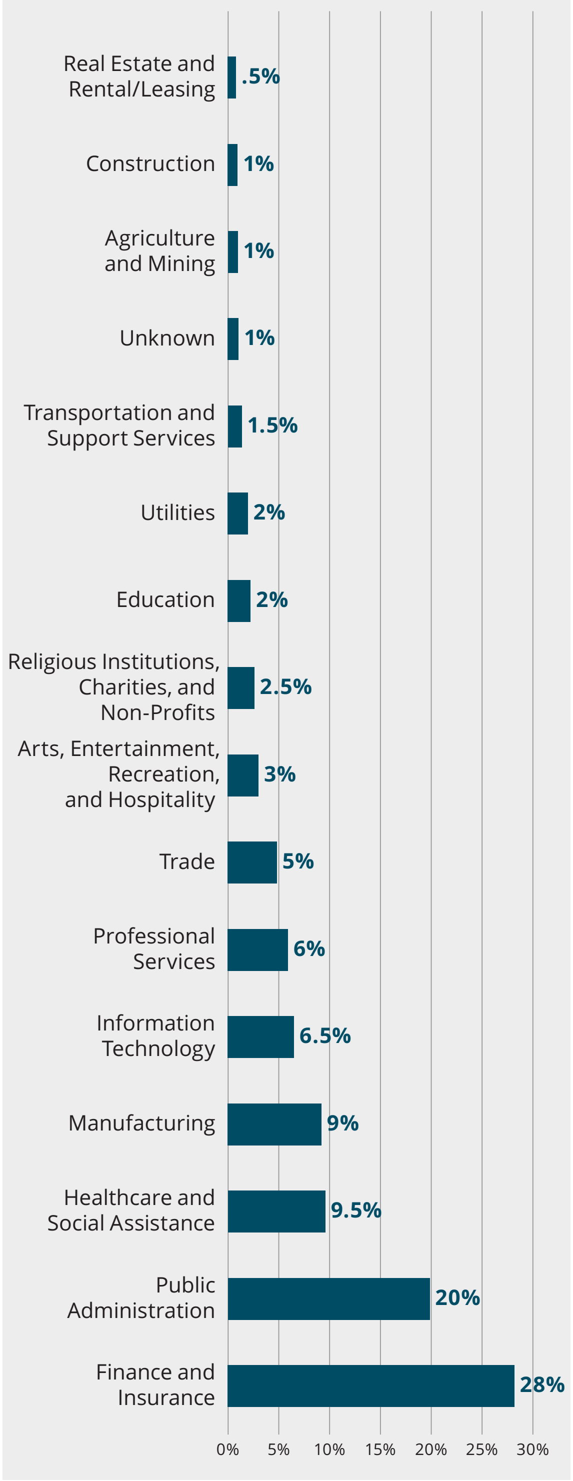


Figure 8: Victim Organization Industry Type (n=1515)

Top Five Stressors

	Incidents
1. Termination	**375**
2. Resignation	**245**
3. Internal Position Change	**55**
4. Organization M&A Activity	**43**
5. Emerging Financial Problems	**33**

Figure 4: Top Five Stressors Across Insider Threat Incidents

Top Five Concerning Behaviors

	Incidents
1. Went to Work for a Competitor	**89**
2. Disgruntled	**57**
3. Suspicious Foreign Travel	**55**
4. Financial Conflict of Interest	**53**
5. Physical Property Theft	**50**

Figure 5: Top Five Concerning Behaviors Across Insider Threat Incidents

Top Five Data Exfiltration Methods Observed

	Incidents
1. Email	**141**
2. Removable Media	**90**
3. Paper	**80**
4. Web	**61**
5. Verbal	**42**

Figure 6: Top Five Data Exfiltration Methods Observed Across Insider Threat Incidents

Top Five Sabotage Methods Observed

	Incidents
1. Critical Data Modified	**135**
2. Critical Data Deleted	**91**
3. Denial of Service Attack—General	**79**
4. Malicious Code Inserted	**42**
5. Social Engineering	**35**

Figure 7: Top Five Sabotage Methods Observed Across Insider Threat Incidents

Finding the Right Balance for Insider Risk Management

Insider risk management requires a multi-pronged approach using capabilities and resources across departments. An organization must *deliberately* implement and operationalize its strategy, and consider organizational values and culture as guideposts to its success. Insider risk management should be an *interactive* process, where strategy and implementation teams collect continuous feedback from stakeholders about the performance of the effort and how the progress aligns with the IRMP's goal of reducing insider risk to *acceptable* levels as described in the organization's risk appetite statements.

There is a litany of stories and articles that describe when insider risk management goes wrong. We are certain that nearly all of these events could have been prevented with the deliberate and interactive approach to insider risk management described in this guide and by setting the right expectation: Insider risk management is a *balancing act*.

As Figure 9 illustrates, insider risk management balances risk across people, management, and organizational dimensions. However, even the most intentional and careful IRMPs generally allow some risk tolerance. The bottom line is that *not all insiders can be stopped*. Organizations must be positioned to sustain critical operations during and recover after an insider threat event.

By staying proactive with an intentionally designed IRMP, an organization can reduce insider risk to the level defined in its risk appetite statement. The IRMP must implement a strategy with the right combination of policies, procedures, and technical controls. Management from all areas of the organization, particularly at the executive level, must appreciate the magnitude and likelihood of insider risk.

Management should align the requirements of the insider risk management strategy with the organization's business policies and processes, culture, and technical environment. Insider threats cannot be 100% prevented; however, organizations can achieve an acceptable level of risk and maintain operational resilience in the event a threat is realized.

As management scientist Peter Drucker said, "Culture eats strategy for breakfast." Therefore, IRMPs must be keenly aware of how their organization's culture helps or hinders their efforts.

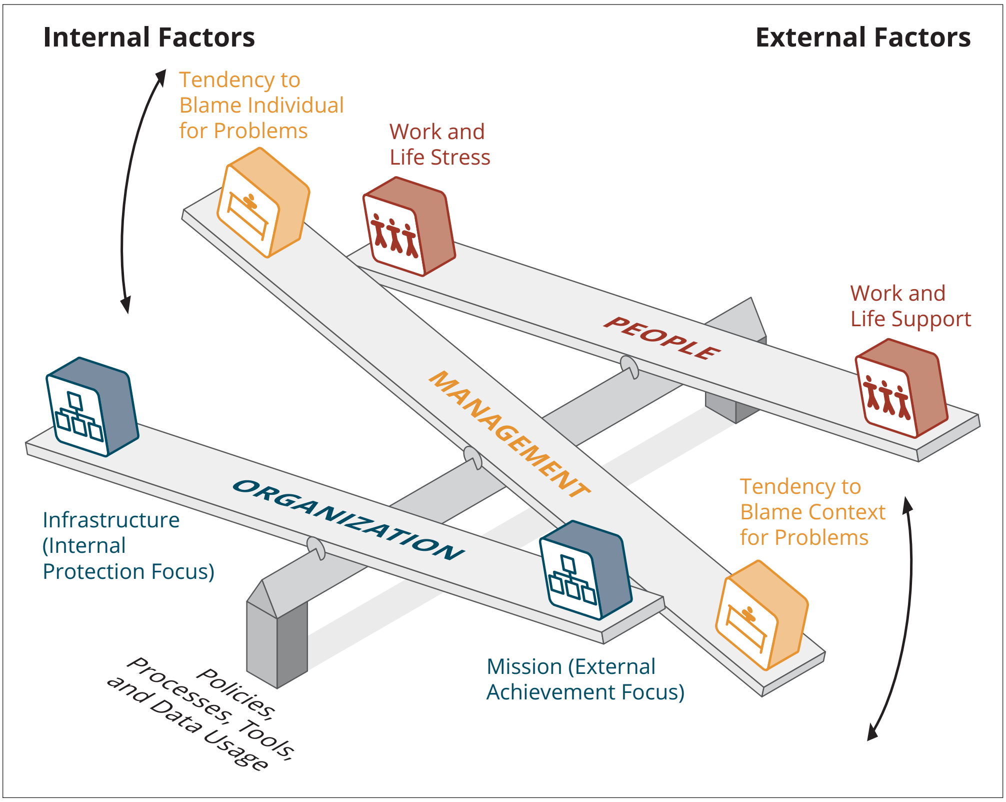

Internal Factors
External Factors
Tendency to Blame Individual for Problems
Work and Life Stress
Work and Life Support
PEOPLE
MANAGEMENT
ORGANIZATION
Tendency to Blame Context for Problems
Infrastructure (Internal Protection Focus)
Mission (External Achievement Focus)
Policies, Processes, Tools, and Data Usage

Figure 9: The Organization's Balancing Act

On Privacy and Civil Liberty Concerns

IRMPs should coordinate with the organization's legal and privacy offices to define privacy and civil liberty requirements for IRMP operations, with a specific focus on activities that use personal data (e.g., employee monitoring, incident detection and response, case management, and pre-hire screening). IRMPs should be aware that privacy rights (and expectations) vary by location and, for organizations servicing or spanning multiple locations such as multinational organizations, there might be a need to design IRMP operations that are scoped to specific jurisdictions to sufficiently manage privacy requirements.

In the U.S., privacy requirements are often conceptualized as a "patchwork." There are many intersecting and related pieces of legislation, agency regulations, and case law at the federal and state levels that shape what are normatively considered ***privacy rights***. IRMPs should work with their organization's general counsel and privacy office to define privacy and related requirements.

IRMPs should seek to answer the following questions:

- What systems collect or use personal data (e.g., a user activity monitoring [UAM] or a user and entity behavioral analytics solution)?
- For each system, what controls are in place to protect personal data? What controls are in place to restrict and control access to personal data? What are the compensating controls?
- What recurring activities concerning privacy requirements should the IRMP prepare for (e.g., audits)?
- What events or activities trigger a privacy requirement or consultation (e.g., a ***data breach***, acquisition of a new system)?
- How are privacy requirements budgeted and overseen?

Privacy Regulation Challenge: General Data Protection Regulation (GDPR)

Outside the U.S., multinational organizations that interact with EU citizens must consider the implications of the European Union's (EU's)[12] General Data Protection Regulation (GDPR)[13] if they have not already. The GDPR is a directive that concerns the processing of personal data by private organizations operating in the EU, whether as employers or as service providers. The GDPR impacts organizations conducting business in the EU (e.g., selling to customers in the EU, employing EU citizens) and is focused on protecting the personal information of EU citizens.

The GDPR went into effect on May 25, 2018 after a two-year window that allowed time for organizations to come into compliance. By extension, an IRMP operating within the EU or accessing data about EU citizens must consider what the GDPR means for its operations.

Meeting the demands of the GDPR within an IRMP might seem untenable, but the goals of the GDPR and IRMP are not as divergent as they can first appear. Ultimately, IRMPs and the GDPR are both concerned with the abuse of sensitive or otherwise privileged information and how it could be misused or abused when it is used for unauthorized purposes or accessed by unauthorized individuals. Privacy cannot exist without security; whereas some security practices might need to be scoped and tailored to better fit the privacy needs of individuals and the regulatory demands of the organization.

Table 1 defines (as they appear in GDPR Article 5) the principles that relate to processing personal data and the potential challenges they can present to IRMPs.

[12] The EU consists of the following member countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

[13] The full text of the regulation is available in English at **https://gdpr-info.eu/**.

Table 1: **GDPR Principles Mapped to IRMPs**

PRINCIPLES RELATING TO PROCESSING PERSONAL DATA	DEFINITION	POTENTIAL CHALLENGES FOR IRMPS
Lawfulness, Fairness, and Transparency	Processed lawfully, fairly and in a transparent manner in relation to the ***data subject***	Lawfulness and fairness of processing is essential to any IRMP. Such a program must exist within the constraints of existing laws and regulations (lawfulness), and analyst bias should not affect processing (fairness).
Purpose Limitation	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes	Data sources originally collected by non-IT functions in an organization can be subject to Purpose Limitation. Refer to **Best Practice 12**, **Table 4** for more information related to socio-technical data sources.
Data Minimization	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	Organizations might seek to maximize the inputs into an IRMP, but they must be mindful of the processing overhead required. The IRMP should collect only as much information as needed.
Accuracy	Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay	None. IRMPs rely on accurate data to perform baselining and for incident response.
Storage Limitation	Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed	None. IRMPs should be expected to demonstrate compliance activities (through documented policy and procedures, etc.) and provide an accurate account of operations related to data retention.
Integrity and Confidentiality	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures	None. Integrity and confidentiality are foundational information security principles.
Accountability	Controller shall be responsible for, and be able to demonstrate compliance	None. IRMPs should be expected to demonstrate compliance activities and provide an account of operations.

Complying with the GDPR does not mean that your organization automatically complies with other similar laws and regulations (e.g., CCPA). In particular, U.S. organizations must stay current on new privacy and civil liberty requirements enacted by the patchwork of various policy-making and regulating bodies.

How to Use This Guide

This guide serves as a resource for stakeholders *building or maturing* IRMPs. Decision makers across the organization benefit from reading it because insider threats are influenced by a combination of technical, behavioral, and organizational issues that must be addressed by policies, procedures, and technologies. An organization's cross-departmental ***workforce members*** who are involved in Management, Human Resources, Legal Counsel, Physical Security, Information Technology, Information Security, Data Owners, and Software Engineers should appreciate the scope and complexity of insider risk management. This guide identifies the organization's groups that have a role in implementing each practice so group members can quickly access relevant recommendations.

Each best practice contains the following elements:

- **Stakeholders Graphic**—This graphic indicates (with a check mark) which stakeholders to involve in the best practice.
- **Challenges**—This section lists known challenges related to the best practice, enabling organizations to quickly spot items to address.
- **Quick Wins and High-Impact Solutions**—This section presents a basic list of quick wins per best practice for jump-starting the organization's IRMP. Some recommendations specifically address 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 workforce members.)
- **Mapping to Standards**—We mapped the best practices to the following external standards or authorities that closely align with the guidance in the *Common Sense Guide*:
  - National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5: *Recommended Security Controls for Federal Information Systems and Organizations* [NIST 2015a]
  - *NIST Cybersecurity Framework (CSF)* [NIST 2018b]
  - *NIST Privacy Framework* [NIST 2021b]
  - *The National Insider Threat Task Force (NITTF) Maturity Framework* [NITTF 2013]
  - *National Minimum Standards* [NITTF 2013]
  - *CERT Resilience Management Model (CERT-RMM)* [Caralli 2016]
  - International Organization for Standardization (ISO) 27002 [ISO 2013b]
  - *CIS v7* [CIS 2021]
  - *European Union General Data Protection Regulation (GDPR)* [GDPR 2021][14]

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

[14] Closely related to the GDPR itself is the *Article 29 Data Protection Working Party Opinion on Data Processing at Work*. The Data Protection Working Party is an independent European advisory body established by Directive 95/46/EC, a predecessor to GDPR. Under Article 94 of GDPR, Directive 95/46/EC was repealed and effectively replaced; ergo, Article 29 Working Party opinions now can be construed as referring to GDPR considerations [GDPR 2021].

BEST PRACTICE 1

BEST PRACTICE 1

Know and Protect Your Critical Assets

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

The most basic function of an ***insider risk management program (IRMP)*** is to protect the ***assets*** that provide the organization with a competitive advantage. According to International Organization for Standardization (ISO) 55000, an asset is something with potential value to an organization and for which the organization has a responsibility [ISO 2014]. In the *Common Sense Guide,* this definition is extended to include that a ***critical asset*** is something of value that—if destroyed, altered, or otherwise degraded—would impact its confidentiality, integrity, or availability and have a severe negative effect on the organization's ability to support its essential missions and business functions.

Critical assets can be tangible and intangible, and, according to the *CERT Resilience Management Model (CERT-RMM)* [Caralli 2016] can include people, information, technology, and facilities, as depicted in Figure 10. An often-overlooked aspect of critical assets is ***intellectual property (IP)***, which can include proprietary software, customer data for vendors, schematics, and internal manufacturing processes.

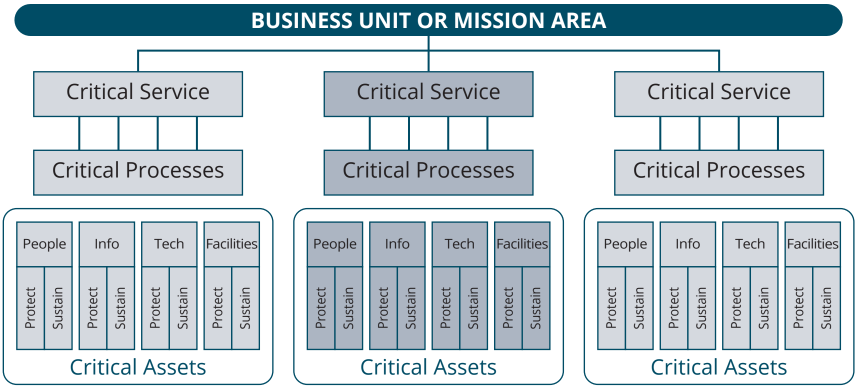


Figure 10: Critical Assets Across Critical Services

The organization must closely watch where data is at rest and in transport. Current technology allows more seamless collaboration than ever, but it also allows the organization's sensitive information to be easily removed from the organization.

When managing risk, it is essential to have an exhaustive inventory of assets. The following questions can help the organization identify requirements for protecting its critical assets:

- For each business unit or mission area,[15] what are the critically supporting services?
- For each critical service, what are the supporting critical processes?
- For each critical process, what are the supporting critical assets?
- For each critical asset, what is its nature (e.g., people, information, technology, or facilities)?
- For each critical asset, who has authorized access? Who does not have authorized access?
- For each authorized user of each critical asset, what kind of access do they have? How frequently is access audited?
- For each critical asset, what is the process for granting access? What is the process for revoking access?
- For each critical asset, what is the present value of its loss or replacement? What are the *direct* and *indirect* costs associated with its loss or replacement?
- For each critical asset, who are the primary stakeholders or stakeholders that must be notified if a loss or incident occurs (e.g., primary points of contact, owners, controllers, customers, emergency contacts)?
- For each critical asset, are there regulatory or otherwise mandatory protection requirements?

The role of the IRMP is to work with asset owners and asset stewards across all areas of the organization to answer these questions. The IRMP should begin by seeking guidance from those who might already maintain a critical asset inventory—generally those responsible for property management or data protection (e.g., a privacy program).

Once the IRMP obtains the answers to these questions within each division, it should obtain input from senior-level management to prioritize protection across the organization. The result is a critical asset inventory that prioritizes assets by criticality.

Once the critical asset inventory is created, the organization can begin identifying potential ***threat scenarios*** related to each critical asset. It should focus on users with current or former authorized access to each asset. The IRMP should determine how each user could use their permission and knowledge to cause damage. This task begins the threat enumeration effort, which is vital for measuring the likelihood and probability of the threat scenario.

Protective Measure: Conducting a Risk Assessment

A risk assessment is one of the best ways for an organization to know its assets and protect them from attack, including from ***insiders***. Results of a risk assessment inform an organization about how a threat actor can misuse their authorized access to organizational assets.

As the assessment team conducts a risk assessment, it profiles how attackers can leverage their access and resources to carry out threat scenarios. Using this process, the team evaluates specific threat scenarios for each critical asset within the scope of the assessment. Assessment findings (1) illuminate the threat impact and likelihood of each scenario and (2) describe how the assets in the environment enable or contribute to the attack's success.

According to the National Institute of Standards and Technology (NIST), the risk management framework includes six steps [NIST 2018a]:

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.*

[15] Lines of business or mission areas are the separate core functions of an organization's principle services.

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 must be answered before an organization can move forward with a protection strategy include the following:

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

Answering these questions helps the organization inventory the data and systems that it must protect from various attacks. NIST Special Publication 800-60 Volume 2 identifies data types that can exist in an organization and the protection levels they should be afforded [NIST 2008].

Federal Information Processing Standards (FIPS) Publication 199 provides guidance about categorizing information and information systems based on their security objectives (e.g., confidentiality, integrity, and availability) and the potential impact of events that jeopardize them (e.g., low, moderate, or high) [FIPS 2004].

Metrics

One of the major difficulties an organization faces is being able to accurately rank and score the different critical assets provided to its decision makers. Often, stakeholders in an organization claim “the asset they know about and control” is, in their opinion, the most critical asset in the organization. Instead of gathering such a subjective and biased ranking of critical assets, it’s better to use metrics and discuss them internally with various ***workforce members***.

Table 2 is not meant to be an exhaustive list of metrics; instead, it provides a sense of the types of metrics that might be considered.

Table 2: **Metrics to Consider in Ranking Critical Assets [Wikoff 2004]**

METRIC	EXPLANATION
Time to restore	How long (e.g., months, weeks, hours) will it take to restore the critical asset if it becomes unavailable?
Loss if it fails	What is the loss (e.g., monetary or perhaps even loss of life) if the critical asset fails?
Mission and customer impact	What is the impact to the organization’s mission and its customer base if the critical asset is unavailable or otherwise is 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, the organization should leverage a statistical approach known as *Pairwise Ranking*.[16] This approach essentially allows a group to rank assets 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.

[16] For more information on ranking critical assets, visit **http://www.thesecurityminute.com/ranking-critical-assets**.

Protective Measure: Maintaining an Asset Inventory

For an organization to better position itself to defend its critical assets, it must know what its critical assets are. A reliable method of identifying and tracking the organization's critical assets is essential to tying ***insider threat*** mitigation efforts to the organization's needs.

This list of critical assets should be regularly updated since it serves as a guide and provides a focus for the organization's IRMP. Continuously updating the organization's list of critical assets can require both manual and automatic processes. The primary method for creating an exhaustive inventory is a ***service-based inventory*** approach. Another method is to create a hardware-based inventory. This inventory can supplement a service-based inventory or serve as a start to a service-based asset inventory.

To perform a service-based inventory, the organization must have a service catalog rather than a conventional inventory. A *service catalog* contains information about the services an organization needs to fulfill its mission. For example, an online store might define its web page as a critical service, and a communications company might identify its 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. These supporting assets, 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.

To perform a *hardware-based inventory*, the organization relies on hardware-based assets typically managed by information technology (IT) departments to start the asset inventory. Typically, the organization has some level of hardware tracking to manage the lifecycle and protection of various pieces of IT equipment issued to workforce members.

For a hardware-based inventory, data stewards should provide the following information:

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

Remember that the hardware-based inventory approach does not produce an exhaustive list of critical assets. The organization should use a hardware inventory to kick off a critical asset inventory only if a critical asset inventory does not exist.

Once the organization identifies its information assets using one of these methods, it should do the following:

- Ask the IT department to add any unidentified assets and their business owners' contact information.
- Ask those business owners to identify the following: those who have authorized access, how access can be granted and revoked, the name of the emergency contact, the loss or replace value of the asset, and whether there are any regulatory requirements to secure the asset.
- Condense all the inventory information into a spreadsheet.

Once the inventory is complete, the organization should assign a set of attributes to each asset, which helps determine each asset's priority.

The organization can define any attributes it needs, but it should consider at least the following:

- environment (e.g., production, integration, model, development)
- security categorization (e.g., confidentiality, integrity, availability[17])
- criticality (e.g., high, medium, low, not applicable)

Protective Measure: Conducting a Privacy Impact Assessment (PIA)

The General Data Protection Regulation (GDPR) stipulates that special categories of personal data must include data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" and that processing of such data is generally prohibited.[18]

The organization should account for the possibility that such personal data can be discovered during a risk assessment or asset tracking process. It should have defined processes for handling or destroying that data as appropriate. Therefore, the organization might want to consider conducting ***Privacy Impact Assessments (PIAs)*** (referred to as ***Data Protection Impact Assessments (DPIAs)*** in the European Union [EU]) in conjunction with a risk assessment or asset inventory.

According to EU GDPR Article 35 [GDPR 2021], a PIA must include the following, at a minimum:

1. *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
2. *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
3. *an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
4. *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

In an employer/employee relationship, a PIA or DPIA is conducted by the employer in the role of controller (i.e., the entity that "determines the purposes and means of the processing of personal data") [GDPR 2021]. According to the GDPR, *personal data* is "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier" [GDPR 2021].

While United States (U.S.) organizations might be most concerned and familiar with Social Security numbers (SSNs) as personal data, this definition could be expanded to include dynamic Internet protocol (IP) addresses in certain circumstances[19] since they relate to citizens of the EU. If a dynamic IP address can be combined with other information held by a third party, such as an Internet service provider (ISP), to identify an individual, that constitutes personal information and must be afforded appropriate considerations and safeguards.

According to the GDPR, a ***data subject*** is "a living individual to whom personal data relates." In this instance, a data subject could be a customer or employee [GDPR 2021].

[17] FIPS PUB 199 provides attribute values for criticality, integrity, and availability [FIPS 2004].

[18] Although exceptions exist under Article 9 for processing such special categories of data, none explicitly give employers reasonable legal grounds for processing such data about an employee.

[19] See the 2016 court decision made in Germany related to Directive 95/46/EC Article 2(a) and Article 7(f) on the definition of personal data: **http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945**.

Challenges to Asset Identification

The organization can face the following challenges when implementing this best practice:

1. **Getting leadership buy-in**. To spend the time, money, and energy required to accurately understand and prioritize the organization's critical assets, it is necessary to receive the appropriate buy-in from leadership.
2. **Determining appropriate metrics**. The organization should determine what a critical asset is by identifying and using appropriate metrics. Simply asking the organization's stakeholders to report on their critical assets will likely lead to over-reporting.
3. **Defining the scope of critical assets**. The organization must understand and contain the scope of its critical assets, especially when using the cloud, remote sites, and virtual systems.
4. **Securing time and funding**. Conducting an inventory or cataloging assets costs workforce time and organizational funding, so finding time and funding to do a complete inventory is critical. To justify the necessary funding and worker hours, consider the importance of this work as well as the risks, financial and otherwise, of not completing the work.
5. **Maintaining an inventory**. An accurate and up-to-date inventory is vital to ensure that lists continue to be correct. The organization should conduct periodic inventory checks, such as complete semiannual or annual reviews, and more frequent (e.g., monthly or quarterly) spot-check audits.

CASE STUDY: A COOL HACK

A hospital facility contracted the insider as a security guard. She was extensively involved in the Internet underground and was the leader of a hacking group. She worked for the victim organization only at night and was unsupervised. The majority of her unauthorized activities involved a heating, ventilation, and air conditioning (HVAC) computer. This HVAC computer was located in a locked room, but the insider used her security key to obtain physical access to it.

The insider remotely accessed the HVAC computer five times over a two-day period. In addition, she accessed a nurses' station computer, which was connected to all of the victim organization's computers, stored medical records, and patient billing information. She used various methods to attack the organization, including password-cracking programs and a botnet. Her 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. She was convicted, ordered to pay $31,000 in 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 extensive 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 modified and impaired patient records, which could affect treatment, diagnoses, and care. It is critical that management and information security teams work with other departments to identify critical systems. In this case, the HVAC computer was located in a locked room, not in a data center or server room that would have afforded the system additional protections and might 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.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Identify critical business services, supporting processes, and supporting assets.

☑ Describe the nature of the information your organization processes by speaking with data owners and users from across the organization.

☑ Identify legal and regulatory requirements for protecting critical assets.

☑ Identify emergency points of contact for all critical assets.

☑ Calculate a present value for the loss or replacement of each asset.

☑ Track who has what kind of access for each asset.

☑ Maintain guidance for granting and revoking access for each critical asset.

☑ Identify the types of monitoring capabilities that allow each critical asset to be controlled and audited.

☑ Prioritize assets and data to determine high-value targets.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	CM-2 Baseline Configuration CM-8 Information System Component Inventory PM-5 Information System Inventory PM-8 Critical Infrastructure Plan RA-2 Security Categorization
NIST Cybersecurity Framework	ID AM ID RA ID RM PR DS PR MA
NIST Privacy Framework	ID.IM-P ID.BE-P ID.DE-P CT.DM-P CT.DP-P
NITTF Maturity Framework	ME-4
National Minimum Standards	B-2 G-1
CERT-RMM	Asset Definition and Management Enterprise Focus
ISO 27002	7.1.1 Inventory of Assets
CIS v7	Control 1 Control 2
GDPR	Article 9 Processing of special categories of personal data Article 32 Security of processing Article 35 Data protection impact assessment

BEST PRACTICE 2

BEST PRACTICE 2

Develop a Formalized Insider Risk Management Program

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

At its essence, a formalized ***insider risk management program (IRMP)*** uses a risk management thought process. An IRMP is the organization's designated and dedicated resource for mitigating ***insider threats*** and managing ***insider risk***. The trust that the organization has for its ***workforce*** and its ***trusted external entities (TEEs)*** can leave it vulnerable to ***malicious insiders*** who often use methods to hide their illicit activities.

To effectively prevent, detect, and respond to the unique ***threats*** from ***insiders***, the organization must take appropriate risk management action. The best time to develop a process for mitigating insider incidents is *before* they occur. When an incident does occur, the process can be updated based on the results.

Protective Measures

Organizations, including the federal government, are increasingly recognizing the need to counter insider threats using specially focused teams. In January 2011, the United States (U.S.) 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]. This memorandum announced the results of evaluating the insider threat safeguards of government agencies. This action by the federal government highlights the pervasive and continuous threat that insiders pose to government and private industry and the need for programs that mitigate this threat.

In October 2011, President Obama signed *Executive Order (EO) 13587—Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* [Obama 2011]. This EO requires all federal agencies that have access to classified information and systems to have a formal IRMP. In addition, *National Industrial Security Program Operating Manual (NISPOM) Change 2* [NISPOM 2006] requires defense contractors to establish and maintain an IRMP with many of the requirements of EO 13587.

An IRMP is an organization-wide program with an established vision and defined roles and responsibilities for its participants. All participants must receive specialized role-based training. The program must establish criteria and thresholds for identifying insider risk, conducting inquiries, referring to investigators, and recommending mitigations.

A well-rounded and properly implemented IRMP must also consider ***workforce member*** privacy. It must maintain a culture that balances achieving the organization's mission with the ability to support the organization's workforce. The goal of most IRMPs should be to keep trusted workforce members on the path of appropriate workplace behaviors rather than simply detecting and mitigating policy violations.

The organization must determine how much it should trust its workforce members while respecting their privacy and civil liberties. Workforce members must clearly understand what they can perform at work and what they can expect to remain private while at work. The IRMP must control inquiries with a process that ensures privacy and confidentiality because IRMP members are trusted to conduct monitoring and resolution. These privacy considerations and a culture of privacy by default can also guard against unintentional personal ***data breaches***. Most importantly, the IRMP must have management's support to be successful.

Researchers at Carnegie Mellon University's (CMU's) Software Engineering Institute (SEI), along with other organizations such as the Intelligence National Security Alliance (INSA), documented the most common IRMP components found in government and non-government organizations [INSA 2013]. This best practice recommends that an IRMP include, at a minimum, the components illustrated in Figure 11.

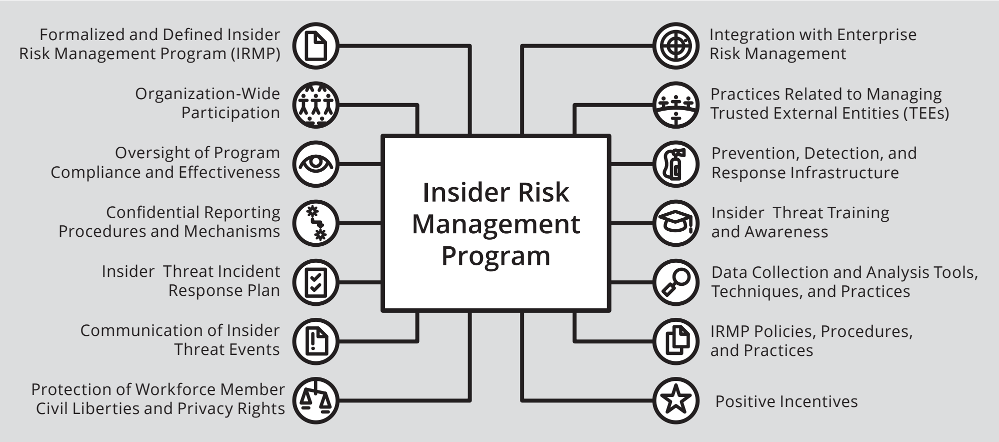

Formalized and Defined Insider Risk Management Program (IRMP)
Organization-Wide Participation
Oversight of Program Compliance and Effectiveness
Confidential Reporting Procedures and Mechanisms
Insider Threat Incident Response Plan
Communication of Insider Threat Events
Protection of Workforce Member Civil Liberties and Privacy Rights
Insider Risk Management Program
Integration with Enterprise Risk Management
Practices Related to Managing Trusted External Entities (TEEs)
Prevention, Detection, and Response Infrastructure
Insider Threat Training and Awareness
Data Collection and Analysis Tools, Techniques, and Practices
IRMP Policies, Procedures, and Practices
Positive Incentives

Figure 11: Components Common to IRMPs

The components that an IRMP should, at a minimum, contain are further explained in the following list:

- **Formalized and Defined IRMP**—The program should include elements such as directives, authorities, a mission statement, leadership intent, governance, and a budget.
- **Organization-Wide Participation**—The program should have active participation from all organizational components that use data access and sharing. Senior leadership should provide visible support for the program, especially when the data the IRMP needs is in siloes (i.e., data lives exclusively in areas or departments such as Human Resources [HR], Physical Security, Information Technology [IT], or Information Security).
- **Oversight of Program Compliance and Effectiveness**—A governance structure, such as an IRMP working group or ***change control*** board, should help the IRMP program manager formulate standards and operating procedures for the IRMP and recommend changes to existing practices and procedures. Also, an executive council or steering committee should approve changes recommended by the working group/change control board. Oversight includes annual self-assessments and external entity assessments that evaluate the compliance and effectiveness of the IRMP.
- **Confidential Reporting Procedures and Mechanisms**—Not only do these mechanisms and procedures enable the reporting of suspicious activity, but when closely coordinated with the IRMP, they also ensure that legitimate whistleblowers are not inhibited or inappropriately monitored.
- **Insider Threat Incident Response Plan**—This plan must be more than just a referral process to outside investigators. It should detail how alerts and anomalies are identified, managed, and escalated, including timelines for every action and formal disposition procedures.

- **Communication of Insider Threat Events**—Event information should be appropriately shared with the correct organizational components, while maintaining workforce member confidentiality and privacy until allegations are fully substantiated. This type of communication includes insider risk trends, patterns, and probable future events so that policies, procedures, training, etc., can be modified as appropriate.
- **Protection of Workforce Member Civil Liberties and Privacy Rights**—Legal Counsel should review the IRMP's decisions and actions at all stages of program development, implementation, and operation.
- **Integration with Enterprise Risk Management**—The IRMP must ensure that all aspects of the organization's risk management include insider threat considerations (not just outside attackers), and the organization should consider establishing a standalone component for insider risk management.
- **Practices Related to Managing Trusted External Entities (TEEs)**—These practices include agreements, contracts, and processes reviewed for insider threat prevention, detection, and response capabilities. (The *Common Sense Guide* uses the term *trusted external entities*, not *trusted business partners*.)
- **Prevention, Detection, and Response Infrastructure**—This infrastructure includes components such as network defenses, host defenses, physical defenses, tools, and processes.
- **Insider Threat Training and Awareness**—This training encompasses three aspects of the organization: (1) insider threat awareness training for the organization's entire workforce (e.g., employees, contractors, consultants), (2) training for IRMP personnel, and (3) role-based training for mission specialists who are likely to observe certain aspects of insider threat events (e.g., HR, Information Security, Counterintelligence, Management, Finance).
- **Data Collection and Analysis Tools, Techniques, and Practices**—These tools, techniques, and practices include user activity monitoring (UAM), data collection, and analysis portions of the program. Detailed documentation is required for all aspects of data collection, processing, storage, and sharing to ensure compliance with workforce member privacy and civil liberties.
- **IRMP Policies, Procedures, and Practices**—The IRMP must have formal documents that detail all aspects of the program, including its mission, scope of threats, directives, instructions, and standard operating procedures.
- **Positive Incentives**—Organizations should entice workforce behavior rather than coerce it by leveraging positive-incentive-based organizational practices centered on increasing job engagement, perceived organizational support, and connectedness at work.

An effective IRMP has cross-functional stakeholders who include members of Management, HR, Legal Counsel, Physical Security,[20] IT, Information Security, Data Owners, and Software Engineering. The organization must have (1) an established incident response plan that addresses insider incidents, (2) a documented escalation chain, and (3) precise definitions of which authorities decide the disposition of incidents.

The organization should implement the following when establishing an IRMP:

- identifying ***critical assets***, including intellectual property (IP) and sensitive or classified data (See **Best Practice 1**.)
- using access control to protect identified data and ***assets*** (See **Best Practices 10** and **19**.)
- monitoring access to critical data and assets (See **Best Practices 12**, **17**, and **19**.)
- monitoring workforce members who have privileged access (See **Best Practice 11**.)
- conducting specialized monitoring (e.g., 30-day rule, outside normal hours, to external sites) (See **Best Practices 4** and **17**.)
- implementing separation of duties (See **Best Practice 14**.)
- conducting quality assurance and continuous improvement (See **Best Practice 17**.)

Documents that specify these best practices should require the organization to use technical mechanisms that ensure proper monitoring, alerting, and reporting.

[20] In this best practice, *physical security* and *personnel security* are referred to as *security*. These two teams can be separate entities in an organization, but they often share the same chain of command.

IRMPs help the organization detect, prevent, and respond to an insider incident. A formalized IRMP includes 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 their roles before an insider incident occurs.

To be prepared to handle insider incidents in a consistent, timely, and professional manner, an IRMP's members must understand the following:

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

An IRMP is similar to a standard incident response team because both teams handle incidents; however, an IRMP responds to incidents that are suspected to involve workforce members. The information the IRMP handles is usually sensitive, requiring team members to treat cases with the utmost discretion and due diligence, particularly because the team members and the suspected insiders work for the same organization, and disclosure could wrongfully harm someone's career. Ensuring privacy and confidentiality helps protect (1) accused insiders who are innocent and (2) the integrity of the inquiry process itself.

Members of teams from across the organization must work together to share information and mitigate threats. Table 3 lists teams and personnel the organization should consider involving; these teams and personnel can provide their perspectives on potential threats as part of the prevention, detection, and response aspects of an IRMP.

Table 3: **Titles for IRMP Positions in Government and Non-Government Organizations**

BUSINESS COMPONENTS	SUBJECT MATTER EXPERTS (SMES)
C-Level Managers	Data Architect (or functionality)
Security (Physical, Personnel, and Information)	System Network Architect
Cybersecurity (if not included in Security)	Information Assurance (IA) Specialists
HR or Human Capital (HC)	Senior Technologist
Information Technology (CIO, Chief Technology Officer [CTO])	HR/HC Specialists
Legal	Financial Specialists
Privacy	Legal Specialists Data Protection Officer (DPO) General Data Protection Regulation (GDPR) 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, TEEs as appropriate)	Records Management Specialists

Each of these teams plays a key role in the IRMP because each has access to information or a perspective that others in the organization typically do not share. For example, HR has sensitive information regarding a workforce member's performance that the IRMP might need to effectively detect ***malicious insider*** activity.

As the IRMP team grows, the value of adding members must be balanced with the increased risk of disclosing personal information or disclosing that an inquiry is being conducted. One way to balance information sharing and privacy is to ask all the involved organizational groups to contribute their threat detection data and ideas, but have only a small, core IRMP team receive and analyze that information.

A significant consideration for any organization is how it should align its IRMP within the organization. CERT researchers have seen that government and non-government organizations use different alignment models. Some include having the IRMP report to the following:

- Chief Risk Officer (CRO)
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Human Resources (HR)
- Security (usually Physical Security)
- Chief Financial Officer (CFO)
- Director of Administration or Chief Operating Officer (COO)
- Chief Legal Counsel
- Ethics (or an investigations unit)

Based on empirical observations from the various reporting models, the IRMP encounters the fewest complications and is most effective when it is directly aligned with the leader of the organization. Directly reporting to the President/CEO/Director/Secretary or their Principal Deputy, such as the Chief of Staff/COO, ensures the workforce understands the following:

- the commitment of senior leadership
- the full cooperation of the rest of the C-level staff and their organizations
- the IRMP's unfettered access to needed data sources and subject matter expertise within the organization

Many organizations that originally aligned their IRMP within intelligence, counterintelligence, investigations, or law enforcement discovered significant complications with regulatory compliance requirements that hindered the effectiveness of the program. Similarly, IRMPs 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 managing people. While a program aligned with IT was predominately focused on IT tools and data. To alleviate these types of issues, some organizations eventually realigned their programs to the senior executive or principal deputy.

Figure 12 shows the notional alignment of the IRMP and its governance structure; it also illustrates the need for each team in the organization to provide input to the IRMP. These inputs can be the result of a data call, or they can be a real-time, automated data feed. For example, the HR management system might provide the IRMP with an automated list of workforce members who are leaving the organization. This information can then be used to determine if additional procedures should be implemented.

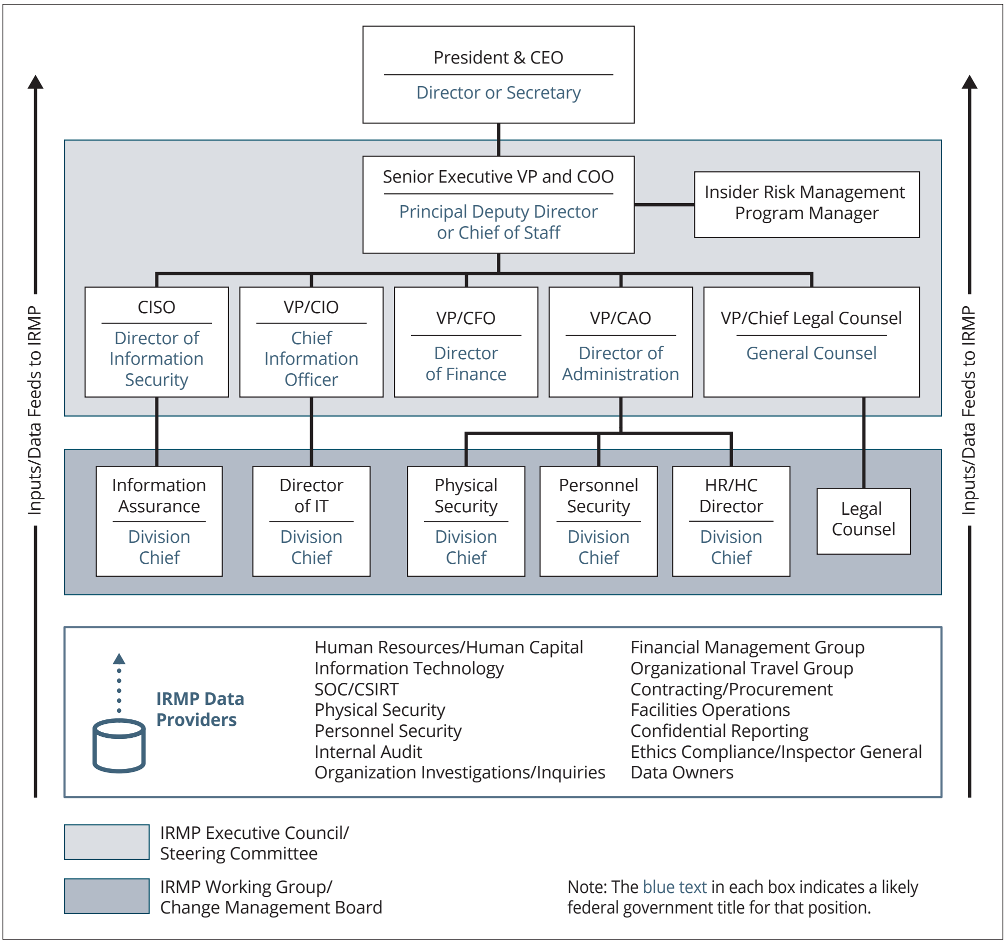

President & CEO
Director or Secretary
Senior Executive VP and COO
Principal Deputy Director or Chief of Staff
Insider Risk Management Program Manager
CISO
Director of Information Security
VP/CIO
Chief Information Officer
VP/CFO
Director of Finance
VP/CAO
Director of Administration
VP/Chief Legal Counsel
General Counsel
Information Assurance
Division Chief
Director of IT
Division Chief
Physical Security
Division Chief
Personnel Security
Division Chief
HR/HC Director
Division Chief
Legal Counsel
IRMP Data Providers
Human Resources/Human Capital
Information Technology
SOC/CSIRT
Physical Security
Personnel Security
Internal Audit
Organization Investigations/Inquiries
Financial Management Group
Organizational Travel Group
Contracting/Procurement
Facilities Operations
Confidential Reporting
Ethics Compliance/Inspector General
Data Owners
Inputs/Data Feeds to IRMP
Inputs/Data Feeds to IRMP
IRMP Executive Council/ Steering Committee
IRMP Working Group/ Change Management Board
Note: The blue text in each box indicates a likely federal government title for that position.

Figure 12: Example IRMP Organizational Structure and Data Providers

Each business unit should have a trusted agent who can provide data feeds or additional information. The IRMP should identify trusted agents early so they can be contacted immediately when data is needed or an incident occurs. Before they are placed in this role, each trusted agent should, at a minimum, submit to a current background check and sign an IRMP nondisclosure agreement (NDA). The IRMP might find that other departments are more willing to cooperate if it requests data only and performs its own analysis. For example, the IRMP should request facility access logs from the Physical Security team and then conduct its own analysis.

The potential IRMP team members listed in Figure 12 can be helpful for prevention, detection, and/or response efforts. However, not every team member needs to be alerted for every potential threat. Instead, the organization should consider which team members must be involved for each type of effort and, during a response, which members should be involved at different levels of response or escalation.

The team should meet regularly to ensure it remains active and effective. Its members should discuss the anomalies detected (proactive response) and allegations (reactive response) of potential insider activity. The team might meet in one physical space or use electronic communication (e.g., videoconference meetings or discussions by secure email). This virtual approach could enable team members in separate locations to collaborate quickly, conveniently, and securely.

The IRMP team should follow security and discretion procedures when using email because many workforce members outside the team (e.g., system administrators and administrative assistants) might have access to its email messages 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 Pretty Good Privacy (PGP). These procedures should also specify that email can be decrypted only briefly, 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 can be impossible to use if the communications system is being attacked or the insider can monitor the meeting, so alternate arrangements should be planned and available. Each organization is different and should create its particular IRMP team and plan according to its size, capabilities, and risk tolerance.

During an inquiry, the IRMP must maintain the confidentiality of all related information to ensure privacy and hide the inquiry from the workforce member suspected of wrongdoing.[21] It is important to remember 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 know about it, and it could ruin someone's career. Therefore, it is of the utmost importance to keep inquiries confidential and discuss them only with those who have a legitimate need to know.[22]

When the IRMP team is conducting an inquiry, its members should be careful about how they request 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 in the organization to avoid alerting the suspect or the data owner. The IRMP core team can then pare the logs to its specific needs.

The organization should include random audits of various data sources as part of policies and standard operating procedures. This practice can reveal previously unidentified threats and provide a good non-alerting cover for data requests made during active inquiries. The organization should consult with legal counsel before implementing any type of auditing program.

Another way the IRMP team differs from an incident response team is its proactive role. For example, previous research shows that workforce members 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 2012, Ariani 2013]. While more research is needed, this suggests that practices to improve workforce member engagement (e.g., strength-based management to improve the fit of a workforce member to their job) can be a good foundation for an enterprise that is resistant to insider incidents.

Other research shows the productivity and retention benefits of employee engagement, so these practices can be a win-win situation for the organization and its workforce [Gallup 2013]. The IRMP should proactively deal with workforce member problems, working to prevent and identify potential threats to minimize harm. The adoption of ***positive incentives*** by the organization and ***detective monitoring*** of the workforce by the IRMP are other examples of proactive roles. (See **Best Practice 21**.)

Any IRMP implemented in an organization must be lawful and abide by all rules and regulations that govern the organization, both domestic and abroad. Monitoring activities must be within bounds, as must the location where monitored information is kept and the people who have access to it. The organization must involve legal counsel before implementing any IRMP and during any inquiry. Consulting legal counsel is vital during the information-gathering process to ensure (1) all evidence is maintained according to legal standards and (2) a prompt legal response is issued when necessary. Legal advice is also necessary to assure that IRMP members share information properly (e.g., ensuring the lawful privacy of workforce members regarding mental and physical health). Organizations that operate in the European Union (EU) (or that have IRMPs that collect data on workforce members within the EU) must consult with the appointed DPO.

[21] IRMPs should thoroughly review and obtain approval of the insider threat incident response plan with internal counsel prior to conducting any incident response activity or action. Depending on the nature of the event, counsel can play a large or moderate role in the inquiry and investigative activity. IRMPs should proactively seek legal guidance and approval before proceeding with any action.

[22] In addition to proactively engaging counsel on the insider threat incident response plan, IRMPs must closely engage internal privacy advisors to ensure proper policies and protocols are in place for handling sensitive personal information related to workforce monitoring, investigation, and response.

The HR team is instrumental in detecting signs of possible behavioral issues related to insider risks. To ensure workforce member privacy, HR must carefully screen any information involved in an inquiry and release only the minimum amount of information necessary and on a need-to-know basis. The HR team can include a behavioral science SME who is embedded or works closely with the IRMP. The HR team can use internal findings to develop a watch list of personnel and release it to certain members of the IA and IRMP teams so they know which logs to review.

Behavioral and technical indicators identified by CERT researchers and other insider threat researchers might be used as potential indicators as part of the organization's IRMP. Examples of workforce behaviors that can signal a potential malicious insider include, but are not limited to, the following:

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

CERT researchers also worked on analyzing various paths that an insider might use to eventually commit theft or an attack. While HR can flag certain behavioral indicators, it also has a responsibility to others in the organization. When a workforce member submits their resignation or leaves the organization by other means, HR must notify members of the IT team so they can perform ***enhanced monitoring*** on the exiting individual.

The following examples show a few of the many pathways to three categories of insider incidents and how an IRMP 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) and IRMP.
3. The IRMP conducts an inquiry of past and present online activity and projects future online activity.

Theft of IP

1. A workforce member who has access to sensitive IP (e.g., trade secrets, source code, engineering or scientific info, strategic plans) quits.
2. HR notifies the CSIRT and IRMP; they 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. A workforce member is experiencing extreme financial difficulty or has a sudden, unexplained change in financial status.
2. Management tells Security or HR, which tells the CSIRT and IRMP.
3. The IRMP 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 workforce members on the HR team's watch list. The teams should identify all the systems and information the high-risk workforce member has access to and ensure that audit logs are capturing a sufficient level of information to identify the information in the list below. (See **Best Practice 10**.)

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

When implementing auditing controls to detect malicious insiders, it might be necessary to perform more granular and verbose auditing. Ideally, the IT and IA teams have implemented a system information and event management (SIEM) solution that collects and correlates all security events. (See **Best Practice 12**.) Typically, SIEM solutions can be customized to look for certain patterns or extract events that meet a given set of criteria. For further discussion of centralized logging, see the SEI report, *Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination* [Hanley 2011b]. The IT and IA teams are also 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 help them detect all types of threats. Physical Security might be able to provide a video surveillance history. Depending on the depth of the established program, legal counsel's advice, and management's risk tolerance, the Physical Security team might also assist investigations by seizing, storing, and processing evidence. Finally, the Physical Security team might need to escort individuals off the organization's premises and work with a threat assessment and/or management team to assess the risk of future attacks, such as targeted violence against the organization.

The IRMP must operate under clearly defined and consistently enforced policies. Regular meetings help the IRMP team ensure compliance with these policies. These meetings 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 risks. Inter-departmental communication on a cross-organizational team helps the IRMP successfully prevent, detect, and respond to insider risks.

Workplace violence prevention programs, such as the U.S. Department of Agriculture's (USDA's) program,[23] similarly call for a threat assessment team consisting of members from multiple departments who work proactively and confidentially to identify and mitigate potential threats. The Occupational Safety and Health Act's (OSHA'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 address the employee privacy issue under well-defined circumstances, and the IRMP must do so as well.

Understanding and Avoiding Potential Pitfalls

IRMPs themselves can be the source of organizational performance problems, or even worse, exacerbate the insider risk that it is intended to mitigate. Previous work by CERT researchers identified the following categories of potential negative unintended consequences of establishing and operating formal IRMPs and suggestions for their mitigation:

- **Interference with legitimate whistleblower processes and protections**—There can be unintended consequences if the IRMP does not treat whistleblowing as a legitimate function with its own processes and procedures. Even if it does, workforce members might not trust that whistleblowers will be treated fairly.
- **Disruption of relationships among IRMP's management and workforce members**—An IRMP can strain the relationships among managers and the workforce members they manage at all levels. An organization's workforce can view the IRMP program staff in an adversarial

[23] See *The USDA Handbook on Workplace Violence Prevention and Response* at **http://www.dm.usda.gov/workplace.pdf [USDA 2001]**.

way—"they are trying to catch us doing something bad!" Workforce members can start gaming the system, hiding their behavior, or neglecting to report co-worker behaviors that the IRMP depends on for an effective detection system.

- **Management's lack of interest or loss of interest in the IRMP**—Support for the IRMP from the chief executive through all levels of management is crucial for the continued success of the IRMP mission. Many organizations establish an IRMP in response to a mandate, but if financial support is inadequate or there are other perceived higher priorities, support can dwindle to merely "paying lip service" to the need. The situation can become worse if the IRMP appears to be ineffective or if the false-positive rate is higher than expected. On the other hand, if the IRMP seems to solve all insider problems or no insider incidents actually occur, management might want to move financial support to other activities. Finally, if the IRMP appears to increase the liability of the organization, especially with regard to employment law, that increase can discourage the support needed for effective program implementation.
- **Purposeful misuse of the IRMP by its members or others**—The intended function of legitimate and necessary activities can be subverted by individuals who have other goals in mind. The IRMP can be used by unscrupulous individuals to falsely accuse or hide the malicious activities of insiders on the IRMP or their co-workers. Targeting certain workforce members over others or using program functions for purposes other than those intended, such as monitoring a workforce member's productivity for a general performance evaluation, is counter to effective functioning.
- **Unintentional misuse of the IRMP by its members or others**—Some misuse of the program's function can be unintentional. These accidents can lead to violations of HR employment law or unintentional disclosure of confidential information as part of the insider detection function. In some cases, these unintentional disclosures can be cause for regulatory consequences as well. In the context of GDPR, a personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed" [GDPR 2021]. The key difference between this GDPR context and a more traditional context is that it includes access, so personal data breaches can include scenarios where the data never leaves an organization. Accordingly, the need for IRMP members to understand the impacts of workforce monitoring and unauthorized or unfounded access to PII on privacy is underscored by regulatory demands. A side effect of insider investigations might also include harm to the reputation or career of someone who was under suspicion but later cleared of an illicit act.

It is fundamental that the organization consider the potential negative unintended consequences of its insider risk management efforts. Management must proactively anticipate unintended consequences and intentionally leverage controls to minimize their potential realization. For more information about potential unintended consequences from IRMPs, see the SEI report, *Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls* [Moore 2015].

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Collaborating across functions**—Strategy and operations for managing insider risk must holistically integrate cross-functional stakeholders to manage people-centric risk.
2. **Justifying the need for an IRMP**—Some organizations are not obligated to maintain a dedicated IRMP team and thus have no apparent incentive to do so. In these situations, instead of maintaining a dedicated team, these organizations can identify and train a specific set of resources to handle insider threats so a plan is in place ahead of time.
3. **Justifying IRMP funding**—It can be difficult to justify the IRMP's expenses, particularly with the high price of software solutions that typically require expert or advanced users to maintain and operate.

4. **Finding team participants**—Small organizations might not have workforce members dedicated to the various roles discussed above; however, a formal IRMP is still possible, even in a small organization. As long as management establishes policies and procedures about who to contact when an insider incident occurs and that person knows what to do, the organization should still be able to respond to an incident.
5. **Avoiding negative unintended consequences**—It is difficult to foresee all the implications of complex organizational change. IRMP designers and managers must think about negative unintended consequences that could happen in the planning stages, be vigilant for spotting them while in operation, and institute mitigations as needed.
6. **Recognizing the right to rectification**—Under GDPR, ***data subjects*** have the right to have inaccurate personal data corrected. For an organization, this means its workforce members can request both access to and corrections of personal data collected about them if circumstances allow. The IRMP and management should account for procedural, logistical, and operational risks that accompany working with workforce members on rectification requests.

Governance of an Insider Risk Management Program

A mature governance structure is essential to effectively developing, deploying, and managing an IRMP. The organization should implement a governance structure that does the following to supervise and advise its IRMP:

- Maintain an updated knowledge base related to insider risks, including staying current with the latest research and capturing lessons learned.
- Provide support to IRMP stakeholders to ensure the groups are meeting their objectives, providing the appropriate inputs to the IRMP manager, and appropriately communicating results and decisions to other IRMP stakeholders.
- Monitor governance practices to ensure that governing bodies are meeting IRMP needs, make recommendations for improvement, and refine the measures as needed.
- Capture and communicate IRMP success stories to internal and external stakeholders to increase program support.
- Perform processes including reviewing the budget, developing future technical requirements, continuously improving operational procedures, and managing risk.
- 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.

CASE STUDY: UNCHECKED ACCESS

In a sabotage case, an IT support business 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. He changed the passwords of all the organization's IT system administrators and shut down nearly all the organization's servers. He 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. He 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 IRMP. 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 IA 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 **Best Practice 20**.

The CERT Insider Threat Incident Repository 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 the 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 about SIEM can be found in **Best Practice 12**.) In addition, the organization should have carefully monitored remote access, as described in **Best Practice 13**.

CASE STUDY: SERIAL EMBEZZLER

An insider was employed as a bookkeeper by the victim organization. Over the course of approximately two years, she 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. She embezzled almost $200,000 from the organization.

Her 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 most of the embezzled funds.

Prior to this incident, the insider was convicted of a similar fraud. An insider risk 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 risk 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 risk team could have more closely monitored the insider's activities and discovered the fraud much earlier. Earlier fraud detection would have reduced the organization's losses.

This fraud case shows how an IRMP could have prevented, detected, and responded to insider risks. Similarly, the losses in the following theft of IP case might have been prevented or reduced if an IRMP had been in place.

CASE STUDY: CHEMICAL REACTION

The insider was employed as a research chemist by the victim organization. He was 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, including more than 15,000 Portable Document Format (PDF) files and more than 20,000 abstracts that contained the victim organization's trade secrets.

After the insider resigned, the victim organization detected his 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 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 the 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 risk team might have prevented, detected earlier, or reduced harm from this insider by monitoring unusual behavior on computer systems, which would have detected the insider's unusual downloads. The team then could have collaborated with senior management and HR to either (1) immediately terminate the insider's employment and engage law enforcement or (2) 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 the competitor company or any other organization acquired or used the IP.) At the very least, the IP was at a very high risk and out of the control of the victim organization for a period of time, and an insider risk team could have prevented, detected, and responded to the threat.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

- ☑ Obtain initial legal approval for all policies and intended practices. Request counsel to identify legal requirements for operating an IRMP, specifically with regards to what can and cannot be done.
- ☑ Establish periodic and event-driven protocols for legal review and approval (e.g., semiannual protocol reviews [periodic], inquiry-based request for legal assistance [event], decision to use enhanced monitoring [event]).
- ☑ Document your organization's definition of an insider threat incident. Identify any necessary triggers that can result in the event being classified as a data breach (e.g., the incident relates to the exfiltration of PII).
- ☑ Define a cross-functional insider threat incident response plan that describes who is responsible for what (and in what time period) during a response to an insider threat event.
- ☑ Consider risk transfer options for managing insider risk. Insurance providers or cybersecurity service providers might be able to be contractually engaged to act on and remedy an incident.

Large Organizations

The recommendations in this subsection apply to large organizations.

- ☑ Formalize an IRMP (with a senior official of the organization appointed as the program manager) that can monitor for and respond to insider risks.
- ☑ Define and deploy insider threat indicators in an insider threat analytic hub that can detect potential precursors to insider threat activity. Maintain continuous real-time monitoring and ensure that indicator lists are contextual to user groups and critical assets.
- ☑ Define and deploy insider risk metrics in an insider threat analytic hub that can aggregate and contextualize insider threat indicators to identify patterns of behavior associated with insider threat.
- ☑ Maintain frequent and close contact among IRMP stakeholders to preserve a readiness state.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AT-2 Literacy Training and Awareness AU-6 Audit Record Review, Analysis, and Reporting IR-4 Incident Handling SI-4 System Monitoring
NIST CSF	ID AM ID RA ID RM PR DS PR MA
NIST Privacy Framework	ID.RA-P GV.PO-P
NITTF Maturity Framework	ME-1 ME-2 ME-4 ME-5 ME-6 ME-17 ME-19
National Minimum Standards	B-1 B-2 B-3 B-4 B-5 B-6 B-7 B-8 G-1
CERT-RMM	Incident Management and Control Vulnerability Analysis and Resolution
ISO 27002	6.1.2 Information Security Coordination 15.1.5 Prevention of Misuse of Information Processing Facilities
CIS v7	Control 3
GDPR	Article 16 Right to rectification Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing Article 32 Security of processing

BEST PRACTICE 3

BEST PRACTICE 3

Clearly Document and Consistently Enforce Administrative Controls

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

Having a consistent, clear message about all organizational administrative controls (such as policies and procedures) reduces the chance that ***workforce members*** will inadvertently damage their organization, or lash out at it or other workforce members over a perceived injustice.

Organizations must ensure that their policies and controls are

- fair, including proportionate consequences for any violations
- communicated to the organization's entire workforce
- consistently enforced

Protective Measures

Administrative controls that are misunderstood, not communicated, or inconsistently enforced can breed resentment among workforce members and can result in harmful ***insider*** actions. There are multiple examples of these actions in the CERT Insider Threat Incident Repository. In these examples, because workforce members did not understand that the organization owned the ***intellectual property (IP)*** they created, they took that IP to their new job, violating organizational policies. These individuals were surprised when they were arrested for a crime they didn't know they committed.

The organization should ensure that administrative controls provide the following:

- concise and coherent documentation, including the justification for the policy or procedure (if needed)
- consistent and regular workforce training about policies, including their justification, implementation, and enforcement

The organization should be particularly clear about administrative controls regarding the following:

- 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 workforce member performance, including requirements for promotions and financial bonuses
- processes and procedures for addressing workforce grievances
- policies and procedures that define acceptable workplace behavior

As individuals join the organization, they should receive a copy of the organization's policies that clearly define (1) what is expected of them as a member of the workforce and (2) the consequences they can expect if they violate those policies. The organization should gather and retain evidence that each individual read and agreed to the organization's policies.

System administrators and anyone else with unrestricted access to information systems (i.e., ***privileged users***) present a unique challenge to the organization. The organization should consider creating a special policy for privileged users about acceptable use or rules of behavior. Organizations should reaffirm this policy with privileged users at least annually and consider implementing solutions to manage the related types of privileged accounts. (See **Best Practice 10**.)

Workforce member disgruntlement is a recurring factor in insider compromises, particularly in cases of insider information technology (IT) sabotage and workplace violence. In each case, the workforce member's disgruntlement was caused by some unmet expectation, including the following:

- an insufficient salary increase or bonus
- limitations on the use of organizational resources
- diminished authority or responsibilities
- perception of unfair work requirements
- perception of being treated poorly by co-workers, supervisors, or the organization

Clearly documenting policies and controls can prevent misunderstandings that can lead to unmet expectations. Consistently enforcing policies can ensure that workforce members do not perceive they are being treated differently from or worse than other workforce members. The organization must also ensure that its management is not exempt from policies and procedures. Otherwise, it appears that (1) not everyone in the organization is held to the same standards and (2) management does not fully support the policy or procedure.

Organizations are not static entities; they inevitably change their policies and procedures. An organization should routinely review its administrative documentation to ensure the documents continue to serve their intended purpose and are up to date. Workforce member constraints, privileges, and responsibilities also change. Organizations must do the following to cope with the effect change has on their workforce:

- Recognize that change is particularly stressful for workforce members.
- Acknowledge the increased risk associated with these stress points.
- Mitigate the risk by clearly communicating what workforce members can expect in the future.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Designing good policy**—It can be difficult to develop organizational policies and controls that are clear, flexible, fair, legal, and appropriate.
2. **Enforcing policy**—The organization must balance consistent policy enforcement with fairness, especially under extenuating circumstances (e.g., natural disasters, individual medical events).
3. **Managing policy**—The organization must regularly review and update its policies to ensure that they continue to meet the organization's needs and ensure that updates are distributed to all workforce members.

CASE STUDY: GRIEVANCE REVENGE

A government agency employed the insider as a lead software engineer. The insider led a team that was developing a software suite. After major issues were found with the first implementation of the software suite, agency 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 planning to outsource future development of the suite, demote her, reduce her pay, and move her to another office. While the project was still under the insider's control, she 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 her laptop, which she turned in when she resigned. She explained that she intentionally deleted the source code as part of wiping her laptop before turning it in, but she did not disclose that she retained a copy of the source code.

The organization discovered that she deleted the only known copy of the source code for the system—a safety-related system being used in production at the time. The system executable continued to function, but because of the missing source code, the organization was unable to fix bugs or make enhancements.

Investigators eventually discovered the encrypted copy of the software at the insider's home. After nine months, the insider finally admitted her crime and provided the cryptographic key to that encrypted software. She 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, distributed, and enforced clearly defined policies, procedures, and processes for software development. If the organization held all software projects to these requirements, the incident might have been avoided because the developer would have known what her employer expected. 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 source code to be submitted to the change management program manager to maintain software baselines. These measures would have ensured that someone other than the insider would have had a copy of the source code.

CASE STUDY: CONSOLIDATED POWER

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 who had the network passwords and had true knowledge of how the network functioned. He refused to authorize additional administrators. The organization reprimanded him for poor performance.

The insider threatened a co-worker after being confronted by that co-worker; the insider was then reassigned to a different project. The insider refused to surrender the network passwords, so the organization terminated his employment and had him arrested. As a result, the organization was locked out of its main computer network for nearly two weeks.

After the insider's arrest, his colleagues discovered that he installed rogue access points in hidden locations and set up the organization's system to fail if anyone attempted to reset it without the proper passwords. The insider provided passwords to the police, but none of them worked. He 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 redundancy reduces the likelihood of a system failing due to the loss or malicious action of an employee. It also enables a system of checks and balances where fellow administrators monitor the network for hardware or software changes.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations. Some organizations might not have a department dedicated to security (e.g., physical security, IT security). However, the underlying theme of this best practice still applies.

☑ Ensure that senior management advocates, enforces, and complies with all organizational policies. Policies that do not have management buy-in will not be enforced equally and will fail. All levels of management must comply with policies. If management does not comply, subordinates will see this noncompliance as a sign that the policies do not matter or they are being held to a different standard than management. The organization should also communicate exceptions to policies clearly to the entire workforce.

☑ Ensure that management briefs the entire workforce about all policies and procedures. Employees, ***trusted external entities (TEEs)***, and temporary workers should sign acceptable-use policies and acceptable workplace behavior policies when they are hired and once every year after that, or when a significant change occurs. Signing these policies is also an opportunity for the organization and its employees, contractors, and TEEs to reaffirm any nondisclosure agreements.

☑ Ensure that management makes it easy for workforce members in all departments to access the organization's policies. Posting policies on the organization's internal website can facilitate widespread dissemination of policies and ensure that everyone has access to the latest policy information.

☑ Ensure that management mandates annual refresher training for the entire workforce. Refresher training should cover all facets of the organization, not just information security. Training should include human resources, legal, physical security, and other areas of interest. Training can include, but is not limited to, changes to policies, issues that emerged over the past year, and information security trends.

☑ Ensure that management enforces policies consistently across the entire workforce to prevent the appearance of favoritism or injustice. The organization's Human Resources department should establish policies and procedures that specify the consequences of particular policy violations. This approach makes it easier for the organization to clearly and concisely enforce its policies.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	PL-1 Policy and Procedures PL-4 Rules of Behavior PS-8 Personnel Sanctions
NIST CSF	ID GV PR IP
NIST Privacy Framework	GV.PO-P GV.RM-P GV.MT-P
NITTF Maturity Framework	
National Minimum Standards	
CERT-RMM	Compliance
ISO 27002	15.2.1 Compliance with Security Policies and Standards
CIS v7	Control 6
GDPR	Article 32 Security of processing

BEST PRACTICE 4

BEST PRACTICE 4

Beginning With the Hiring Process, Monitor and Respond to Suspicious or Disruptive Behavior

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

Organizations should proactively identify and immediately address suspicious or disruptive behavior to reduce the risk of ***insider threats***.

Protective Measures

The organization's approach to reducing its ***insider risk*** should start in the hiring process. Background checks on prospective ***workforce members*** should reveal previous criminal convictions. These background checks should include a credit check, verifying credentials and past employment, and discussions with prior employers regarding the individual's competence and approach to dealing with workplace issues.

The organization must consider legal requirements (e.g., notifying the candidate and securing consent from the candidate) when creating a background-check policy. Prior to making employment decisions based on background information, the organization must consider legal guidance, including the Equal Employment Opportunity Commission's (EEOC's) best practices[24] and state and local regulations limiting the use of criminal background checks or credit checks. The organization must use background information lawfully, with due consideration of the nature and duration of any offense, as part of a risk-based decision process for determining the workforce member's access to critical, confidential, or proprietary information or systems.

The organization should require background checks for all potential workforce members; contractors and subcontractors should be investigated just as thoroughly as employees.[25] Background-check information should be safeguarded appropriately to protect the privacy of the workforce member in accordance with the General Data Protection Regulation (GDPR) and guidance from any relevant European Union (EU) member state.

The organization should assign risk levels to all positions and more thoroughly investigate individuals applying for positions assigned with a higher risk or that require a great deal of trust [NIST 2020]. Periodic reinvestigations might be warranted when individuals move to higher risk roles in the organization, again complying with all legal requirements.

The organization should invest its time and resources in training its supervisors to recognize and respond to workforce members' inappropriate or concerning behavior. 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 workforce member to commit repeated violations

[24] **http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm** [EEOC 2012]

[25] See **Best Practice 1** for further discussion on background checks.

that escalated in severity and increased the risk of significant harm to the organization. The organization must consistently enforce policies and procedures for all workforce members, including the consistent investigation of and response to rule violations.

Because financial gain is a motive for committing fraud, the organization should be alert to any indication from workforce members of financial problems or unexplained financial gain. ***Malicious insiders*** have used information technology (IT) to modify, add, or delete organizational data (as opposed to software or software 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 a workforce member's financial situation, including increased debt or expensive purchases, might be signs of potential insider threat. Again, the organization must consider legal requirements, such as workforce member notifications, when responding to such situations.

The organization should have policies and procedures that enable workforce members to report concerning or disruptive behavior by their co-workers. To respond to concerning or disruptive behaviors, the organization should take consistent monitoring steps according to written policies to eliminate the biased application of monitoring or even the appearance of such a bias.

The organization should investigate all reports of concerning or disruptive behavior until an appropriate organizational response is determined. If a workforce member exhibits concerning behavior, the organization should respond with care. Disruptive workforce members should not be allowed to migrate from one position to another in the organization and evade documentation of disruptive or concerning activity.

The organization should treat ***threats*** and boasts about malicious acts or capabilities (e.g., "I could just come in here and take everyone out!") and other negative sentiments as concerning behavior. Many workforce members might have concerns and grievances from time to time, and a formal and accountable process for addressing those grievances can satisfy those who might otherwise resort to malicious activity. In general, organizations should help any workforce member resolve their workplace difficulties.

Once the organization identifies a workforce member's concerning behavior, it might take several steps to manage the risk of malicious activity. These steps can include the following:

- evaluating the workforce member's access to critical information ***assets*** and level of network access
- reviewing logs of the workforce member's recent activity
- presenting the workforce member with options for coping with issues causing the behavior, such as access to a confidential Employee Assistance Program (EAP)

If the workforce member exhibits potentially violent behavior, the organization should devise a thorough threat assessment and management plan.

Legal counsel should ensure that all monitoring activities are within the bounds of the law. For example, private communications between workforce members 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 employee 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 a workforce member's email messages or computer files for monitoring simply because the workforce member made a protected disclosure [NIST 2018a].

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Sharing information**—The organization can find it difficult to share workforce member information with those charged with protecting organizational systems. To ensure compliance with laws, regulations, and company policies, the organization must consult legal counsel before implementing any program that involves sharing workforce member information.

2. **Maintaining workforce morale**—It can be difficult for the organization to avoid conveying a sense that "big brother" is watching over every workforce member's action, which can reduce morale and affect productivity.
3. **Using arrest records**—In 2012, the EEOC issued 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 [EEOC 2012]. This guidance clarifies that employers should not rely on arrest records instead of convictions, because arrest records are less indicative that the candidate actually engaged in 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, the organization must consult legal counsel before using or disclosing arrest record information from a background check. Related to this, a previous CERT study showed that 30% of ***insiders*** who committed IT sabotage had a previous arrest history. Ultimately, that correlation might not be meaningful. A 2011 study using a large set of data from the federal government showed that 30% of all United States (U.S.) adults have been arrested by age 23. In 1987, a study showed similar statistics, with 35% of people in California having been arrested between the ages of 18-29 [Tillman 1987]. Many insider crimes were performed by insiders over age 29. Future research that focuses on particular job categories might show different averages of previous arrest rates for insiders convicted in the U.S. However, currently, the use of arrest data is both legally and scientifically questionable.
4. **Monitoring only legally allowable communications**—The organization must take special care to prevent monitoring private communications between workforce members and their doctors and lawyers as well as between federal workers and the Office of Special Counsel or an agency inspector general. In the EU, the organization should take special care to allow for additional notices to workforce members related to monitoring email or other electronic correspondence.[26]

CASE STUDY: CONTRACTOR WITH A HISTORY

An organization employed a contractor to perform system administration duties. The contractor compromised the organization's systems and obtained confidential data about millions of its customers. Although 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 case illustrates the need to contractually require contractors to perform background checks on their employees.

CASE STUDY: UNTRUSTWORTHY EXECUTIVE

A large shipping and storage corporation employed the insider as an executive-level officer. After 11 years of employment there, he gained the company's trust. However, prior to his employment at the victim organization, he stole money from a few other companies he worked for. He was convicted, but he served his sentence on work release. After claiming that he "cleaned up his act," he was employed by the victim organization and quickly climbed to an 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 the prices of invoices charged to his department and collected part of the payments. Furthermore, he paid an outside organization run by a conspirator for services never rendered. In return, the conspirator wired part of the payments to him. 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. He was sentenced to six years of imprisonment and ordered to pay full restitution.

[26] In a 2007 case, *Copland v. United Kingdom*, failure to notify an employee about the collection and storage of electronic correspondence was deemed a violation of employee privacy. Additional guidance can be found in Article 29 Working Party "Working document on the surveillance of electronic communications in the workplace" [Working Party 2002] and "Opinion 2/2017 on data processing at work" [Working Party 2017].

This case illustrates the need for organizations to consider how a potential employee's background can imply an increase of insider risk before making a hiring decision. Management must not only evaluate a candidate's complete background and assess the organization's willingness to accept the risk before extending an offer to a candidate but also consider what additional mitigations are appropriate. Organizations must also ensure that legal agreements with ***trusted external entities (TEEs)*** convey the organization's requirements for background checks.

CASE STUDY: CERTIFIED INTIMIDATION

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 his co-workers that he installed ***backdoors*** and planned to use them to harm the organization, but the remaining co-workers were afraid to speak up due to the recent terminations. He 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, he falsely claimed to hold a certification and that he was recommended by a headhunter. The organization failed to verify that claim. He also concealed his violent criminal history, including assault with a deadly weapon, corporal injury to a spouse, possession of a firearm, and the fraudulent use of two Social Security numbers (SSNs).

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

After the insider's termination, the organization noticed that he repeatedly attempted to remotely access its servers. The organization asked him to stop, but he denied making such attempts. The organization anticipated the insider's attack and hired a computer security consulting firm. The consultants blocked his Internet protocol address (IP address) at the organization's firewall, deleted his accounts, checked for backdoors, and watched for illicit access. The consultants failed to check one server where the insider had access. Later, the consultants performed a forensic examination and detected that he used virtual private network (VPN) accounts to log in over the two-week period between his termination and the incident.

The organization was unaware that those accounts existed; the insider created them before his termination. Those accounts were in the names of his superiors and gave him remote access to the organization's ***critical assets***. The insider accessed the server, deleted crucial files, and rendered the server inoperable. He was arrested, convicted, sentenced to one year of imprisonment, and ordered to undergo mental health counseling.

In this case, the organization failed to do the following:

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

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

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

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

His co-workers and management should have raised concerns about these events. Any workforce member who has concerns about another's actions should be able to report the issue without fear of reprisal. The availability of an anonymous 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.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Ensure that potential workforce members undergo a thorough background check, which, at a minimum, should include a criminal background check and credit check.

☑ Encourage workforce members to report suspicious behavior to appropriate personnel for further investigation.

☑ Provide a confidential method for reporting suspicious behavior without repercussions.

☑ Investigate and document all suspicious or disruptive behavior.

☑ Enforce policies and procedures consistently for all workforce members.

☑ Consider offering an EAP. These programs can help workforce members deal with many personal issues confidentially.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	PS-1 Policy and Procedures PS-2 Position Risk Designation PS-3 Personnel Screening PS-8 Personnel Sanctions
NIST CSF	DE AE
NIST Privacy Framework	PR.PO-P
NITTF Maturity Framework	ME-4 ME-15
National Minimum Standards	C-1 H-1 H-2 H-3 H-4
CERT-RMM	Monitoring Human Resource Management
ISO 27002	8.1.2 Screening
CIS v7	
GDPR	Article 10 Processing of personal data relating to criminal convictions and offenses Article 88 Processing in the context of employment Article 29 Working Party Opinion 2/2017 on data processing at work Article 29 Working Party Working document on the surveillance of electronic communications in the workplace

BEST PRACTICE 5

BEST PRACTICE 5

Anticipate and Manage Negative Issues in the Work Environment

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

When negative workplace issues arise, having clearly defined and communicated policies helps the organization consistently enforce its policies and reduce risk.

Protective Measures

The organization must communicate its policies and practices to new ***workforce members*** on their first day. These policies and practices should include acceptable workplace behavior, dress code, acceptable use policies, working hours, career development, conflict resolution, and other workplace issues. The mere existence of these policies is not enough; new and veteran workforce members must all be aware of these policies and the consequences of violating them.

The organization must enforce its policies fairly and consistently to maintain a harmonious work environment. Inconsistent enforcement of policies quickly leads to animosity in the workplace. In many analyzed ***insider threat*** cases, inconsistent enforcement or perceived injustices in 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 insiders to sabotage information technology (IT) ***assets*** or steal information.

Raises and promotions (e.g., annual cost of living adjustments, performance reviews) can have a major impact on the workplace environment, especially when workforce members expect raises or promotions but do not receive them. Workforce members should not count on these awards as part of their salary unless they are assured they will receive them in their contract; even then, the award amount specified in the contract might be variable. However, when these awards become part of the company's culture, workforce members expect them year after year.

The end of a performance period is one time when workforce members can have unmet expectations. If management knows in advance that the organization cannot provide raises or promotions as expected, it should inform workforce members as soon as possible and offer an explanation. Other times of heightened financial uncertainty in the workplace environment include the end of a contract performance period, especially when there is no clear indication that 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 workforce members know there will be a reduction in the workforce, but they do not know who will be laid off. Likewise, for example, an incumbent contractor who loses a re-compete bid might be disappointed. In all cases of heightened uncertainty or disappointment surrounding raises, promotions, and layoffs, the organization should be on increased alert for abnormal behavior and enact enhanced security measures to mitigate ***insider risk***.

Workforce members with issues need a way to get assistance in the organization. Workforce members must be able to openly discuss work-related issues with management or Human Resources staff without the fear of reprisal or negative consequences. When workforce issues arise because of external factors, including financial and personal stressors, workforce members can find a service such as an Employee Assistance Program (EAP) helpful. These programs offer confidential counseling to assist workforce members, which helps them restore their work performance, health, or general well-being. Cases in the CERT Insider Threat Incident Repository show that financial and personal stressors appear to motivate many insiders who stole or modified information for financial gain. If these insiders had access to EAPs, they might have found another way to cope with their problems.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Predicting financial conditions**—The organization can find it difficult to predict financial issues that could affect workforce member salaries and bonuses.
2. **Maintaining trust between workforce members and management**—Workforce members might be reluctant to share information with their manager about work-related issues for fear of it affecting multiple aspects of their employment.

CASE STUDY: TURNCOAT EMPLOYEE

A manufacturing company employed the insider as a salesperson. The organization required its salespeople to regularly update a proprietary customer- and lead-tracking system. After being warned he would be fired if he did not update the system as required, the insider still neglected to do so; the organization penalized the insider with a $2,500 salary reduction instead of firing him.

The insider became disgruntled and sought employment with a competitor. He informed the competitor that he planned to bring customer information with him if he was hired. The victim organization became suspicious of his activities, causing him to tell his contact at the competitor to delete all of their email correspondence, which the contact did.

The insider received an employment offer from the competitor. Two weeks later, he accessed the victim organization's computer system and downloaded customer records to his home computer. He 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. He immediately began contacting customers from the victim organization and recruiting them for the beneficiary organization. Once the victim organization discovered his 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 he 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, he might have been stopped before he could disclose the customer data. This case also underscores the need for nondisclosure agreements (NDAs), acceptable use agreements, and even noncompetition agreements.

CASE STUDY: DISGRUNTLED OVER LAYOFFS

The victim organization, a bank, triggered a mass resignation of employees who were 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 insider signed a non-solicitation agreement on the day of her resignation and later stole customer information via remote access. Six months before these events, she and a former co-worker planned to form a new company and hire their colleagues, with whom they held meetings. The organization filed a civil lawsuit against her.

This case highlights the need for organizations to proactively protect their data. Layoffs heighten tension and stress at an organization. This tension can lead to a negative atmosphere; management should be aware of the insider risk such an atmosphere poses. As part of an organization's risk management process, it should identify critical intellectual property (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 might have been possible.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Enhance the monitoring of workforce members who have an impending or ongoing personnel issue in accordance with the organization's policy and laws. Enable additional auditing and monitoring controls outlined in policies and procedures. Regularly review audit logs to detect activities outside of the workforce member'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 workforce members. This communication allows for a more transparent organization, and workforce members can better plan for their future.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	PL-4 Rules of Behavior PS-1 Policy and Procedures PS-6 Access Agreements PS-8 Personnel Sanctions
NIST CSF	DE AE
NIST Privacy Framework	PR.PO-P
NITTF Maturity Framework	ME-16
National Minimum Standards	C-1 E-1 E-2 E-3
CERT-RMM	Human Resource Management
ISO 27002	8.2.1 Management responsibilities 8.2.3 Disciplinary process 8.3.1 Termination responsibilities
CIS v7	
GDPR	

BEST PRACTICE 6

BEST PRACTICE 6

Consider Threats From Insiders and Trusted External Entities in Enterprise-Wide Risk Assessments

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	✓	✓	✓	✓	✓	✓	○

Organizations must develop a comprehensive, risk-based security strategy to protect their ***critical assets*** against ***threats*** from inside and outside the enterprise, including from ***trusted external entities (TEEs)***,[27] such as outsourced ***workforce*** payroll and benefit services, system administration, patch development services, security services, Internet service providers (ISPs), and cloud service providers. (See **Best Practice 16**.) All of an organization's resources, not just its ***workforce members***, should understand the stakes of system compromise, loss or exposure of critical data, and impact (both physically and legally) of workplace violence incidents. (See **Best Practice 9**.)

Protective Measures

Most organizations find it impractical to implement 100 percent protection from every threat to every organizational resource. Instead, the organization should expend its security efforts commensurately with the criticality of the information or other resources 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. The organization must carefully determine the likelihood and potential impact of an ***insider*** attack on each of its ***assets*** [NIST 2018a], including human life.

The 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 an organization identify critical assets, potential threats to those assets, and mission impact if those assets are compromised. The organization 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.[28] Likewise, proper policies and controls should be implemented and adhered to regarding workplace violence prevention. Having too many security restrictions can impede the organization's mission, and having too few can permit a security breach.

[27] External entities are trusted in the sense that they are given authorized insider access.

[28] See **https://www.sei.cmu.edu/about/divisions/cert** for information about CERT research in organizational security.

Organizations often focus too much on low-level technical vulnerabilities. For example, many organizations rely on automated computer and network vulnerability scanners. While such techniques are important, CERT research 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 this best practice's Case Studies section.

Many organizations focus on protecting information from access by external parties but overlook insiders. An information technology (IT) 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. An organization must recognize the potential danger posed by insiders who have knowledge of and access to its critical assets, and it 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 the other organizations and individuals they collaborate, partner, contract, or otherwise associate with. Specifically, outsourced TEEs (e.g., contractors, consultants, ISPs, cloud service providers) should be considered to be potential insider threats in an enterprise risk assessment. The boundary of the organization’s enterprise should 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.

The organization should consider making contractual agreements that ensure that all TEEs use a commensurate level of scrutiny for vetting workforce members, protecting data, and enforcing information security policies. Some TEEs might provide little, if any, transparency into or flexibility regarding service performance, especially public and shared infrastructure service providers such as power, water, telecommunications, police, and fire fighters. In those cases, the organization should manage their risk based on available information and experience.

Greater transparency and flexibility are possible with custom service providers (e.g., contractors conducting system administration). In the middle are IT service providers (e.g., ISPs, cloud service providers, patch developers). The organization can have some influence and control over these providers’ practices. For example, the organization can do the following:

- scrutinize the practices of providers to the extent possible
- review guidance on the provider’s products by the government, regulators, or others
- understand the risks associated with the components to be used
- choose to accept associated risks or switch providers
- test patches that affect critical services prior to their installation
- ultimately retain control over which patches are actually installed

The organization’s reliance on TEEs is known in the resilience standards and literature as an *external dependence*, and the management of the relationships with external entities is known as *external dependencies management (EDM)* [CISA 2021a].

> [EDM guidance recommends that,] *to effectively manage external dependencies, organizations should establish* [the following:]
>
> - *a strategy and basic plan for EDM*
> - *key processes for identifying, prioritizing, monitoring, and tracking external dependencies*
> - *guidance and procedures on the formation of relationships with external entities*
> - *an approach for managing and governing existing external entity relationships*
> - *ongoing oversight, reporting, and correction of external entity performance*
> - *an approach for improving the organization’s EDM processes and program*

This EDM guidance provides useful recommendations for organizations that wish to limit their exposure to insider threats in their TEEs.

An organizational risk assessment that includes insiders as a potential threat addresses an insiders' potential impact to the confidentiality, integrity, and availability of the organization’s mission-critical information and resources. A malicious insider can affect the integrity of the organization’s information in various ways (e.g., manipulating customers’ financial information or defacing the organization’s websites). A malicious insider can also violate the confidentiality of information by stealing it (e.g., trade secrets, customer information, or sensitive managerial email messages) and inappropriately disseminating it.

Many organizations lack the appropriate agreements governing confidentiality, IP, and non-disclosure to effectively instill their confidentiality expectations in their workforce members and external entities. Having appropriate agreements better equips the organization for legal action. Insiders can also affect the availability of their organization’s information by deleting data, sabotaging entire systems and networks, destroying backups, and committing other denial-of-service (DoS) attacks. Finally, insiders can perpetrate workplace violence that results in the loss of life.

In the types of insider incidents just mentioned, current or former workforce members, or TEEs could compromise their organization’s critical assets. The organization should focus its protection strategies on those assets: financial data, confidential or proprietary information, other mission-critical systems, personnel, and data. In addition to IT assets and personnel, the organization’s critical assets can also include physical assets such as facilities or vehicles. The organization should also protect its workforce members with appropriate safety and security training.

Mergers and acquisitions can also create a volatile environment that poses potential ***insider risk*** for the acquiring organization. Before the acquiring organization transfers workforce 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 checks and before 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 organization’s untrusted system to the acquiring organization’s trusted system. If these systems must be connected, the acquiring organization should first conduct a risk assessment on the new systems and mitigate any threats found. The acquiring organization must now also consider adding confirmation of the newly acquired external entities’ General Data Protection Regulation (GDPR) compliance to its due diligence research and contractual agreements since the acquiring organization is taking ownership of the tracking and reporting of ***data breaches*** to regulators.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Assessing risk**—The organization can have difficulty comparing the levels of risk from insiders versus outsiders.
2. **Lacking experience**—The organization might not include insider risk as part of enterprise risk assessments, so assessment participants might need training.
3. **Prioritizing assets**—Data and physical information system assets can be complex (e.g., individual hosts running multiple virtual machines with different business needs) or even be scattered across the organization, making it difficult to assign risk or priority levels. (See **Best Practice 1** for further discussion of asset prioritization.)

CASE STUDY: DORMANT LOGIC BOMB

A mortgage company employed a contractor as a programmer and UNIX engineer. The organization notified the insider that her contract would be terminated because she made a script error earlier in the month, but she 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 the monitoring of alerts and logins, delete the root passwords to the organization's servers, and erase all data (including backup data) on those servers. She designed the script to remain dormant for three months and then greet administrators with a login message. Five days after her 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 contractor of changes in the terms of their employment. In this case, the organization should not have permitted the contractor to finish out the workday and should have had her 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 electronic backup processes. The organization should consider restricting backup and restore capabilities to a few select individuals to prevent malicious insiders from destroying backup media and other critical system files and from sabotaging the backup process.

CASE STUDY: ABUSIVE CONTRACTOR

A government agency employed a contractor as a systems administrator who 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 behavior 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 organization's system administrators to ask if the machines and servers were functioning properly, which aroused their 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 of supervised release. On his job application to the organization, the contractor 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 TEEs that require the contractor to perform background checks 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 background checks on its employees.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Have all workforce members and TEEs sign nondisclosure agreements (NDAs) upon hiring and termination of employment or contracts.

☑ Ensure that all workforce members and TEEs sign workplace violence prevention and/or appropriate workplace behavior documentation when hired.

☑ Ensure all workforce members and TEEs routinely re-acknowledge agreements and policies (e.g., acceptable use policy [AUP], social media policy, mobile device policy, ***intellectual property [IP]*** policy).

☑ Ensure each TEE performs background checks on all of its workforce members who will have access to your organization's systems or information. These background checks should be commensurate with your organization's own background checks and be required as a contractual obligation.

☑ During a merger or acquisition, perform background checks on all workforce members 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 the garbage. Electronic documents can be easier to track.

☑ Avoid direct connections with the information systems of TEEs if possible. Provide TEEs 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.

Large Organizations

The recommendations in this subsection apply to large organizations.

☑ Prohibit personal items in secure areas because they can be used to conceal company property or to copy and store the organization’s data.

☑ Conduct a risk assessment of all systems to identify critical data, business processes, and mission-critical systems. (See the National Institute of Standards and Technology [NIST] Special Publication 800-30, *Risk Management Guide for Information Technology Systems* for guidance [NIST 2002].) Be sure to include insiders and TEEs 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, restrict encryption tools to authorized users, and 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 from having access to system backup media or electronic backup processes.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	RA-1 Policy and Procedures RA-3 Risk Assessment PM-9 Risk Management Strategy
NIST CSF	DE AE
NIST Privacy Framework	PR.PO-P
NITTF Maturity Framework	ME-4
National Minimum Standards	B-2 E-1 G-1 G-2 G-3 G-4
CERT-RMM	Access Control and Management External Dependencies Management Human Resource Management
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
CIS v7	
GDPR	Article 33 Notification of a personal breach to the supervisory authority

BEST PRACTICE 7

BEST PRACTICE 7

Be Especially Vigilant Regarding Social Media

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	✓	✓	✓	✓	✓	✓	○

Workforce members who use social media sites can threaten an organization's ***critical assets***. Organizations should provide training, policies, and procedures about how workforce members should use social media.

The recommendations in this best practice are based on ***malicious insider*** cases, results from the *2015 CyberSecurity Watch Survey* [PWC 2015], and an information security analysis of this ***threat*** vector. This best practice also considers findings from CERT research on unintentional ***insider threat*** cases [SEI 2014a, SEI 2014b, Strozer 2014].

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 be obtained from the social media profiles of many users or by searching online. The availability of this information opens workforce members 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 2009].

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

Social media sites can also be used to determine who within an organization might be susceptible or willing to participate in an attack. For example, if a workforce member participating in a social networking site posts negative comments about their job or organization, attackers can see this as a sign that the workforce member is disgruntled and possibly open to participating in illicit activity. Malicious individuals can also use these sites to map an organization's workforce structure and identify people in high-value roles (e.g., C-level executives, financial personnel, system administrators) for targeted attacks.

Organizations and individuals alike must practice sound operational security (i.e., OPSEC) with social media. What can seem like a simple social media interaction can reveal a lot about an individual or organization. For example, a workforce member who uses an online support forum to troubleshoot a device or software product can unintentionally reveal sensitive organizational information, such as a particular product name and version or Internet protocol (IP) address.

Social media profiles and web searches can reveal a large amount of personal information, which attackers can use to compromise personal accounts. For example, resetting a user's email password can require answering a few security questions (e.g., place of birth, date of birth, mother's maiden name, ZIP code, name of favorite sports team, name of hometown). Attackers can find the answers to these questions on social networking sites, making it relatively simple to reset another user's email password.

Memorizing and using bogus information 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 can enter bogus password recovery information unique to each site. Password recovery is more complicated for users of multiple sites, but the password-recovery threat vector would be lessened.

Organizations must establish policies and procedures to protect against insider threat. Policies should address what is and is not acceptable workforce member participation in social media sites.[29] Organizations should consider what their workforce members might post, no matter how harmless it may seem. For example, it might be appropriate to have a policy that prohibits workforce members from posting about organizational projects since such posts can reveal sensitive information.

Every organization should include social engineering training in its security awareness training program. This training should describe how information gathered from social media can be used to cause harm, including potential recruitment into a criminal organization or extremist group. This training could include a live demonstration about what types of data can be collected from a randomly selected profile. To avoid embarrassing a workforce member, the trainer should select the profile of a person not affiliated with the organization or use screen captures of a workforce member's profile with identifying information redacted.

Organizations must ensure that their social media policies are legal. In her third report on the legality of language in employers' social media policies [Purcell 2012], Anne Purcell, the National Labor Relations Board's (NLRB's) Acting General Counsel, recommends avoiding policy language with the following characteristics:

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

[29] For a list of sample social media policies and templates see **https://www.shrm.org/resourcesandtools/tools-and-samples/policies/pages/socialmediapolicy.aspx** [SHRM 2021].

If an organization monitors social media, it must do so cautiously. Employers must be careful not to penalize or fire workforce members for discussing work conditions online, such as their salary. Protected speech might even include complaints about supervisors. Another concern is that using social media could inform an organization about certain protected class statuses (e.g., race, disability, parenthood, or sexual orientation), which could open the door to discrimination lawsuits.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Establishing, monitoring, and enforcing policy**—The organization can find it difficult to control what workforce members post on social media sites. Training that includes a personal takeaway can help increase awareness and compliance. The organization can also find it challenging to monitor all social media sources, especially when workforce members use the sites' privacy controls.
2. **Classifying data**—The organization should have a data classification policy that establishes what protections must be afforded to data at different sensitivity levels. Establishing this policy requires a review of the organization's information, and the organization must train its entire workforce about these data classification levels.
3. **Monitoring social media legally**—If the organization monitors social media, it must do so with the assistance of legal counsel. The legal landscape in this area is currently changing, so related policies should be reviewed and changed as needed.
4. **Limiting reliance on social media data**—An organization with European Union (EU) workforce members and ***trusted external entities (TEEs)*** might want to limit the extent to which they rely on social media as a data source and the likelihood that social media data might be available for analysis in the future. The General Data Protection Regulation (GDPR) grants individuals the ***right to be forgotten****,* which means that social media providers can, in some circumstances, be compelled to delete an individual's data at their request. If an individual realizes that social media content might make them less appealing to a future employer, or jeopardize a relationship with their current employer, they might seek to remove it from the Internet altogether.

CASE STUDY: FICTIONAL CHARACTER

As an experiment, 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 with her, taken while he was on patrol overseas, which contained embedded geolocation data. Another person 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 case study 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. If the other people who had contact with the fictitious cyber threat analyst verified her credentials, they might not have fallen victim to the researcher's experiment.

CASE STUDY: DISCLOSED INFORMATION ONLINE

An attacker compromised the email account of a former United States (U.S.) political 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 the candidate met their spouse) and reset the password. The attacker then read through her email and posted it to a public forum [Zetter 2008].

This case study emphasizes that the organization should train its workforce about the risks of disclosing information online, especially personal information. Disclosing a seemingly harmless piece of information can lead a potential attacker down a “bread-crumb trail” of information, enabling the attacker to compromise personal or even organizational accounts and infrastructure.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to 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 email messages or phone calls to the organization’s information security team members, who can track the email messages to identify any patterns and issue alerts to users.

Large Organizations

The recommendation in this subsection applies to large organizations.

☑ Consider monitoring the use of social media across the organization, but that monitoring should be limited to looking in a manner approved by legal counsel for postings by employees, contractors, and external entities.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AT-2 Literacy Training and Awareness AT-3 Role-Based Training PS-1 Policy and Procedures PS-3 Personnel Screening
NIST CSF	DE AE
NIST Privacy Framework	PR.PO-P
NITTF Maturity Framework	
National Minimum Standards	E-1 G-1
CERT-RMM	Monitoring
ISO 27002	
CIS v7	
GDPR	Article 29 Data Protection Working Party Opinion 2/2017 on data processing at work

BEST PRACTICE 8

BEST PRACTICE 8

Structure Management and Tasks to Minimize Insider Stress and Mistakes

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

Organizations must understand the psychology of their ***workforce*** and the demands placed on the workforce by leadership. Having that knowledge, organizations should create a work environment that is conducive to positive outcomes.

An organization's drive for productivity can cost it efficiency and security. While it's human nature to make mistakes, rushing to complete multiple tasks in a high-stress environment can cause someone to make even more mistakes. Examples of these mistakes include unintentionally disregarding ***social engineering***, forgetting about an important ***security control***, or failing to consider the repercussions of sharing information. In high-stress environments, ***workforce members*** can perceive that their concerns are not being considered and develop negative attitudes toward management and the organization. Mistakes and negative attitudes in the workplace can create ill will and increase the chance that a workforce member will undermine the trust the organization bestowed on them.

Protective Measures

To reduce the likelihood of ***insider risk***, an organization should consider ways to reduce the stress levels of its workforce. These reduction measures include the following:

- focusing less on top-line productivity and more on achieving productive outcomes
- instituting policies and practices that allow workforce members more time to achieve mission-oriented objectives
- following responsive, human-oriented management rather than project-oriented management
- scheduling time to plan tasks and spark new ideas for doing things that benefit the organization

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Balancing stress with productivity**—It can be difficult for the organization to find the balance between preventing workforce members from leaking data and encouraging them to achieve desired outcomes.
2. **Baselining workforce productivity**—Workforce members achieve at varying levels; similarly, they reach stressful points at different times and under different conditions. It can be difficult to measure the stress of the entire workforce to determine who is overworked, skipping steps, and/or multi-tasking.

3. **Getting a return on investment**—The organization must weigh the costs and risks that reducing stress has on workforce productivity against the cost of data exfiltration and other forms of ***insider threat***.

Case Studies

Stress can cause ***insiders*** to make mistakes that can damage the organization. It can also cause insiders to commit malicious attacks. The following case studies describe five unintentional and two ***malicious insider*** incidents.

In all of these cases, it is clear 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 to neglect checking every action against the simple question, "Should I do this?" Lowering the stress level at the organization, lowering the workload of overburdened workforce members, and encouraging quality outcomes could have limited, if not eliminated, the damage caused in all these cases.

Unintentional Insider Threat Cases

The following five cases illustrate how stress can cause unintentional insider threat.

CASE STUDY: WARTIME STRESS

One of the costliest (and oldest) cases in the CERT Insider Threat Incident Repository happened during World War II. The chairman of the Military Affairs Committee disclosed confidential military information during a press conference. The disclosed information dealt with the underwater depths of Japanese and United States (U.S.) submarines and their 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 the deaths of 800 service members to the chairman's disclosure.

CASE STUDY: FATIGUE

A tired and overworked bank teller fell asleep at the keyboard and accidentally transferred millions of dollars.

CASE STUDY: RUSHED WORK

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 was trying to distribute the minutes quickly and did not realize that they entered incorrect addresses in the email header.

CASE STUDY: OVERLOOKED PROCEDURES

A file cabinet that was sent to a correctional facility for repair contained highly classified documents that were not removed prior to transport. An inmate who was repairing the cabinet found two dozen pages of classified material. Since it was a priority to repair the cabinet quickly, no one reviewed its contents before moving it.

CASE STUDY: HURRIED TASKS

During a magazine promotion, a coding error exposed the personal data of about 12,000 people, including the credit card information of about 50 people. Attackers used some of this exposed information for identity theft. The coders at the magazine were rushed to finish the coding in time to launch the promotion.

Malicious Insider Threat Cases

In terms of malicious ***threat*** induced by stress, the following two cases “paint the picture” clearly.

CASE STUDY: ESCALATING STRESS

The insider—a director at the victim organization, a local government entity—was part of an escalating stressful conflict with a government official. As a result, the insider shredded documents from the government official’s human resources (HR) files. The following day, the insider was caught deleting email from the computer of a subordinate, who observed and reported the previous day’s shredding incident. Roughly two weeks later, the insider began deleting work-related email messages and spreadsheets. The insider was terminated shortly after the incident and was not prosecuted.

CASE STUDY: ISOLATION

The insider was employed as a computer engineer by a ***trusted external entity (TEE)***, an information technology (IT) contracting company. This company managed computer systems for a foreign government, which became the victim organization. A month before the incident, the insider resigned from the TEE. In his resignation letter, he wrote that he felt “isolated and stressed due to his physical segregation from the rest of his team.” The insider also complained that 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; he then drank to excess and became intoxicated. Although no longer employed at the TEE, the insider lived with a former colleague who was still employed there. The insider used his roommate’s work computer and credentials to open a virtual private network (VPN) connection, crash multiple government servers, and delete 11,000 accounts of government employees at the victim organization. The insider was arrested, convicted, and sentenced to three years of imprisonment. The insider claimed he was trying to expose security vulnerabilities in the government’s IT systems. The impact related to this incident exceeded $1 million.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to 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 workforce members to think through projects, actions, and statements before committing to them.

☑ Create an environment that encourages workforce members to focus on one thing at a time, instead of multi-tasking.

☑ Provide stressed workforce members with ways to de-stress (e.g., massages, time off, games, or social activities).

☑ Routinely monitor the workloads of workforce members to ensure they are commensurate with the workforce member’s skills and available resources.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	CM-1 Policy and Procedures SC-4 Information in Shared System Resources
NIST CSF	ID BE
NIST Privacy Framework	PR.PO-P
NITTF Maturity Framework	ME-16
National Minimum Standards	G-2 G-4 I-1 I-2 I-3
CERT-RMM	Risk Management
ISO 27002	
CIS v7	
GDPR	

BEST PRACTICE 9

BEST PRACTICE 9

Incorporate Insider Threat Awareness Into Periodic Security Training for All Workforce Members

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	✓	✓	✓	✓	✓	✓	○

Without broad understanding by and buy-in from an organization's ***workforce***, technical and administrative controls will be short lived. To build a stable culture of security in an organization, it should conduct periodic security training that includes promoting the awareness of the many forms of ***insider risk***.

Protective Measures

The organization's entire workforce must understand that ***insider*** incidents do occur, and when they do, these incidents can have severe consequences. ***Workforce members*** must also understand that *insiders do not fit a single profile*. Analysis of actual incidents collected in the CERT Insider Threat Incident Repository reveals that insiders have a range of technical abilities (from minimal to advanced), across a range of ages (from late teens to retirement), across a range of positions (from low-wage earners to executives), and across the amount of time at the organization (new hires to seasoned company veterans).

No single profile exists that organizations can use to predict potential ***insider threat*** activity. *Demographic information cannot be used to identify a potential insider threat*. However, an organization can monitor and analyze workforce members behavior to identify potential indicators associated with higher insider risk. This behavior-based approach enables organizations to use evidence based on actual activity to identify opportunities to correct or support workforce members.

During security awareness training, the organization should provide resources to enable workforce members to identify evidence-based behavioral characteristics associated with high insider risk, such as the following:

- an individual who threatens the organization or brags about the damage that they could do to the organization or their co-workers
- an individual who downloads sensitive or proprietary data within 30 days of their resignation
- an individual using the organization's resources for a side business or discussing starting a competing business with their co-workers
- an individual attempting to gain their co-worker's passwords
- an individual attempting to gain access through trickery or exploitation of a trusted relationship (often called ***social engineering***)

During awareness training about recognizing negligent or reckless behavior, the organization should provide resources to identify the following characteristics:

- an individual having a high level of risk tolerance (i.e., someone willing to take more risks than the norm)
- an individual attempting to multi-task (Individuals who multi-task might be more likely to make mistakes.)
- an individual sharing large amounts of personal or proprietary information on social media
- an individual lacking attention to detail

The organization's entire workforce (including managers) should be trained to recognize the malicious use of social engineering tactics. Someone using these tactics engages others to join schemes that could cause harm to the organization, particularly to steal or modify information for financial gain. Informing workforce members about this manipulation and its consequences can make them more aware of it and 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 gains remote access to a system might need to use a co-worker's account to access a server containing sensitive information.

Cases in the CERT Insider Threat Incident Repository reveal that social engineering is sometimes a step toward acquiring unauthorized access or an attempt to obfuscate further illicit activities. The organization should train its workforce to be wary of unusual requests, including ones that do not concern accounts and passwords. These requests include social engineering by outsiders attempting to gain access to credentials.

The security training program should include the organization's entire workforce and strive to create a security culture that is appropriate for the organization. The training program should be offered at least once a year. In the United States (U.S.), September is National Insider Threat Awareness Month; that can be an excellent time to offer additional training and content geared toward insider threat awareness, such as access to conference talks, internal presentations about insider threats, or quizzes to test knowledge of insider threats in an interactive and engaging manner. Besides recognizing National Insider Threat Awareness month, organizations should define how often refresher training on insider risk should be conducted.

The following are insider risk topics that the organization should consider including in its training program:

1. **Human Resources.** Review insider risk policies and processes across the organization. Remind the workforce about the resources available to them, such as an Employee Assistance Program (EAP).
2. **Legal.** Review insider risk policies, summarize the issues that arose in the past year, and discuss how to avoid them in the future.
3. **Physical Security.** Review the policies and procedures that describe how workforce members and ***trusted external entities (TEEs)*** access the organization's facilities. Discuss the proper handling of physical ***assets***, including how to protect them during an evacuation or other emergency.
4. **Data Owners.** Discuss projects that might be more susceptible to insider risk (e.g., strategic research projects that involve new trade secrets). Demonstrate the value of ***intellectual property (IP)*** and the potential damage of an insider attack. When applicable, cover insider trading as well.
5. **Information Technology.** Educate the workforce about procedures for recognizing viruses and other malicious code. Discuss which devices are prohibited or permitted for authorized use on the organization's information systems. Conduct simulated phishing campaigns to test and educate the workforce about real phishing attacks.
6. **Software Engineering.** Review the importance of auditing configuration management logs to detect malicious code.

The organization should take measures to guard against insider threat. To increase the effectiveness and longevity of these measures, they 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 might view customer information as its most critical asset and focus its security measures on protecting that data.

Training about reducing risks to customer service processes should focus on the following:

- protecting computer accounts used in these processes (See **Best Practice 10**.)
- auditing access to customer records (See **Best Practice 12**.)
- consistently enforcing defined security policies and controls (See **Best Practice 3**.)
- implementing system administration safeguards for critical servers (See **Best Practices 11** and **12**.)
- using secure backup and recovery methods to ensure the availability of customer service data (See **Best Practice 18**.)

No matter which assets an organization focuses on, it should train its workforce to be vigilant against a broad range of insider threat actions, which are covered by several key best practices:

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

The organization should base its security training on documented policies and provide a confidential means of reporting security issues. Confidential reporting (1) enables workforce members to report suspicious events without fear of repercussion and (2) circumvents the cultural barrier against whistleblowing. The organization must ensure that the workforce understands that the organization applies established policies and procedures fairly, does not accept arbitrary and personal judgment, and expects managers to respond to security issues fairly and promptly.

The organization must notify workforce members that it monitors system activity, especially system administration and privileged activity. All workforce members should be trained to understand their individual security responsibilities, such as protecting their own passwords and work products. The training should clearly communicate information technology (IT) acceptable-use policies (AUPs) and acceptable workplace behavior. The organization should require each workforce member to complete a yearly acknowledgment of the AUP (or rules of behavior), which can be done at required training events.

The organization must teach each workforce member to be responsible for protecting the organization's information and critical assets. It should also regularly remind its workforce about procedures for anonymously reporting suspicious co-worker behavior and rebuffing recruitment attempts by individuals inside or outside the organization.

The organization must inform its workforce about the confidentiality and integrity of the organization's information (e.g., IP) and that compromises to that information will be dealt with harshly. This training can correct a common misconception that workforce members have about IP. For example, some believe that 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 organization's property.

In some insider threat cases, technical workforce members sold their organization's IP because they were dissatisfied with their pay, or they gave 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 data compromise. For this particular type of insider risk, using training to set expectations about salary and career enhancement can reduce disgruntlement by providing clarity.

The organization should consider implementing an information classification system that defines categories of information and how each category of information should be protected. For example, the U.S. Government uses a classification system that includes Unclassified, Confidential, Secret, and Top Secret information. It defines each of these categories and includes procedures for properly handling classified information. An organization can consider using a similar classification system that could include categories such as Company Public, Company Confidential, and so on. If an organization uses an information classification system, it must train its workforce to use it correctly.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Managing the training program**—It can be challenging for an organization to keep its workforce engaged after several iterations of training. It must determine how often to train individual workforce members and how to measure the effectiveness of the training. (Note that it can be difficult to discuss prior incidents without revealing sensitive information.)
2. **Classifying information**—Implementing an information classification program requires a lot of time and workforce buy-in. Workforce members must be trained to correctly classify and handle marked documents. Documents must be reviewed and marked appropriately, and additional access control protections must be incorporated.
3. **Improving the organization's culture**—If the organization has a culture that does not value IP or information security, workforce members might resist implementing the concepts presented in training. The organization can work through this challenge by getting buy-in from workforce members, focusing on the workforce protection aspect of the program. The organization can also help its workforce members learn by using case studies about past security incidents involving the organization; this approach can counter their beliefs that an attack could not occur at their organization.

CASE STUDY: GENEROUS CONSPIRACY

A tax office employed the insider as a manager. She had detailed knowledge of the organization's computer systems and helped design the organization's newly implemented computer system. She convinced management that her department's activities should be processed outside of this new system. All records for her 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. She had at least nine accomplices— insiders and outsiders—with unspecified roles in the scheme. One of her external accomplices, her niece, deposited checks into the bank accounts of 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 her motivations was that she enjoyed acting as a benefactor, giving co-workers money for things like private school tuition, funerals, and clothing.

She avoided suspicion by telling her co-workers that she had received a substantial family inheritance. The 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, she had $8 million in her bank account.

Had the organization provided training about suspicious activities that indicate insider activity, this incident might have been detected earlier. In this case, the insider made purchases that were out of reach for others in her position. In addition, she abused drugs and alcohol and had a gambling habit—indicators that her co-workers might have noticed. With proper training, a workforce member might have recognized the combination of these risk factors and reported the activities, and the organization would have investigated and identified the crime.

CASE STUDY: KEYSTROKE CAPTURE

A disgruntled employee placed a hardware keystroke logger on a computer at work to capture confidential company information. After the organization fired him unexpectedly, he tried to coerce a non-technical employee still at the company into recovering the device for him. Although the coerced employee did not know the device was a keystroke logger, she recognized the risk of providing it to him and notified management instead. Forensics revealed that the insider removed the device and transferred the keystrokes file to his computer at work at least once before being fired.

In this case, the coerced non-technical employee was wary (correctly) of an unusual request about network systems and accounts, including physical access, so she reported the activities, and the keystroke logger was detected. This case is a great example of the benefits an organization can realize when it trains its workforce members to recognize and be cautious of social engineering.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Develop and implement an enterprise-wide training program that discusses various topics related to insider risk. To be effective, senior management must support the training program and actively participate in it. Management must not be exempt from taking the training; otherwise, other workforce members could perceive exemptions as a lack of support and an indicator of unequal enforcement of policies.

☑ Require all new workforce members to complete security awareness training, including insider threat training, before giving them access to any organizational computer system. Make sure to include training for workforce members who may not need to access computer systems daily, such as janitorial and maintenance staff. These workforce members may require a special training program that covers security scenarios they may encounter, such as social engineering, an active shooter, and sensitive documents left out in the open.

☑ Require annual training and conduct periodic awareness campaigns (e.g., quizzes, posters, newsletters, alert email messages, and brown-bag lunch programs).

☑ Establish an anonymous and/or confidential mechanism for workforce members to report security incidents, and encourage them to use it. Consider providing incentives by rewarding those who use the system.

Large Organizations

The recommendation in this subsection applies to large organizations.

☑ Have the information security team conduct periodic inspections by walking through areas of the organization, including workspaces, and identifying security concerns. If security issues are discovered, bring them to the workforce member's attention privately and in a calm, nonthreatening manner. Workforce members spotted doing something good for security, like stopping a person without a badge, should be rewarded. Awarding a certificate or other item of minimal value can improve workforce morale and increase security awareness.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AT-1 Policy and Procedures AT-2 Literacy Training and Awareness AT-3 Role-Based Training
NIST CSF	PR AT
NIST Privacy Framework	GV.AT-P CM.PO-P CM.AW-P
NITTF Maturity Framework	ME-7
National Minimum Standards	I-1 I-2 I-3
CERT-RMM	Organizational Training and Awareness
ISO 27002	8.2.2 Information security awareness, education and training
CIS v7	Control 17
GDPR	

BEST PRACTICE 10

BEST PRACTICE 10

Implement Strict Password and Account Management Policies and Practices

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	✓	✓	○	✓	✓	✓	○

Organizations should use strict password and account management policies and practices to prevent ***insiders*** from compromising user accounts to circumvent manual and automated control mechanisms.

Protective Measures

No matter how vigilant an organization is against ***insider risk***, if the organization's user accounts can be compromised, insiders have the potential to circumvent attack prevention mechanisms. Establishing user account and password management policies and practices is critical to impeding an insider's potential to use the organization's systems for illicit purposes. Combining fine-grained access control with proper computer account management ensures that access to all of the organization's critical electronic ***assets*** is attributed to individual ***workforce members***.

The following are just some of the methods that insiders use to compromise accounts:

- obtain passwords through ***social engineering*** or because workforce members openly shared them
- obtain passwords stored by workforce members in clear-text files on their computer or in email messages
- obtain passwords left on sticky notes or paper left in plain sight, or easily accessible places (e.g., under the keyboard, phone, or mouse pad; in an address book)
- use an unattended computer where the user is still logged in
- use password crackers
- use keystroke loggers
- watch while a user types in their password, also known as "shoulder surfing"

Password policies and procedures should ensure that (1) all computers automatically execute password-protected screen savers after a fixed period of inactivity and (2) workforce members use the following good habits:

- Ensure all passwords are strong.[30]
- Do not share passwords with anyone.
- Lock the workstation before stepping away from it.
- Block visual access to screens when typing passwords.

[30] See the National Institute of Standards and Technology (NIST) *Special Publication 800-63B, Digital Identity Guidelines* (**https://pages.nist.gov/800-63-3/sp800-63b.html**) [NIST 2021a].

An organization should use shared accounts only when absolutely necessary. Often, an organization uses these accounts out of administrative convenience rather than necessity. Using shared accounts inhibits traceability and individual activity attribution, which is required in some regulations and is critically important for investigations. To alleviate this issue when shared accounts are necessary, the organization should consider using shared account password management (SAPM) tools that automate processes and enforce controls for the remaining shared accounts. When combined, these steps reduce the likelihood of an insider executing an attack in a non-attributable way. In addition, workforce members should report all attempts or suspected attempts of unauthorized account access to the organization's help desk or information security team.

The cases in the CERT Insider Threat Incident Repository reveal that some insiders create ***backdoor*** accounts that provide them with system administrator or privileged access following their termination. Other insiders can use their accounts after they leave the organization because the accounts were not revoked. Yet other insiders use other types of shared accounts, including those set up for access by external entities such as contractors and vendors. Insiders also used training accounts that the organization used repeatedly without changing the password.

Systems used by non-workforce members should be isolated from other organizational systems, and accounts should not be replicated across these systems. In addition, the organization should carefully consider the risks of issuing guest accounts to visitors.

Periodic account audits combined with technical controls allow the organization to identify the following suspicious accounts:

- backdoor accounts
- shared accounts
- accounts created for external entities
- infrequently used accounts (particularly if administrators perform excess password resets on them)

Account management policies that include strict documentation of all access privileges for all users enable a straightforward termination procedure that reduces the risk that former workforce members will attack. The organization 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 and investigators to trace all online activity on those accounts to an individual user.

These limits, procedures, and controls weaken an insider's potential to engage in illicit activity without being monitored and identified. An organization using centralized account management systems, such as Lightweight Directory Access Protocol (LDAP) directory services, for authentication can reduce the risk of overlooking an account during termination or during a periodic audit.

The organization's password and account management policies must also apply to all ***trusted external entities (TEEs)*** 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. TEEs should not be granted shared accounts for access to organizational information systems. A TEE must not share passwords, and when a TEE principle offboards an agent, 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.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Balancing risk and business processes**—Finer grained access controls, account management, and other account security measures can incur tradeoffs and costs associated with business inefficiencies.
2. **Managing accounts**—An organization with a large number of distributed user workstations can find it challenging to manage local accounts.

CASE STUDY: UNAUTHORIZED ACCESS

The insider, a contractor, was formerly employed as a software developer and tester by the victim organization. The organization terminated him for poor performance but failed to change a shared account password upon his departure. After termination, he used a shared account to remotely access 24 of the victim organization's user accounts. He 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 username was used to log into her computer just a few hours earlier when, in fact, she had not logged in, 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. He made several claims, including that he logged in only to check on a program he wrote; that he was not fired from the victim organization, but rather that his contract had not been renewed; that a former co-worker asked him to log in to help with a problem; and that he was 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 having to pay unspecified fines and penalties. He exploited 13 systems that stored trade secrets valued at approximately $1.3 million.

Many other cases in the CERT Insider Threat Incident Repository involve insiders who log into systems using shared passwords that were not changed when the insider was terminated. Organizations should have proper account management practices and identify all shared accounts. Whenever an individual departs an organization, the organization should use this record to identify the accounts the individual could have access to and change the passwords on these accounts.

CASE STUDY: PROJECT REVENGE

An e-commerce company employed a chief project engineer, the insider. The organization removed her from a major project and subsequently terminated her employment. Afterward, her accomplice, an employee of the victim organization, allegedly gave her the password to the server storing the project he had worked on.

According to some sources, she wanted to delete the project file for revenge. Other sources claim that she wanted to hide the file during a presentation so that her accomplice could recover the file, appear to be a hero, and avoid being fired. She 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 her accomplice were arrested. The insider was found not guilty.

CASE STUDY: SHARING ISN'T CARING

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, such a policy might have deterred the activities of the insider and his accomplice.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to 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. The policy should also 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 require that users request new accounts via a help desk ticket. (Members of the help desk should not be able to create accounts.) 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 to create strong passwords. Some systems can tolerate long passwords. Encourage users to use passwords that include proper punctuation and capitalization, thereby increasing password strength and making it more memorable to the user.
- ☑ Security training should include instruction about how workforce members can block visual access to others as they type their passwords.
- ☑ Ensure all shared accounts are absolutely necessary and are addressed in a risk management decision.

Large Organizations

The recommendations in this subsection apply to large organizations.

- ☑ Use a centrally governed solution for identity and access management (IAM) of workforce member accounts.
- ☑ If your organization is using a central account management system, add contractors to groups linked to projects, organizations, or other logical groups. This approach allows administrators to quickly identify contractors and change access permissions. Accounts themselves can contain contractor status tipoffs (e.g., adding "CONT" to the account name or description).

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AC-2 Account Management IA-2 Identification and Authentication
NIST CSF	PR AC
NIST Privacy Framework	CT.PO-P CT.DM-P PR.DS-P PR.PT-P
NITTF Maturity Framework	
National Minimum Standards	
CERT-RMM	Identity/Access Management
ISO 27002	11.2.3 User password management 11.2.4 Review of user access rights
CIS v7	Control 16
GDPR	Article 32 Security of processing

BEST PRACTICE 11

BEST PRACTICE 11

Institute Stringent Access Controls and Monitoring Policies on Privileged Users

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	✓	✓	○	✓	✓	○	✓

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

Protective Measures

According to CERT researchers at Carnegie Mellon University's (CMU's) Software Engineering Institute (SEI), a majority of the ***insiders*** who committed sabotage and more than half of those who stole confidential or proprietary information held technical positions at victim organizations. Technically sophisticated methods of carrying out and concealing malicious activity have included the following:

- 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 in the SEI report *An Analysis of Technical Observations in Insider Theft of Intellectual Property,* only 6 cases contained clear information about the insider's concealment methods [Hanley 2011a]. Using stringent access controls and monitoring policies that focus 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[31] have greater access to systems, networks, and/or applications than other users. Privileged users pose an increased risk because they have the following characteristics:

- They have the technical ability and access to perform actions that ordinary users cannot.
- They can usually conceal their actions by using their privileged access to log in as other users, modify system log files, and falsify audit logs and monitoring reports.
- They typically have oversight of and approval responsibility for change requests to applications or systems, even when their organization enforces technical separation of duties. (See **Best Practice 15**.)

[31] In 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.

The organization can configure systems and networks to facilitate ***non-repudiation*** by using certain policies, practices, and technologies. If ***malicious insider*** activity occurs, non-repudiation techniques allow each online activity to be attributed to a single ***workforce member***, no matter their 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 creating ways to circumvent non-repudiation 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.

The organization should consider having privileged users sign a privileged user agreement or rules of behavior that outline what is required of them, including what they are and are not permitted to do with accounts they can access. These types of agreements help instill the responsibilities of elevated access in privileged users. Monitoring technologies and policies must be lawful, and the organization should consult legal counsel before implementing them.

User activity monitoring (UAM) tools have advanced significantly since the last publication of the *Common Sense Guide,* and organizations must learn about and fully understand the limitations of these tools. The practices discussed above help the organization identify users after suspicious activity is detected; however, the organization must take additional steps to prevent malicious actions from occurring in the first place.

For example, 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 the organization's information and refuse to provide the key. The organization should evaluate encryption solutions and how they can impact UAM 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 be required to peer review their 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. A small organization that cannot afford to employ more than one system administrator must recognize its increased risk. Several case studies in this guide describe an organization victimized by its sole system administrator.

An organization that can afford only one system administrator can use some methods to separate the auditing role from the single administrator. For example, an organization can make log information available to non-technical managers, independent audit reviewers, or investigators. To achieve effective separation of duties, any method used must assure that the system administrator has no control over the auditing function. For more information about separation of duties, see **Best Practice 15**.

Many of the insiders documented in the CERT Insider Threat Incident Repository, especially those who engaged in information technology (IT) sabotage, were former workforce members of the victim organizations. The organization must be especially careful to disable system access to former system administrators and technical or privileged users. Thoroughly documented procedures for disabling access can help ensure that the organization does not overlook stray access points.

In addition, the organization should consider implementing the ***two-person rule***, which requires two people to participate in a task for it to be executed successfully, for the critical functions performed by these users and reduce the risk of extortion after they leave the organization. (See **Best Practice 15**.)

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Justifying payroll costs**—It can be difficult for the organization to justify the cost of the additional workforce members 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 that the organization trusts them.

CASE STUDY: A BOMB PRESCRIPTION

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 email messages discussing the anticipated layoffs of the victim organization's computer systems administrators. The insider, fearing she 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 her employment, she did not remove the logic bomb. When the logic bomb failed to detonate on the intended day, she 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.

CASE STUDY: COMPUTER INTRUSION

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 that they rehire his partner. 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 him, the IT company refused to help him with an unemployment compensation claim. Using the backdoor account he previously created, he accessed one of the organization's servers several times, sometimes using his home network and sometimes using public networks.

He deleted the data of two customers and made it difficult for one of the customers to access the company's server. The IT company contacted a government agency to help with its investigation, which identified him by the user account and logs. He was arrested and pled guilty to computer intrusion.

In both of these case studies, the insiders were able to make changes to the system without verification. In the first case, the insider planted a logic bomb on 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 might have been detected earlier or even stopped.

CASE STUDY: BAD TRADE

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 a backdoor that enabled him to hide trading losses, without detection, totaling nearly $700 million over several years.

The types of controls discussed in this best practice would have been effective in preventing this investment trader from manipulating source code.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Conduct periodic account reviews to avoid privilege creep. Workforce members should have sufficient access rights to perform their everyday duties. When a workforce member changes their role, the organization should review their account and rescind permissions that they no longer need.

Large Organizations

The recommendations in this subsection apply to large organizations.

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

☑ Use ***multifactor authentication (MFA)*** for privileged user or system administrator accounts.[32] Requiring MFA reduces the risk of a user abusing privileged access after an administrator leaves the organization, and the increased accountability of MFA can inhibit some currently employed privileged users from committing acts of malfeasance. Assuming that the former workforce member's MFA mechanisms have been recovered, the account(s) will be unusable.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AC-2 Account Management AC-6 Least Privilege AU-2 Event Logging AU-6 Audit Record Review, Analysis, and Reporting AU-9 Protection of Audit Information CM-5 Access Restrictions for Change IA-2 Identification and Authentication (Organizational Users) MA-5 Maintenance Personnel
NIST CSF	PR AC
NIST Privacy Framework	CT.PO-P CT.DM-P PR.DS-P PR.PT-P
NITTF Maturity Framework	
National Minimum Standards	H-1 H-2 H-3 H-4
CERT-RMM	Identity/Access Management Monitoring
ISO 27002	10.10.2 Monitoring System Use 10.10.4 Administrator and Operator Logs
CIS v7	Control 16
GDPR	Article 32 Security of processing

[32] NIST Special Publication 800-53, AC-6 (Access Control) requires MFA for moderate-to-high-risk systems [NIST 2015a].

BEST PRACTICE 12

BEST PRACTICE 12

Deploy Solutions for Monitoring Workforce Member Actions and Correlating Information from Multiple Data Sources

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	✓	✓	✓	✓	✓	✓	○

An effective ***insider risk management program (IRMP)*** collects and analyzes information from many different sources across the organization. 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 risk*** analysis increases, so too does the organization's ability to produce 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 that indicate potential insider activity. Monitoring ***workforce*** actions should be implemented with solutions that use a risk-based approach and focus first on the organization's ***critical assets***.

Protective Measures

The cyber activity of ***workforce members*** 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 online workforce activity. The volume of information necessary for network-based monitoring is often much less than what is required for collecting host-based logs and other information from every system on the network.

Insider-risk-related activity that is inferable through network analysis can include authentication, access to sensitive files, unauthorized software installations, web browsing activity, email/chat messaging, printing, and many others. However, there are some actions the organization might need to monitor that do not leave any trace on the network. These actions can include copying local files to removable media, attempting to escalate local privileges, and many others. These actions can be monitored using host-based log collection and host-based monitoring systems.

For incident detection to be most effective, the organization must be able to correlate data from multiple sources, whether those sources are network and host based or are from multiple hosts. One of the most powerful tools an organization can use to perform event correlation is security information and event management (SIEM). SIEM is designed to provide a centralized view of a wide array of logs from sources that include databases, applications, networks, and servers. SIEM enables the organization to write queries or generate alerts that pull together data from previously disparate data sources. This ability enhances potential analytic capabilities for ***insider threat*** prevention, detection, and response.

SIEM enables the organization to continuously monitor its workforce members' actions. This monitoring further allows the organization to establish a baseline of normal activity and detect irregular events. An organization can use a SIEM solution to conduct more granular monitoring of privileged accounts. SIEM should be able to highlight events related to any actions a normal user cannot perform, such as installing software or disabling security software. SIEM facilitates sorting through these events by highlighting those that need further review and discarding background noise. Increasing the auditing level for certain events creates additional audit records that must be reviewed.

SIEM can also enable the organization to conduct ***enhanced monitoring***. A SIEM solution with a robust set of data enables an analyst to conduct relevant retrospective analysis of data even when an alert was not generated. This analysis is especially important for monitoring the activity of workforce members who are leaving the organization, or who have violated or are suspected of violating organizational policy.

Based on the work of Software Engineering Institute (SEI) CERT researchers and feedback from industry, malicious insiders often conduct illicit activities within 90 days of their termination. When a workforce member submits their resignation, the Human Resources (HR) team should notify the IRMP, which should then notify the information assurance (IA) team so that its workforce can review the workforce member's actions (1) over at least the past 90 days and (2) going forward to detect potential insider activity. HR should also alert IA if a workforce member is reprimanded or counseled for violating a work policy.

Communication between HR and IA should take place between representatives from each division working in the IRMP. The IRMP provides a way to quickly and seamlessly respond to insider incidents by including representation from all key stakeholders within an organization.

SIEM is not limited to information security events. Other information, such as physical security events and ***threat*** intelligence, can also be sent to a SIEM solution to allow for more comprehensive detection and contextualization of the insider activity of interest. For example, if an organization sends workforce badge access records to a SIEM solution, it would be possible to detect unauthorized account usage by checking to see if a workforce member who is logged into a workstation locally is physically present in the facility.

This same method can also be used to detect unauthorized remote access if a workforce member is physically in the facility. It is also possible to detect after-hours physical access and correlate it with ***digital access logs***. Typically, many alerts, triggers, and indicators are 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 risk depends on knowing what data to collect. There are numerous data sources, found in many organizations, that are recommended for incorporating into an insider risk analytic capability. Table 4 provides a list of these data sources, a brief description of each, and the types of analysis that each data source supports.

Table 4: **Description of Data Sources for Insider Risk Analysis**

DATA SOURCE NAME	DESCRIPTION
Technical Data Sources	
Account Creation Logs	Account creation logs can be correlated with information from HR 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 identifying multiple accounts that are associated with the same user.

DATA SOURCE NAME	DESCRIPTION
Antivirus Logs	Host-based antivirus logs 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 about user activity, and invalid login attempts can point to users attempting to (1) access information that is out of scope for their job roles and (2) masquerade as another user.
Chat Logs	Analyzing communication between co-workers can help identify potentially malicious activity and provide insight into workforce members' concerning personality traits.
Configuration Change Logs	Logs of changes to network devices and other resources can be analyzed and correlated with other data sources to identify unauthorized configuration changes.
Data Loss Prevention Logs	Data loss prevention (DLP) systems can identify when critical information traverses the network.
Domain Name System Logs	The domain name system (DNS) can be used to efficiently analyze what services and websites workforce members 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 workforce members' concerning personality traits.
File Access Logs	File access logs 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 workforce members 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 Detection/Prevention System Logs	***Intrusion detection system (IDS)*** and ***intrusion prevention system (IPS)*** logs can detect malicious insider activity since many of the technical actions are the same as the external actions these systems are designed to detect.
Mobile Device Manager Logs	Mobile device manager logs can be used to identify users attempting to circumvent ***security controls*** and use 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 indicate an insider is attempting to access information or resources outside of their need to know.
Printer/Scanner/Copier/Fax Logs	These common exfiltration 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.

DATA SOURCE NAME	DESCRIPTION
Removable Media Manager Logs	Removable media is a common exfiltration method, and logs should be monitored for detecting when sensitive information is copied and policy is violated.
Telephone Logs	Telephone logs can be used to identify suspicious communication with foreign parties or competitors.
User Activity Monitoring Logs	Alerts from user activity monitoring (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.
Virtual Private Network Logs	Virtual private network (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.
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 regularly monitoring the wireless spectrum.
Non-Technical Data Sources	
Anonymous Reporting	Leads from anonymous reporting should be followed because they are a useful way to identify potentially malicious insiders based on observed suspicious behavior.
Acceptable Use Policy Violation Records	Violations of acceptable use policies (AUPs) could be part of identifying malicious activity or identifying rule breakers who might be more likely to commit malicious actions.
Asset Management Logs	Movement of critical assets should be reviewed and analyzed for suspicious activity.
Background Checks	A background check can provide useful context about a workforce member to help the IRMP 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	Corporate credit card records are useful in detecting anomalies and resolving allegations. This data can also reveal unreported or unauthorized travel.
Disciplinary Records	Disciplinary records can help the IRMP identify problem workforce members 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.
Intellectual Property Policy Violation Records	Violations of ***intellectual property (IP)*** policies could be part of malicious activity or point to rule breakers who might be more likely to commit malicious actions.
Performance Evaluations	Performance evaluations can provide useful context about a workforce member to help the IRMP gain a “whole-person” perspective. This data source can also be used to identify significant changes in workforce member performance.
Personnel Records	Personnel records provide information that includes a workforce member’s job titles, supervisors, promotions, and discipline history.
Physical Access Records	Physical access records 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 might be more likely to commit malicious actions.

DATA SOURCE NAME	DESCRIPTION
Security Clearance Records	Security clearance records can provide useful context about a workforce member to help the IRMP gain a "whole-person" perspective.
Travel Reporting	Travel reporting information can be correlated with other data sources to identify anomalous or suspicious behavior.

The data sources listed in Table 4 are not comprehensive enough to completely prevent or detect all insider threats in all organizations. Some organizations might not collect all the listed data, and some organizations have different data sources available that provide additional information about workforce members and critical assets.

Incorporating all the listed data sources into an analytic capability is a significant technical challenge. SIEM solutions make federation easier, and these tools are increasingly providing advanced analytic capabilities. However, subscription and licensing models can make the desired scope of the solutions financially prohibitive.

With limited resources, the organization must know its critical assets, understand what types of actions those critical assets are susceptible to, and prioritize incorporating data sources based on each source's applicability to the analysis that predicts or detects those actions. (See **Best Practice 1**.) Figure 13 provides a consolidated view of the recommended data sources to be included in an analytic capability for insider threat detection, prevention, and response.

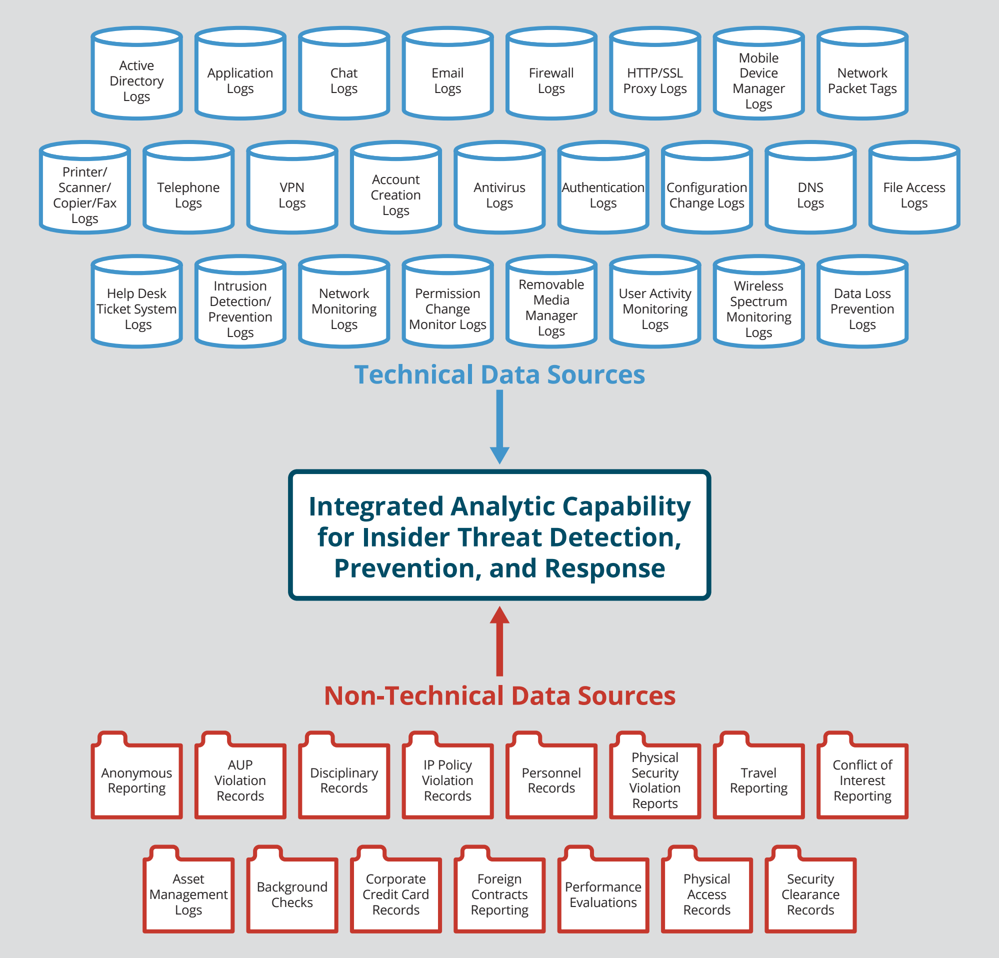

Active Directory Logs
Application Logs
Chat Logs
Email Logs
Firewall Logs
HTTP/SSL Proxy Logs
Mobile Device Manager Logs
Network Packet Tags
Printer/ Scanner/ Copier/Fax Logs
Telephone Logs
VPN Logs
Account Creation Logs
Antivirus Logs
Authentication Logs
Configuration Change Logs
DNS Logs
File Access Logs
Help Desk Ticket System Logs
Intrusion Detection/ Prevention Logs
Network Monitoring Logs
Permission Change Monitor Logs
Removable Media Manager Logs
User Activity Monitoring Logs
Wireless Spectrum Monitoring Logs
Data Loss Prevention Logs
Technical Data Sources
Integrated Analytic Capability for Insider Threat Detection, Prevention, and Response
Non-Technical Data Sources
Anonymous Reporting
AUP Violation Records
Disciplinary Records
IP Policy Violation Records
Personnel Records
Physical Security Violation Reports
Travel Reporting
Conflict of Interest Reporting
Asset Management Logs
Background Checks
Corporate Credit Card Records
Foreign Contracts Reporting
Performance Evaluations
Physical Access Records
Security Clearance Records

Figure 13: An Integrated Analytic Capability for Insider Threat Detection, Prevention, and Response

The organization should create monitoring policies and procedures before institutionalizing a monitoring program. The organization should inform its workforce members that their use of any information system is monitored. Workforce members are typically informed through logon banners, security awareness training provided to them before using a system, and annual refresher training. The organization should consult legal counsel before implementing a monitoring program to ensure the program meets all legal requirements and disclosures, including those related to securely storing and processing workforce member data.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Dealing with false positives**—The organization should tune its alerting systems to reduce the number of false positives. For alerts generated by SIEM, tune both the alerting rules and the systems that send the data that the rules evaluate.
2. **Establishing a baseline**—The organization should understand expected workforce member behavior and where anomalies in behavior can indicate risk. Baselines must exist at multiple levels for different use cases (e.g., individual, role, department, organization).
3. **Accessing information**—Various departments from across the organization must work together to determine what information will be collected, which information will be federated in the SIEM solution, and who has permission to review the alerts.
4. **Contextualizing and understanding risks**—The organization must ensure that sufficient information for understanding the motive for and impact of an event can be obtained by analysts/investigators. Where feasible, this information should be incorporated into evaluations and prioritizations before alerts are sent to analysts.
5. **Instrumenting for physical risks**—The organization should understand that the technical and ***non-technical observables*** captured through its SIEM solution can indicate not only cyber-technical insider risks but also kinetic ones. The organization might decide to incorporate physical security or risk assessment personnel into its IRMP to provide the necessary expertise to discern potential kinetic or workplace violence threats.

CASE STUDY: DAMAGING HELP

A help desk technician at a large telecommunications firm installed hacking tools on his company-assigned computer, stole other employees' credentials, and passed those credentials to an external conspirator who used them to gain unauthorized access to the company's website, which he defaced. This incident 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 on his system, demoted him, and imposed policy restrictions that forbade him from accessing the Internet from his office. However, the company did not fully implement these restrictions and he was able to use an expired customer account to access the Internet and his email. He 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 solution. Access logs eventually connected the insider and outsider to the incident.

CASE STUDY: AN UGLY PICTURE

An insider disabled the antivirus application in her organization's system, installed malware, used that malware to gain unauthorized access to her supervisor's system, and planted a ***logic bomb*** on a critical server.

If the organization had implemented proper auditing and used an internal IDS/IPS system in this case study, various security events that the insider caused would have triggered the following alerts: disabling the antivirus application, anomalous malware traffic passing through an IDS sensor, and system changes resulting from installing a ***logic bomb***.

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 SIEM would have been able to generate a high-priority alert that would have demanded immediate attention.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Implement rules within the SIEM solution to automate alerts.

☑ Create a log management policies and procedures. Ensure they address log retention (consult legal counsel for specific requirements), what logs to collect, and who manages the logging systems.

Large Organizations

The recommendation in this subsection applies to large organizations.

☑ Ensure that someone working in an insider risk capacity regularly monitors the SIEM solution to (1) look for trends in alerts and activities and (2) hunt for critical incidents that might not make it into the highest priority alerts. Depending on the environment, this work can involve multiple personnel who monitor workforce member activity full time.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AU-1 Policy and Procedures AU-2 Event Logging AU-6 Audit Record Review, Analysis, and Reporting AU-7 Audit Record Reduction and Report Generation AU-8 Time Stamps AU-12 Audit Record Generation
NIST CSF	PR PT DE AE DE CM DE DP
NIST Privacy Framework	CT.PO-P CT.DM-P PR.DS-P PR.PT-P
NITTF Maturity Framework	ME-8 ME-10 ME-11 ME-12 ME-14 ME-16
National Minimum Standards	H-1 H-2 H-3 H-4
CERT-RMM	Monitoring
ISO 27002	10.10.2 Monitoring System Use 10.10.4 Administrator and Operator Logs
CIS v7	Control 4
GDPR	Article 88 Processing in the context of employment

BEST PRACTICE 13

BEST PRACTICE 13

Monitor and Control Remote Access from All End Points, Including Mobile Devices

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
○	○	○	○	✓	✓	✓	○

Remote access to critical organizational ***assets*** must be closely guarded and protected. As organizations shift to operate with a fully remote, mostly remote, or hybrid (mixed remote and in-person) presence, proactive risk analysis should identify what information sources are available to monitor remote activity and what level of remote access is necessary for ***workforce members*** to carry out their duties.

Protective Measures

According to the analysis of cases in the CERT Insider Threat Incident Repository, ***insiders*** often attack organizations remotely, either while working for the organization or after termination, using legitimate access that the organization provides. While remote access can greatly enhance workforce productivity, and there is an anticipated shift to more permanent virtual operations post-COVID 19, remote access to critical data, processes, or information systems must be provided with caution. Insiders have admitted that it is easier to conduct malicious activities from home because it eliminates their concern about a co-worker physically observing their malicious acts.

To mitigate ***threats*** from ***remote workforce members***, the organization must identify the following:

- What organizational services (e.g., signing into Microsoft Teams) can be accessed remotely?
- For each service that can be accessed remotely, what visibility is available that the organization can use to monitor user activity?
- For each service that can be accessed remotely, what detective and preventive controls are available that the organization can use to restrict or stop activity?
- For each service that can be accessed remotely, what responsive controls are available that the organization can use to contain and handle an incident?

Access to data or functions that could inflict major damage to the organization should be protected with enhanced controls and monitoring. An organization that is unable to furnish organization-owned equipment to its remote workforce members should consider restricting access to its systems by using a proxy or virtual private network (VPN). These technologies act as a “launching pad” into the organization’s network, often through a secured terminal service or remote desktop session.

Smartphones and other mobile devices now put many of the same functions of a desktop computer in the palm of your hand. Whether the organization or the workforce member owns the device, the organization should be aware of the capabilities these devices have and how they are used in the enterprise. The organization should include mobile devices in its risk assessment and consider some specific features:

- cameras
- microphones
- remote access
- applications
- wireless capabilities (e.g., Wi-Fi, Bluetooth, cellular, WiMAX)
- mass storage capabilities

Mobile devices can be used to exfiltrate data. The cameras and microphones on phones can be used to capture the organization's sensitive information (e.g., architectural drawings, trade secrets, confidential discussions). Pictures can be stored on a phone or immediately sent from the device via email or text messages. These devices can also synchronize their data immediately to cloud storage, social media services, or personal computers outside the administrative control of the organization.[33]

Mobile devices also allow users to remotely manage organizational assets with applications that enable the remote management of servers, workstations, and network infrastructure devices. Some applications enable remote access to the workforce member's desktop. Before allowing this type of access, the organization should identify a justifiable business need, establish usage policies and procedures, and carefully monitor their use by the organization's workforce.[34]

The organization should also perform a ***Privacy Impact Assessment (PIA)*** or ***Data Protection Impact Assessment (DPIA)*** on mobile device management (MDM) services and/or products under consideration with input from legal counsel. Whenever possible, the organization should opt for the service that best balances the security needs of the organization with the privacy needs of the workforce. For organizations under GDPR compliance, Working Party 29 advises that, "Employees whose devices are enrolled in MDM services must also be fully informed as to what tracking is taking place, and what consequences this has for them" [Working Party 2002]. After being informed about the impact of MDM services, particularly when using a personal device, workforce members can seek to use approved devices owned by the organization, which resolves the information security concerns of the organization.

The organization should be aware of who has these types of applications installed on their mobile devices, and who can access the device and its associated services. When a workforce member leaves the organization, the organization must disable the workforce member's access to these applications. If the organization's data is on a workforce member's phone (e.g., email messages), the organization should establish an agreement to require workforce members to give the organization the ability and permission to remotely erase the device if it is lost or stolen, or if the workforce member is terminated.

The organization must also carefully weigh the risks of allowing personally owned devices to connect to the enterprise network. If the organization allows workforce members to only use equipment owned by the organization, it can then control how the device is used and managed,

[33] Data spillage and incident response become more challenging when the data is spilled using a phone because of the multitude of possible synchronized storage locations; this topic is beyond the scope of this guide.

[34] Remember that legal counsel should review any monitoring policies before a monitoring program is implemented.

often through an MDM server. The organization must be aware of the applications installed on these devices and how they can introduce vulnerabilities into the organization. Hurlburt, Voas, and Miller explored this issue in a 2011 article [Hurlburt 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 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. The organization should investigate enterprise-controlled "app stores" or other commercially available mobile device configuration management technologies that offer the organization the ability to control device configurations, including applications that are approved for installation.

Some smartphones can tether (i.e., use the cellphone network to access the Internet) or allow VPN access to the organization's network via a laptop or other device. Tethering can be implemented as either a Universal Serial Bus (USB) connection from the smartphone to a computer, or by broadcasting a Wi-Fi network that is accessible to any other devices with Wi-Fi capabilities. These functions allow telecommuters to access information on the go; however, they are entry points into the corporate network that must be monitored and controlled.

If users can use tethering to bridge their trusted, corporate connection or devices with an untrusted, tethered connection, then they can completely bypass all enterprise network security by directing their illicit activity through the unmonitored connection. Furthermore, these devices can create ***backdoors*** into the system by introducing an unknown network connection to a computer. Insiders can take otherwise air-gapped computers online via tethering. In one case, an insider left a rogue modem attached to the organization's equipment to allow them to dial in and perform administrative tasks. Using current technology, a tethered smartphone could conceivably be used to accomplish the same objective.

Insiders can use mobile devices, including smartphones and tablets, to exfiltrate video or photographs of data using an Internet service provider (ISP) connection that is not owned by the organization (e.g., a public cellular network). Technology such as ***intrusion detection systems (IDSs)*** and ***intrusion prevention systems (IPSs)*** (also known as intrusion detection and prevention systems [IDPS]), firewalls, and network logs cannot detect this type of exfiltration because these networks are not connected to the organization's information technology (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, the organization must treat mobile devices with mass storage as removable media and establish appropriate protections to mitigate any risks associated with them. (See **Best Practice 19.**)

When an organization determines 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 organization-owned devices enhances the organization's ability to control access to its information and networks as well as monitor the activity of its remote workforce members.

For all remote logins, the organization should log information such as account logins, date and time connected and disconnected, and Internet protocol (IP) address. It is also useful to monitor failed remote logins, including the reason the login failed. The organization can make this monitoring more manageable and effective by minimizing authorization for remote access to critical data.

Disabling remote access is an often-overlooked but critical part of the workforce member termination process. Workforce member termination procedures must include the following:

- Retrieve any of the workforce member's equipment owned by the organization.
- Disable the workforce member's remote access accounts (e.g., VPN and dial-in accounts).
- Disable the workforce member's firewall access.
- Disable all of the workforce member's remote management capabilities.
- Change the workforce member's passwords for all of their shared accounts (e.g., system administrator, database administrator [DBA], privileged shared accounts).
- Close all of the workforce member's open connections.
- If previously agreed to, remotely erase all devices associated with the workforce member if they contain organizational information.

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

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Managing remote devices**—The demand for organizations to permit the use of personally owned devices is growing, and the associated management and privacy issues can be challenging.
2. **Demonstrating a return on investment**—The organization might have difficulty prohibiting personally owned devices and should conduct a risk-benefit analysis that supports its decision.

CASE STUDY: SNEAKY PHOTOGRAPHERS

Two engineers worked for an international tire manufacturing company that supplied equipment to other manufacturers. The two insiders were contracted by an overseas company to design a particular piece of equipment. They 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 to them. The victim organization's plant restricted access to parts of its facility behind several secure doors, and it 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 acted as 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.

This type of attack poses a challenge for many organizations. Organizations' security policies and workforce members 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 followed the policy.

Areas that contain sensitive trade secrets must 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 that area. In addition, NDAs and other legal documents should be verified long before a visitor arrives on company property. Organizations should require workforce members to regularly reaffirm their agreement. 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 might not have occurred.

CASE STUDY: UNCHARITABLE PHOTOS

In this not-yet-adjudicated case, a worker at a charity allegedly took many photos of donors' check and credit card data with her smartphone. She then sent the photos off-site using her smartphone. That charity's donors were alleged victims of fraud related to that exfiltrated data.

Regardless of whether this insider is found guilty, it is clear that modern mobile devices can exfiltrate personally identifiable information (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.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Disable remote access to the organization's systems when an employee or contractor separates from the organization. Disable access to the organization's VPN service, application servers, email, network infrastructure devices, and remote management software. Close all open sessions. Collect all organization-owned equipment, including ***multifactor authentication (MFA)*** tokens, such as RSA SecurID tokens or smart cards.

☑ Include mobile devices, with a list of their features, in enterprise risk assessments.

☑ Prohibit or limit the use of personally owned devices.

☑ Prohibit devices with cameras in sensitive areas.

Large Organizations

The recommendations in this subsection apply to large organizations.

☑ Implement a central management system for mobile devices.

☑ Monitor and control remote access to the organization's infrastructure. VPN tunnels should terminate at the furthest perimeter device and in front of an IDS and firewall to allow packet inspection and network access control. In addition, IP traffic-flow capture and analysis devices placed behind the VPN concentrator allow the 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 be allowed to do so only through an application gateway. This restriction limits the number and type of applications available to an untrusted connection.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AC-2 Account Management AC-17 Remote Access AC-19 Access Control for Mobile Devices
NIST CSF	PR AC
NIST Privacy Framework	PR.PO-P PR.DS-P PR.AC-P PR.PT-P
NITTF Maturity Framework	ME-8
National Minimum Standards	E-1 E-2 E-3
CERT-RMM	Technology Management
ISO 27002	11.4.2 User authentication for external connections 11.7.1 Mobile computing and communications
CIS v7	Control 6
GDPR	Article 9 Processing of special categories of personal data Article 29 Working Party Opinion 2/2017 on data processing at work

BEST PRACTICE 14

BEST PRACTICE 14

Establish a Baseline of Normal Behavior for Both Networks and Workforce Members

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	○	○	✓	✓	✓	✓	○

This best practice builds on **Best Practice 12**. Once organizations identify and fuse the most information-rich data streams related to their ***critical assets***, they can then begin to analyze the data.

Every organization has a unique network topology that has characteristics (e.g., bandwidth utilization, usage patterns, protocols) that can be monitored for security events and anomalies. Similarly, all ***workforce members*** in the organization have their own unique characteristics (e.g., typical working hours, resource usage patterns, resource access patterns). Deviations from normal network and workforce member behavior can signal possible security incidents, including ***insider threats***. To be able to identify deviations from normal behavior, the organization must first establish what characterizes normal network and workforce member behavior.

Protective Measures

To create a baseline of normal activity, the organization must do the following:

- Identify the data points to collect that are relevant to the use case.
- Determine how long data points will be collected to establish a baseline.
- Decide which tools to use for collecting and storing the data.

Various tools are available for baselining normal network activity and identifying anomalies, and other specialized tools have emerged in recent years for baselining normal workforce member behavior and identifying anomalous activity.

The organization must ensure that it collects 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. The organization must account for normal activity spikes as part of the baseline so that it accurately reflects its operations. Collecting baseline data for too long, however, increases the likelihood that abnormal or malicious behavior will become part of the baseline, and it can render the information inaccurate. If data patterns show seasonality (e.g., cycles on daily, weekly, monthly bases), consider using time series methods for baselining.

Computers on any given network typically must communicate to a relatively small number of devices. For example, a workstation might need access only to a domain controller, file server, email server, and print server. If this workstation communicates with any other devices, it might simply be misconfigured, or someone might 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. Use of the organization's virtual private network (VPN) should be carefully monitored because it allows users to access organizational resources from nearly any place that has an Internet connection.

The organization can have policies that define permissible times for network access. For example, an organization might permit workforce members to have some VPN access only during business hours, while others may permit access at any time. Monitoring access times and/or enforcing access policies help an organization detect ***insider*** activity.

An organization that does not require VPN connections from foreign countries should consider permitting (via block listing) VPN connections only from countries where a business need exists. The organization 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***, the organization should also consider limiting access only to ***assets*** the organization owns. When this is not possible, an application gateway can restrict which resources are remotely accessible. The organization should also monitor VPN connections for any abnormal behavior, such as a sudden download of data that exceeds normal use.

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 Simple Mail Transfer Protocol (SMTP) traffic may be a cause for concern. Similarly, use of protocols with a nonstandard port should be flagged for review (e.g., using the Secure Shell [SSH] protocol on port 80, instead of the usual port 22).

The organization should review firewall and ***intrusion detection system (IDS)*** logs to determine normal activity levels. Security information and event management (SIEM) helps security workforce members sift through event logs and establish a baseline of normal firewall and IDS behavior. Sudden changes in the number of alerts can indicate abnormal behavior and should be investigated. For example, a sudden surge in port 21 (file transfer protocol [FTP]) firewall denials caused by a workstation can indicate that someone is attempting to directly contact an FTP server to upload or download information.

Workforce members tend to develop patterns in the files, folders, and applications they access, and when and where they access the organization's resources and facilities. Deviations from a workforce member's normal access patterns can indicate that they are (1) accessing information outside of their need-to-know (e.g., violating organizational policies such as acceptable use policies [AUP] and intellectual property policies) or (2) attempting to conceal malicious behavior.

Identifying anomalous workforce member activity when compared to a workforce member's peers (e.g., workforce members with the same job title, workforce members that work in the same department, or workforce members that work in the same office) can also identify workforce members whose actions are not in line with their roles and responsibilities within the organization.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Establishing a trusted baseline**—The organization can find it challenging to establish a baseline that analysts can be confident represents acceptable behavior. Baselining current activities might incorporate ongoing and unrecognized malicious activity, including insider attacks.
2. **Ensuring privacy**—The organization can find it challenging to maintain workforce member privacy while collecting data to establish a baseline.

3. **Scaling**—Creating baselines for all workforce members and for all use cases might be technologically and financially infeasible. A single, all-encompassing baseline can conceal concerning behavior if some details go undetected, and this type of baseline is insufficient for most uses. Where baselines are not feasible for individual workforce members or resources, the organization can benefit from establishing baselines for its individual subunits. The organization might need to experiment with levels of detail to decide what best suits its needs.

CASE STUDY: SUNDAY PII DOWNLOADS

The victim organization, a financial institution, employed the insider as a senior financial analyst. Every Sunday, he came to the organization's offices and downloaded 20,000 mortgage applicant records to a Universal Serial Bus (USB) flash drive. He also sometimes downloaded the records during normal working hours. Over a two-year period, he downloaded and sold more than two million records that contained personally identifiable information (PII).

The organization noticed that the insider was coming to work outside of normal working hours, but it believed he was merely hardworking. It had a policy that prohibited flash drives or other storage devices from being used on its computers. The organization 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, he 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 the name of a fictitious consulting company. At least 19,000 mortgage applicants became victims of identity theft. Dozens of class-action lawsuits were filed against the victim organization, which was experiencing financial difficulties and was bought out one year after the incident began.

CASE STUDY: CUSTOMER DISSERVICE

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 its Internet protocol (IP) address.

A manager at the victim organization investigated and discovered that the insider entered the facility after hours and disclosed at least one customer's credit card information on the Internet. She also copied and transferred the organization's proprietary, copyrighted files via the Internet. Despite a warning from management, she continued her activity until her employment was terminated. She was arrested and convicted.

In both cases, the insiders' behavior deviated significantly from baseline network behavior, and both cases present examples of accessing systems outside of normal work hours. One insider accessed and downloaded large volumes of information that were beyond normal system usage.

An organization must establish a normal baseline of activity and be watchful for activity that exceeds that baseline. To avoid the appearance of discrimination or wrongdoing, the organization must carefully document and adhere to policies and procedures for monitoring any workforce member's activity. It should also get legal advice as the policies and procedures are developed, finalized, and implemented.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Use appropriate tools to monitor network and workforce member 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. Explicitly allow access only from countries where a genuine business need exists.[35]

☑ 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 network baseline documentation.

Large Organizations

The recommendations in this subsection apply to 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 are accessible via VPN and from what remote IP addresses. Alert on anything that is outside normal activity.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AC-17 Remote Access AU-5 Response to Audit Logging Process Failures AU-6 Audit Record Review, Analysis, and Reporting CM-7 Least Functionality RA-3 Risk Assessment SC-7 Boundary Protection
NIST CSF	DE AE DE CM DE DP
NIST Privacy Framework	
NITTF Maturity Framework	ME-8 ME-14 ME-16
National Minimum Standards	E-1 E-2 E-3
CERT-RMM	Monitoring
ISO 27002	11.4.2 User authentication for external connections 11.7.1 Mobile computing and communications
CIS v7	Control 6
GDPR	

[35] Regional Internet registries maintain IP address assignments. Registries include African Network Information Centre (AfriNIC), American Registry for Internet Numbers (ARIN), Asia Pacific Network Information Centre (APNIC), Latin America and the Caribbean (LACNIC), and Réseaux Européens Network Coordination Centre (RIPE NCC). Some companies maintain IP data that is available under various licenses. Regional Internet registry data is more accurate.

BEST PRACTICE 15

BEST PRACTICE 15

Enforce Separation of Duties and Least Privilege

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

Although this practice was discussed in relation to ***privileged users***, organizations should implement separation of duties for all ***workforce members*** involved in all business processes. This practice limits the damage that ***malicious insiders*** can inflict on critical business processes, systems, and information.

Protective Measures

Separation of duties requires dividing functions among multiple people to limit the possibility that one workforce member 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. An organization can use technical or non-technical 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, workforce members are less likely to engage in malicious acts if doing so means they must collaborate with another workforce member.

Typically, organizations define roles that characterize (1) the responsibilities of each job and (2) the level of access the job holder requires to the organization's resources to fulfill those responsibilities. An organization can mitigate ***insider risk*** by defining and separating the roles responsible for key business processes and functions. For example, an organization can establish the following:

- Require online management authorization for critical data-entry transactions.
- Implement configuration management processes that allow 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 workforce members to perform backup and restore functions.
- Design auditing procedures to prevent collusion among auditors.

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

An organization must manage least privilege as an ongoing process, particularly when workforce members move through the organization as they are promoted, transferred, relocated, or demoted. As workforce members change jobs, organizations tend not to review their required access to information and information systems. Often, organizations provide workforce members access to the systems or information required for their new job without revoking their access to information and systems required for their previous job. Unless a workforce member retains responsibility for tasks from their previous job, the organization should disable their access to previously required information and information systems.

The organization can use physical, administrative, and technical controls to enforce least privilege. Gaps in access control have often facilitated insider crimes. Workforce members can easily circumvent separation of duties if it is enforced by policy rather than by technical controls. Ideally, an organization should include separation of duties in the design of their business processes and enforce them through technical and non-technical means.

Access control based on separation of duties and least privilege is crucial for mitigating the risk of insider attacks. These principles have implications in both the physical and virtual worlds. In the physical world, the organization must prevent workforce members 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. The organization must prevent workforce members 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.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Separating duties and enforcing least privilege**—A smaller organization might find it difficult to implement separation of duties and least privilege security models because it might not have the workforce resources to accommodate the practices. Implementing these practices at a granular level might interfere with business processes.
2. **Balancing security and the organization's mission**—The organization can find it challenging to strike a balance between implementing these recommendations and accomplishing its mission.

CASE STUDY: BOGUS ALIEN LICENSES

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 and charged them $800-$1,600 per license. Applicants exchanged payment with an insider in the parking lot and then were sent into the victim organization to be processed by another insider.

When a fraudulent license request was made, the insiders falsified department records so it would appear that the immigrants had surrendered an out-of-state license in exchange for their new license. The primary insider also committed Social Security fraud by misusing valid Social Security numbers (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 of imprisonment.

CASE STUDY: BAD CHECKS AND INVOICES

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 the accounting system. The insider issued checks to himself and modified the payee names in the accounting system. To conceal his fraud, he listed vendors that the organization commonly did business with as the payees. The insider also modified bank statements to match the fictitious invoices created. The fake invoices were then stapled to the altered bank statements and filed. The insider was convicted, ordered to pay $400,000 in restitution, and sentenced to over two years of imprisonment, followed by five years of supervised release.

In this case, these individuals were 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 the organization should restrict their level of access. If a workforce member requires additional access, the organization should consider creating a separate account with more granular control and additional logging and auditing.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ To avoid privilege creep, carefully audit a workforce member's access permissions when they change roles in your organization. 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 standard operating procedure 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.

Large Organizations

The recommendations in this subsection apply to large organizations.

☑ Review positions in the organization that handle sensitive information or perform critical functions. Ensure the workforce members filling these positions cannot perform critical functions without oversight and approval. (Backup and restore tasks are often overlooked.) One person alone should not be permitted to perform both backup and restore functions. Separate these roles, and regularly test the backup and recovery processes (including media and equipment). In addition, someone other than the workforce members performing backup and restore functions should transport backup tapes off site.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AC-5 Separation of Duties AC-6 Least Privilege
NIST CSF	PR AC
NIST Privacy Framework	CT.PO-P CT.DM-P PR.DS-P PR.PT-P
NITTF Maturity Framework	
National Minimum Standards	
CERT-RMM	Access Management
ISO 27002	10.1.3 Segregation of Duties 11.2.2 Privilege Management
CIS v7	Control 14
GDPR	

BEST PRACTICE 16

BEST PRACTICE 16

Define Explicit Security Agreements for Cloud Services, Especially Access Restrictions and Monitoring Capabilities

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	○	✓	○	✓	✓	✓	○

Organizations should include provisions for data access control and monitoring in all agreements with cloud service providers. This best practice fine-tunes the guidance provided in **Best Practice 6** for ***trusted external entities (TEEs)*** to specifically address concerns associated with cloud service providers.

Cloud computing enables organizations to quickly establish 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 2011].

A recent study by Ponemon Institute found that “Seventy-eight percent of respondents say users in their organizations accidentally through carelessness, lack of awareness, or account compromise exposed sensitive data; 67 percent of respondents say the organization experienced an account compromise that exposed sensitive data; and 31 percent of respondents say users destroyed sensitive data.” [Ponemon 2021]. Therefore, organizations cannot assume that responsibility for securing sensitive data in the cloud can rest on the cloud service provider.

Protective Measures

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

1. ***private cloud* services**—operated solely for one organization
2. ***community cloud* services**—shared among several organizations
3. ***public cloud* services**—available to any customer
4. ***hybrid cloud* services**—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 types of cloud services, the cloud service provider—a TEE—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.

However, using cloud services can 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. The organization must often trust the service provider's claim that its policies and procedures ensure the organization will receive the required levels of protection. The organization might want to work with the service provider to obtain independent audit reports or conduct an audit themselves to confirm these levels of protection.

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

To understand the cloud environment effectively, sufficient and regular auditing and monitoring of the environment must occur. Depending on the capabilities of the cloud service provider and the service agreement, the service provider might offer monitoring capabilities on behalf of the customer.

To effectively manage the environment and ensure that 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 the 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. Written agreements with the service provider must define these capabilities. The organization should consider requesting or implementing methods for secure authorization and access control specific to clouds [Shin 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 provides users with almost total control of the applications running in that cloud. Many of the control technologies are complex and relatively new, and thereby increase the risk of introduced security vulnerabilities, including those resulting from misconfigurations. To help protect the control plane, the organization can perform near-real-time auditing of access, internal events, and external communications among its components to help distinguish anomalies from normal behavior.

The organization should consider each of its potential ***insider risks*** related to cloud services and determine whether (and to what extent) service level agreements (SLAs) and the provider's insurance cover the identified risks. An ***insider*** at the cloud provider organization can be a rogue administrator who might cause harm, such as the following, to the organization:

- exploits a cloud-related vulnerability to gain unauthorized access to the organization's systems
- steals data from a cloud system
- uses cloud systems to carry out an attack on an employer's local resources

The organization should consider the different types of potential rogue administrators:

- hosting-organization administrators
- virtual-image administrators
- systems administrators
- application administrators

Differences in security policies or access control models between cloud-based and local systems can enable insiders to exploit vulnerabilities that might not otherwise be exposed. Attacks can exploit the increased latency between servers in a cloud architecture or—to cause more damage during an attack—exploit delays due to problems validating the organization's identity to the cloud provider [Claycomb 2012].

Even insiders attacking data, non-cloud data, or systems can use cloud parallel processing to crack password files, access a distributed cloud platform to launch a distributed denial of service (DDoS) attack, or use cloud storage to exfiltrate data from an employer. SLAs should identify all known risks that the provider identified in its enterprise risk assessment, and the organization should ensure that the cloud service provider's insurance would cover losses in case of a provider's business failure.

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

- Specify Human Resources (HR) requirements as part of legal contracts.
- Strictly enforce supply chain management and assess suppliers.
- Define processes for security breach notification.
- Ensure transparency in overall information security and management practices.

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

To improve its data access latencies around the world and increase its resilience to local Internet problems, cloud providers often establish data centers in multiple countries. However, each country has particular laws, cultural norms, and legal standards that are enforced with varying levels of strictness regarding contracts, security, background checks, and corruption.

Employees of cloud service providers have ultimate control over the hardware, and consequently, they have control over the 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 [DHS 2021].

The organization should review the particular risks related to the countries their data can go to and whether contracts with the cloud service provider offer adequate assurance of data security. Under the European Union (EU) General Data Protection Regulation (GDPR), organizations must consider (1) the potential for any international transfers of data and (2) whether levels of security comparable with GDPR guidelines are provided.

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 information technology (IT) system processes. The consultant has expert knowledge about the migration process and is given information about the organization's IT systems. Therefore, the consultant has the means—equivalent to the organization's workforce members—to cause the organization a great deal of harm. Vetting and performing background checks on outside consultants for this process should be particularly rigorous; oversight of these consultants is critical.

Cloud infrastructure audits should periodically evaluate cloud security, including auditing virtual machines, to ensure they meet security configuration requirements. Continuously monitoring 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.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Working with cloud service providers**—The organization might find it challenging to establish contracts with cloud service providers due to the provider's business model. It can be a challenge to find a service provider that meets the organization's expectations of both physical and logical security. Some providers leave security up to the customer [Ponemon 2011].
2. **Accepting risk**—The organization should consider cloud services as it does 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. The organization should keep in mind that it is ultimately entrusting the organization's data and outsourced services to an external entity. A failure by the TEE, whether security related or otherwise, can expose the organization to negative publicity or legal action.
3. **Finding established standards**—The organization might not have or be able to find established standards for mitigating insider risks in a cloud computing model.

CASE STUDY: FAKE RETAIL VPN

A retail organization that used Universal Serial Bus (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 his termination, he contacted the IT department, using the fictional name he had created, and convinced them to activate the VPN token. Several months later, he used the VPN token to access the network and delete virtual machines, shut down a storage area network (SAN), and delete email mailboxes. It took the IT staff 24 hours to restore operations, and it cost the organization more than $200,000.

CASE STUDY: LUNCH HOUR DELETE SPREE

Senior management of a pharmaceutical company had a dispute with an IT employee. The insider resigned, but her supervisor and close friend convinced the company to keep her on as a contractor. A few months later, she left the company completely. She used her home network to install software on the victim organization's server. Then, using a restaurant's Internet connection and a compromised user password to access the server, she 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 because of her purchases in the restaurant near the time of the attack. She was arrested and pleaded guilty.

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

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations that use cloud services. Cloud services that are not owned and operated by the organization deserve further scrutiny.

☑ Before entering into any agreement, conduct a risk assessment of the data and services that your organization plans to outsource to a cloud service provider. Ensure that the service provider poses an acceptable level of risk and has implemented mitigating controls to reduce any residual risks. Carefully examine all aspects of the cloud service provider to ensure it 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 its workforce members (e.g., operations staff, technical staff, janitorial staff) before they are hired. In addition, verify that the service provider conducts periodic credit checks and reinvestigations to ensure that changes in a workforce member'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 who is responsible for restricting logical and physical access to your organization's cloud assets.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AC – Access Control AU – Audit RA – Risk Assessment SC – Secure Communications SA – Services and Acquisitions
NIST CSF	PR AC
NIST Privacy Framework	CT.PO-P CT.DM-P PR.DS-P PR.PT-P
NITTF Maturity Framework	ME-8
National Minimum Standards	H-1
CERT-RMM	External Dependencies Management
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 10.2.1 Service delivery 10.2.2 Monitoring and review of third party services 10.2.3 Managing changes to third party services
CIS v7	Control 14
GDPR	Chapter 5: Transfers of personal data to third countries or international [organizations]

BEST PRACTICE 17

BEST PRACTICE 17

Institutionalize System Change Controls

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	○	○	○	✓	✓	✓	✓

Organizations must control changes to systems and applications to prevent the insertion of ***backdoors***, keystroke loggers, ***logic bombs***, and other malicious code or programs. Organizations should thoroughly implement ***change controls*** and continue to implement them over time and in all project stages.

Protective Measures

Security controls are defined in National Institute of Standards and Technology (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 2015a]. Change controls are security controls that ensure the accuracy, integrity, authorization, and documentation of all changes made to computer and network systems.[36]

When consulting cases in the CERT Insider Threat Incident Repository, a wide variety of ***insider*** compromises rely on unauthorized modifications to the victim organizations' systems, which suggests the need for stronger change controls. To develop stronger change controls, the organization must first identify baseline software and hardware configurations. It can have several baseline configurations, given the different computing and information needs of different users (e.g., accountant, manager, programmer, receptionist). As the organization identifies its different baseline configurations, it should also characterize the hardware and software components related to each configuration.

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

- cryptographic checksums (e.g., using SHA-256)
- interface characterization (e.g., memory mappings, device options, serial numbers)
- recorded configuration files

[36] Access the Institute of Internal Auditors *Information Technology Controls* at **https://na.theiia.org/Pages**.

Once the organization documents this information, it can validate the computers implementing each configuration by comparing them against the documentation. 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 [Grim 2014].

Depending on the computing environment, configurations can change frequently. The organization's change management process should include *characterization* and *validation.* The organization should define different roles within the change management 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 (e.g., planted logic bombs). Some commercial software products monitor the system to detect configuration changes.

The organization must protect change logs and backups to detect unauthorized changes and, if necessary, roll back the system to a previous valid state. Cases in the CERT Insider Threat Incident Repository include ***malicious insiders*** who modified change logs to conceal their activity or implicate someone else for their actions. Other insiders sabotaged backups to further amplify the impact of their attack.

Malicious code placement and other malicious insider information technology (IT) actions can defeat common defensive measures, such as firewalls and ***intrusion detection systems (IDSs)***. While these defenses are useful against external compromises, they are less useful against attacks by malicious insiders since 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 can reduce the likelihood of a successful compromise. However, to detect the latest malicious code, antivirus software must update the latest malicious code detection signatures regularly. ***Zero-day exploits*** (i.e., exploits that have never been seen before) and logic bombs (e.g., maliciously configured or scheduled ordinary processes such as incomplete backups) are likely to be missed by signature-based antivirus solutions. Change controls help address the limitations of these defenses.

Just as the organization can implement tools for detecting and controlling system changes, it should also implement configuration management tools for detecting and controlling changes to source code and other application files. As described in **Best Practice 15**, some insiders have attacked organizations 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 using a configuration management system. However, once the system is in production and development stabilizes, some organizations relax the controls, leaving it vulnerable and open to exploitation by technical insiders.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Managing the project**—Change controls can increase the amount of turnaround time required for system changes.
2. **Monitoring**—Changing the information system can entail adjustments to monitoring mechanisms, so IT ***workforce members*** might 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 that have unique configurations and require special management and patching procedures, it also introduces risk. Having many baselines with similar software or configurations can allow an attacker to exploit a single vulnerability on a large scale.

CASE STUDY: RISKY BOMB INVESTMENT

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, she was employed by the same organization as a securities trader. For unknown reasons, she became angry with management; she might have been displeased with her bonus, even though she made more than $125,000 a year.

Motivated by revenge, the insider inserted a logic bomb into the risk assessment program she 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 therefore, the traders 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 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 that did occur. The insider later claimed that she created the program for personal use, but she contradicted this claim when she revealed that a trader made a large profit using the insider's program. The insider was terminated, arrested, and convicted, but sentencing details are unknown.

CASE STUDY: FINANCIAL TAKEDOWN

A financial services firm employed the insider as a systems administrator. He heard that bonuses would be half what they normally were and complained to his supervisor. When the organization announced the cut to employee bonuses, he responded by building and distributing a logic bomb on the organization's 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 the firm's stock price down. 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 organization never fully recovered.

A forensics investigation connected the insider to the incident through virtual private network (VPN) access and copies of the logic bomb source code found on his home computers. He was arrested, convicted, and sentenced to 97 months of imprisonment.

In both cases, the insiders were able to manipulate critical production systems by adding malicious code to them. The insiders caused the victims (e.g., organizations, their customers, their 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 earlier, and the attack could have been mitigated or neutralized before causing substantial harm.

Quick Wins and High-Impact Solutions

All Organizations

The recommendation in this subsection applies to all organizations.

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

Large Organizations

The recommendations in this subsection apply to large organizations.

☑ Implement a change management program within your organization. Ensure that a change control board vets all changes to systems, networks, and 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 and any planned changes.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	CA-2 Control Assessments CM-1 Policy and Procedures CM-3 Configuration Change Control CM-4 Impact Analysis CM-5 Access Restrictions for Change CM-6 Configuration Settings
NIST CSF	PR PT DE DP
NIST Privacy Framework	GV.MT-P CT.PO-P PR.PO-P
NITTF Maturity Framework	
National Minimum Standards	
CERT-RMM	Technology Management
ISO 27002	10.1.2 Change Management
CIS v7	Control 5 Control 11
GDPR	

BEST PRACTICE 18

BEST PRACTICE 18

Implement Secure Backup and Recovery Processes

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	○	○	○	✓	○	✓	○

Despite all the precautions an organization takes, it is still possible that an ***insider*** will carry out a successful attack. Organizations must prepare for that possibility and enhance their resilience by implementing and periodically testing secure backup and recovery processes.

Protective Measures

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

- Reduce the amount of downtime (from days to hours) needed to restore systems from backups.
- Avoid weeks of manual data entry when current backups are not available.
- Reduce the amount of time (from years to months) needed to reconstruct information that has no backup copies.

Backup and recovery strategies should include the following:

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

The organization should also legally and contractually require accountability and full disclosure of any ***trusted external entities (TEEs)*** responsible for providing backup services, including off-site storage of backup media. Service level agreements (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 demonstrate the ***threat*** presented by TEE ***workforce members***. The organization should also apply these mitigation strategies to threats posed by backup service providers.

The organization should encrypt backup media, and it should verify and record cryptographic checksums (e.g., SHA-256 checksums) before the media leaves the organization. This practice ensures that the confidentiality and integrity of the data remains intact while in transport and storage. The organization should manage encryption keys to ensure the data is available when needed.

When possible, the organization should have multiple copies of backups and store redundant copies in a secure, off-site facility. Different individuals should be responsible for safekeeping each copy so that multiple individuals would need 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 TEE 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 workforce members responsible for backing up the information resign or are terminated, the organization should always follow the two-person rule when managing 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 Incident Repository describe attackers who deleted backups, stole backup media (including off-site backups in one case), and performed actions with consequences that could not be undone due to faulty backup systems. In these cases, some system administrators neglected to perform backups in the first place, while other insiders sabotaged established backup mechanisms. These actions can amplify the negative impact of an attack on an organization by eliminating the only means of recovery.

The organization should take the following actions related to backup and recovery processes 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 are applied to other systems.
- Apply the two-person rule to protect the backup process and physical media so that one person cannot act without the knowledge and approval of another workforce member.

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

The organization must regularly test its backup and recovery processes. Most importantly, it must test its backup media. A regular exercise, conducted as part of disaster recovery or continuity of operations exercises, should test the organization's ability to restore data from backup. A tabletop exercise is not sufficient.

An effective 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. Requiring the test to restore to a random date from past archives with no notice of that date until the restore test, helps test for and prevent bad backups while simultaneously preventing malicious backup administrators from tampering with test processes.

For example, a malicious backup administrator who knows of an impending exercise could configure the backup and recovery mechanisms to function properly to conceal any ongoing malicious activity. If the organization separates the backup and recovery roles, this test will also verify whether organizational policies and procedures are working.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Justifying operational costs**—It can be difficult for the organization to justify the additional costs needed to implement more sophisticated and resilient backup and recovery processes, separation of duties, and on-site and off-site storage media and facilities.
2. **Managing keys**—The organization might need to purchase additional hardware or software to properly manage encryption keys and ensure that backup and recovery processes will succeed.
3. **Testing the restoration process**—It can be difficult for the organization to remain diligent with testing the full backup and restore process; however, this process should be tested regularly to ensure that personnel, policies, and technology are current and operating as expected.

CASE STUDY: MIDNIGHT DELETE SPREE

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 even included the contact information of her manager. On the Friday before the incident, she called in sick. She contacted the business owner's wife about the ad that was placed on Saturday. The victim's wife tried to convince the insider that the ad was for a job at a company the victim's wife owned and was not an ad for the insider's position.

At 11:00 p.m. on Sunday, the insider entered the company's premises and deleted the company's data before leaving at around 3 a.m. The owner arrived at the business office on Monday to discover that 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. She was convicted, ordered to pay $3,000 in restitution, and sentenced to five years of probation with 100 hours of community service; she was also required to take court-ordered anger management classes, complete a mental health evaluation, and undergo 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 had implemented off-site storage of backup data, it would have been able to recover within a reasonable amount of time.

CASE STUDY: BOMB BREADCRUMBS

The insider was employed as a programmer by the victim organization, a financial institution. He was responsible for managing the organization's specialized financial software computer network. He had administrative level access to and familiarity with the company's computer systems, including the database server.

He was advised of adverse employment issues and subsequently placed on a performance improvement plan. Shortly after these events, he planted a ***logic bomb*** on the organization's network. He was terminated when he failed to show up at work without providing prior notice. At the time of his 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 he authored the logic bomb. There was also evidence that he deleted computer records that contained his command history of access to the logic bomb. He was arrested, convicted, and sentenced to 12 months of imprisonment, followed by 6 months of electronic monitoring and home confinement, and 3 years of supervised release.

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 attempt to delete those logs.

This case (1) highlights how backups help to mitigate the damage from an insider incident and (2) illustrates the importance of implementing a backup and recovery process for both resuming business operations and identifying the perpetrator.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to 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. Use a professional off-site storage facility; do not simply send backup media home with workforce members. 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, firewalls) are part of your organization's backup and recovery plan as well as its configuration management plan.

Large Organizations

The recommendations in this subsection apply to large organizations.

☑ Implement a backup and recovery process that involves at least two people: a backup administrator and a restore administrator. Both individuals should be trained to perform either role but not authorized to perform both roles simultaneously outside of critical or emergency circumstances.

☑ Regularly test both backup and recovery processes. Ensure that your organization can reconstitute all critical data as defined in its business continuity plan and/or disaster recovery plan. Ensure that each of these processes does not rely on any single person to be successful.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	CP-2 Contingency Plan CP-3 Contingency Training CP-4 Contingency Plan Testing CP-6 Alternate Storage Site CP-9 System Backup CP-10 System Recovery and Reconstitution
NIST CSF	RS RP RS CO RS AN RS MI RS IM RC RP RC IM RC CO
NIST Privacy Framework	PR.DS-P PR.PO-P PR.PT-P
NITTF Maturity Framework	
National Minimum Standards	
CERT-RMM	Knowledge and Information Management
ISO 27002	10.5.1 Back-up
CIS v7	Control 5 Control 11
GDPR	

BEST PRACTICE 19

BEST PRACTICE 19

Mitigate Unauthorized Data Exfiltration

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	○	○	✓	✓	✓	✓	○

Information systems offer many ways to share information—from Universal Serial Bus (USB) flash drives and other removable media to printers and email. Each type of these devices presents unique challenges for preventing data exfiltration. To reduce the risk of an ***insider*** compromising sensitive information, organizations must understand where their information systems are vulnerable to data exfiltration and implement mitigation strategies.

Protective Measures

To mitigate the risk of insiders removing (or exposing) data, the organization must first understand where and how data can be removed. Because many types of technologies and services can become exit points for data, the organization must be able to account for all devices that connect to its systems as well as all physical and wireless connections to its systems. The following are possible exit points that the organization should review:

- Bluetooth
  - wireless file transfers
- Removable Media
  - USB flash drives
  - USB drives (non-flash)
  - compact disc-rewritable (CD-RW) and/or digital video disc-rewritable (DVD-RW)
  - phones with storage
  - media cards (e.g., compact flash, secure digital [SD] cards)
  - projectors with data storage
  - cameras and video recorders
  - microphones
  - web cameras
- Loss of a Device
  - laptop
  - CD
  - hard drive

  - mobile device
  - removable media
- Enclave Exit Points
  - Internet connections
  - interconnections with ***trusted external entities (TEEs)***
- Internet Services
  - file transfer protocol (FTP), secure shell (SSH), and SSH file transfer protocol (SFTP)
  - instant messaging and Internet chat (e.g., GChat, Facebook Chat)
  - cloud services (e.g., online storage, email)
- Hardware
  - printers, fax machines, copiers, and scanners

Removable media is prevalent in every organization, and many ***workforce members*** 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 for Microsoft-Windows-based environments can control which types of devices can be installed on a client system [Bishop 2010]. Other commercial solutions allow a finer grained approach to controlling USB devices and offer additional features, such as shadow copying files, which makes a snapshot copy of any file that is moved to removable storage. This copy allows the 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 its data, the organization should establish a policy that requires workforce members to use only media devices owned by the organization for transferring files.

Organizations that identify, as part of a risk assessment, that USB devices are a ***threat*** should consider adopting policies and procedures that restrict who reviews, approves, and conducts file transfers. For example, the organization can limit the use of these devices to a trusted agent, or at least a second person (using the ***two-person rule*** [Infosecurity 2010]). The following is an example policy an organization could implement:

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

Software development organizations can especially benefit from having a separate, disconnected network for source code and other types of software-related intellectual property (IP). The development network should not (1) connect to any of the other organizational networks, (2) have Internet access, or (3) allow unrestricted access to removable media capabilities. These restrictions eliminate the possibility of emailing sensitive data from the development network and force workforce members to use the data transfer process, if established, for moving data between systems.

The organization must also understand and define all network connections to the 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 TEE are outside of the organization's enclave and are potential exit points for sensitive organizational information.[37] Data passing through these exit points requires further scrutiny. The organization 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 can 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 enable the decryption and inspection of secure sockets layer (SSL)-encrypted traffic.

The organization must also consider implementing a web-filtering solution that blocks access to certain websites. Typical block lists include competitors' sites[38] and known malicious domains. ***Malicious insiders*** have been known to send their organization's sensitive 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 Internet protocol (IP) addresses and ranges.

If particular workforce members need access to SSH, FTP, or SFTP, a limited access terminal (i.e., ***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. In addition, devices administered by a jump box use certain ports and protocols that allow only that box to connect.

Some commercial solutions enable the organization to capture a complete video of the user's session. This video capture enables management or security personnel to review what commands were executed on a particular system and who executed them. Session video capture has the added benefit of clarifying what changes were made to a system if it malfunctions.

The organization also needs to be aware of cloud-based services or software as a service (SaaS). These services (e.g., email, online storage, online office productivity suites) present another opportunity for data exfiltration. Generally, these types of offerings are outside the organization's enclave, so they might offer little control of where data is stored or transmitted. Malicious insiders can use these services, especially cloud storage and email services, to exfiltrate data. The organization should carefully monitor and restrict access to these services, such as by implementing a proxy for all network traffic and implementing block lists as previously discussed.

Finally, malicious insiders have been known to exfiltrate information by using other devices within the organization, such as printers, scanners, copiers, and fax machines. For example, if the 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.

The organization must carefully control and monitor these devices. Where possible, it should use print servers to facilitate logging. These logs can be helpful in detecting anomalous behavior, such as a large volume of documents being printed, sensitive documents being printed, or documents being printed after normal work hours.

[37] Organizations should notify workforce members through an acceptable use policy (AUP) that their Internet use and private email use conducted on employer resources will be scrutinized.

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

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Balancing security with productivity**—The organization might find it challenging to determine an appropriate level of security to prevent data leakage while enabling workforce members to telecommute and freely collaborate with other organizations.
2. **Getting a return on investment**—The organization must weigh the costs and risks of data exfiltration against the costs of protection mechanisms and their effects on productivity.

CASE STUDY: SODA SECRETS FOR SALE

A top executive of a beverage manufacturer employed the insider as an executive administrative assistant. Her 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. She copied some documents and physically stole others. She 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 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 Federal Bureau of Investigation (FBI) conducted an undercover investigation.

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

CASE STUDY: CAUSTIC CHEMICAL TRANSFER

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

At the victim organization, he 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. He attempted to force the transfer by asking the IT department how to perform the transfer, falsely stating that it had been approved. Before his departure, the victim organization performed a forensic examination on his 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 him about downloading confidential documents and his connection to the beneficiary organization. He initially confessed that he downloaded documents to an external drive, but he denied any additional actions or connections to the beneficiary organization. He considered the documents to be reference materials.

A subsequent investigation revealed that the insider copied the documents to his personal computer, and there was evidence that he transferred information to his personal online email account. The incident was detected before the information could be shared with the beneficiary organization.

CASE STUDY: STOLEN TAX REFUNDS

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

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

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Establish a ***cloud computing*** policy. Be aware of cloud computing services and how workforce members might use them to exfiltrate data. Restrict and/or monitor what workforce members can transfer to 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 ensure the organization's sensitive information is removed from its 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 secure copy protocol (SCP), to only workforce members with a justifiable business need, and carefully monitor their use.

Large Organizations

The recommendations in this subsection apply to large organizations.

☑ Inventory all connections to the organization's enclave. Ensure that service level agreements (SLAs) and/or memoranda of agreement (MOAs) are in place. Verify that connections to your organization's enclave are still in use and have a justified business need to exist. Implement protection measures, such as firewalls, devices that capture and analyze IP traffic flow, and ***intrusion detection systems (IDSs)*** at these ingress and egress points so that data can be monitored and scrutinized.

☑ Isolate development networks and disable connections to other systems or the Internet.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	AC-20 Use of External Systems CA-3 Information Exchange CM-7 Least Functionality MP-2 Media Access MP-3 Media Marking MP-5 Media Transport PE-5 Access Control for Output Devices SC-7 Boundary Protection
NIST CSF	RS RP RS CO RS AN RS MI RS IM RC RP RC IM RC CO
NIST Privacy Framework	PR.AC-P PR.DS-P PR.PO-P
NITTF Maturity Framework	
National Minimum Standards	G-1
CERT-RMM	Technology Management
ISO 27002	12.5.4 Information Leakage
CIS v7	Control 7 Control 9 Control 12 Control 13
GDPR	

BEST PRACTICE 20

BEST PRACTICE 20

Develop a Comprehensive Workforce Member Termination Procedure

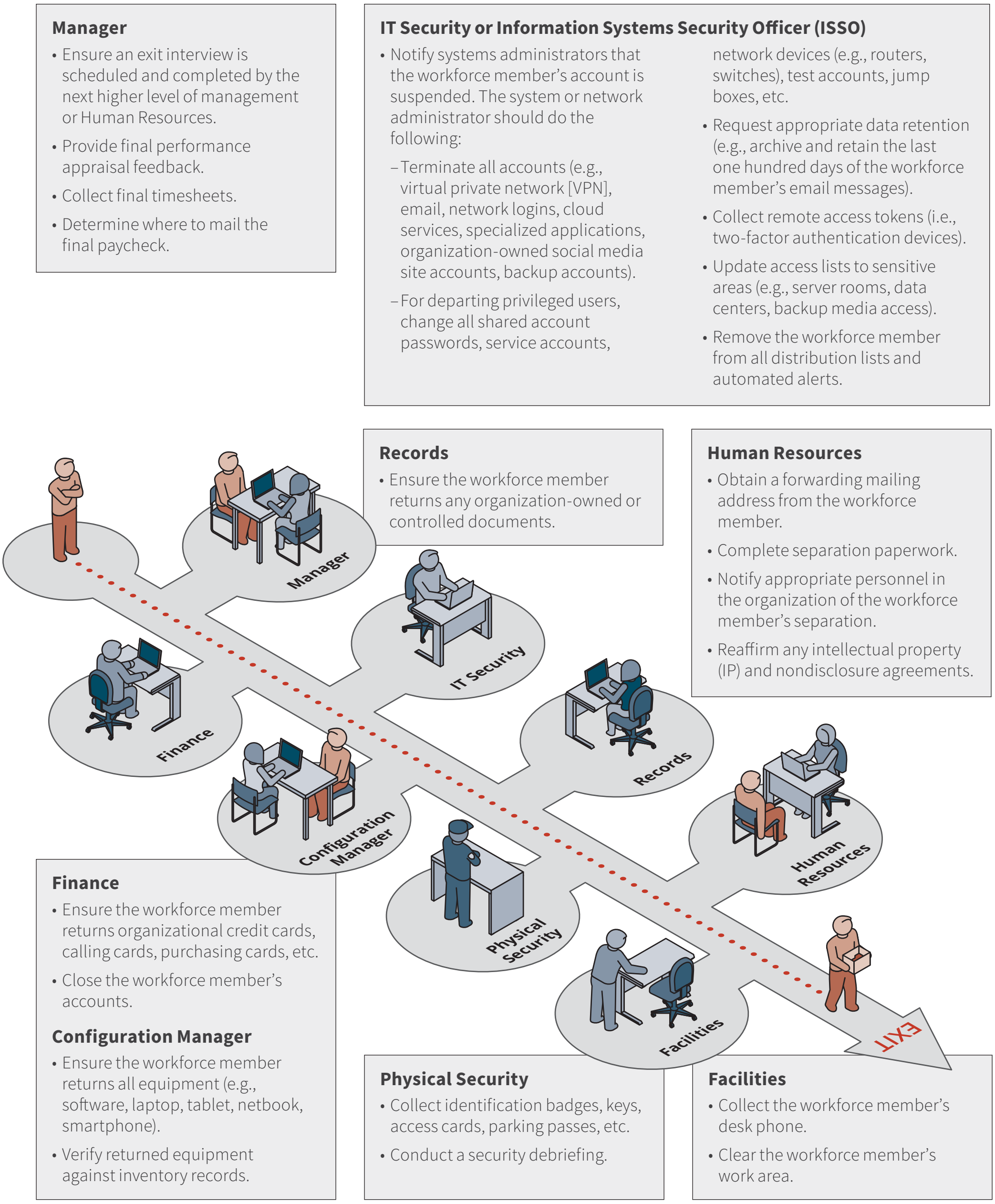
Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	✓	✓	✓	✓	✓	✓	○

Organizations must have a termination procedure that reduces the risk of damage from former ***workforce members***. Termination procedures should ensure that the former workforce member's accounts are closed, their equipment is collected, and the remaining personnel are notified. Proper account and inventory management processes can help the organization reduce its ***insider risk*** when a workforce member separates from the organization. Workforce member termination should be done in a consistent and respectful manner, which can help decrease future disgruntlement that could lead to a workforce member returning and committing an act of workplace violence.

Protective Measures

The organization must develop policies and procedures that encompass all aspects of the termination process. To prepare for a workforce member's departure, various members of the organization must complete tasks before the workforce member's last day. A termination checklist can help the organization track the steps a workforce member must complete.

At a minimum, a termination checklist should include each task, who should complete the task, who should verify task completion, when the task must be completed, and a signature line for the initials of the person completing the task. The completed checklist should be returned to Human Resources (HR) before the workforce member leaves the organization. Figure 14 includes a list of tasks 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 Human Resources.
- Provide final performance appraisal feedback.
- Collect final timesheets.
- Determine where to mail the final paycheck.

IT Security or Information Systems Security Officer (ISSO)

- Notify systems administrators that the workforce member's account is suspended. The system or network administrator should do the following:
  - –Terminate all accounts (e.g., virtual private network [VPN], email, network logins, cloud services, specialized applications, organization-owned social media site accounts, backup accounts).
  - –For departing privileged users, change all shared account passwords, service accounts, network devices (e.g., routers, switches), test accounts, jump boxes, etc.
- Request appropriate data retention (e.g., archive and retain the last one hundred days of the workforce member's email messages).
- Collect remote access tokens (i.e., two-factor authentication devices).
- Update access lists to sensitive areas (e.g., server rooms, data centers, backup media access).
- Remove the workforce member from all distribution lists and automated alerts.

Records

- Ensure the workforce member returns any organization-owned or controlled documents.

Human Resources

- Obtain a forwarding mailing address from the workforce member.
- Complete separation paperwork.
- Notify appropriate personnel in the organization of the workforce member's separation.
- Reaffirm any intellectual property (IP) and nondisclosure agreements.

Finance

- Ensure the workforce member returns organizational credit cards, calling cards, purchasing cards, etc.
- Close the workforce member's accounts.

Configuration Manager

- Ensure the workforce member returns all equipment (e.g., software, laptop, tablet, netbook, smartphone).
- Verify returned equipment against inventory records.

Physical Security

- Collect identification badges, keys, access cards, parking passes, etc.
- Conduct a security debriefing.

Facilities

- Collect the workforce member's desk phone.
- Clear the workforce member's work area.

Figure 14: Termination Checklist

The CERT Insider Threat Incident Repository includes cases that involved unreturned organization-owned property. As part of the separation process, the organization must collect its physical property (e.g., badges, access cards, keys, two-factor authentication tokens, mobile devices, laptops). Any of these items, if not returned, can enable the former workforce member to attack the organization. Collecting these items cannot completely prevent these attacks, but it does mitigate the risk. A physical inventory system that tracks all equipment issued to workforce members allows the organization to understand who has what property at any given time.

Another step in the separation process is to reaffirm with the departing workforce member any agreements about intellectual property (IP) and nondisclosure. This step in the process is an opportunity to remind the workforce member about their obligations to the organization even after separation. While an organization's priority is the confidentiality surrounding its information ***assets***, a workforce member's departure requires consideration of their privacy as well. ***Right to erasure*** (or, as it is more commonly known, the ***right to be forgotten***) applies most often to customer relationships with an organization, but all ***data subjects*** have the right to request the erasure of personal data if certain circumstances apply (e.g., if General Data Protection Regulation [GDPR] applies).

For workforce member relationships, the most relevant circumstance is if a workforce member's personal data might be unlawfully processed or is no longer necessary for processing (e.g., a workforce member exited an organization and their data is not needed by the ***insider risk management program [IRMP]***). As such, the organization should consider its legal responsibility to comply with such requests and how they might impact the data monitoring and aggregation efforts of the IRMP.

Finally, the organization should review the departing workforce member's online actions around the time of their termination. CERT research findings, along with feedback from those who operate IRMPs, suggest that at least 30 days of a workforce member'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 2011b].

This review should include email activity to ensure that the workforce member did not send email messages that contained sensitive organizational data outside the organization, such as to a personal email account or a competitor. If the organization allows workforce members to access cloud-based, personal email services, the organization should maintain access logs (e.g., 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 workforce members are not storing sensitive organizational information in the cloud.

Once a workforce member has left the organization, HR should notify all workforce members of the separation. HR might be reluctant to do this because of privacy concerns, but it does not need to say how or why the workforce member left the organization. A simple message such as the following should suffice to notify workforce members: "Joe Smith no longer works for the organization. Please do not disclose confidential information to Joe Smith."

Informed workforce members can alert management and security if they observe a former workforce member in the organization's facility. If workforce members do not know about terminations, they can 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.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Disclosing information**—The organization might have legal concerns about how much information to release about a recently terminated workforce member.
2. **Completing exit procedures**—Each department within the organization might need its own termination checklist that is tailored to that department's needs.

CASE STUDY: WEB DATA TERMINATION

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

CASE STUDY: VINDICTIVE MESSAGING

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 organization and went to work for another organization. Six months after leaving the victim organization, the insider used a valid email account, which the victim organization had not disabled, to send email messages to 5,600 of the organization's customers.

The email messages 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 Incident Repository contains many cases of organizations failing to delete or block all accounts associated with a former workforce member. Well-defined termination procedures coupled with solid account management processes should increase an organization's confidence that former workforce members can no longer access its systems.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

☑ Develop an enterprise-wide checklist to use when someone separates from your organization.

☑ Establish a process for tracking all accounts assigned to each workforce member.

☑ Reaffirm all nondisclosure and IP agreements as part of the termination process.

☑ Notify all workforce members about any workforce member's departure, where permissible and appropriate.

☑ Archive and block access to all accounts associated with a workforce member who has departed the organization.

☑ Collect all of a departing workforce member's organization-owned equipment before the workforce member leaves your organization.

Large Organizations

The recommendations in this subsection apply to large organizations.

☑ Establish a physical-inventory system that tracks all assets issued to each workforce member.

☑ Conduct an inventory of all information systems, and audit the accounts on those systems.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	PS-4 Personnel Termination PS-5 Personnel Transfer
NIST CSF	PR AT
NIST Privacy Framework	PR.DS-P PR.PO-P
NITTF Maturity Framework	
National Minimum Standards	G-1
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
CIS v7	Control 16
GDPR	Article 17 Right to erasure ('right to be forgotten') Article 19 Notification obligation regarding rectification of personal data or restriction of processing

BEST PRACTICE 21

BEST PRACTICE 21

Adopt Positive Incentives to Align the Workforce and the Organization

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

Workforce management practices that increase ***perceived organizational support*** are called ***positive incentives*** because they attempt to entice (rather than force) a ***workforce member*** to act in the interests of the organization. Enticing workforce members to act in the interests of the organization through positive incentives reduces the organization's baseline ***insider risk***. Positive incentives that align workforce values, experience, and attitudes with the organization's objectives form a foundation on which to build traditional security practices that rely on forcing functions. The combination of incentives and forcing functions improves the effectiveness and efficiency of the organization's ***insider threat*** defense.

This practice is related to **Best Practices 5** and **8**. The difference is that this best practice focuses on using positive incentives to improve workforce member attitudes independent of whether a specific negative issue or ***insider*** stress exists or is even identifiable. It's not necessary to detect negative work issues or insider stress to reduce the frequency of insider incidents by adopting positive incentives.

Protective Measures

Insider threat is unique in the realm of cybersecurity because the potential ***threat*** agents—the organization's employees and ***trusted external entities (TEEs)***—play fundamental roles in accomplishing the organization's mission. Goodwill among the workforce is essential to both minimizing intentional insider threat and ensuring organizational performance.

CERT research suggests that the organization's practices and managerial processes can create a working environment conducive to insider threats by undermining the workforce's goodwill [Moore 2015, Moore 2018]. The vast majority of insider incidents are perpetrated by individuals who started out in their organizations as committed and loyal workforce members. But as professional and/or personal stressors intervened, they found themselves motivated to act counter to the organization's interests [Shaw 2015].

This insight does not imply that the organization is at fault in insider compromise—most insider threat cases are violations of the law or of agreements with the organization that are prosecutable in court. Nevertheless, organizations can reduce the *frequency of insider* *misbehavior and its associated costs* by instituting practices that reduce insider disgruntlement [Moore 2017]. Without properly addressing the context where insider threats occur, insider misbehavior is likely to repeat as a natural response to the organization's existing counterproductive practices.

Traditional security practices focus on negative incentives that attempt to ***force*** compliance through constraints, monitoring, and punishment. This best practice recommends adopting positive incentives to *entice* individuals to act in the interests of the organization. In general, positive incentives create positive attitudes in the workforce that result in positive deterrence of insider threat.

The following positive incentives focus on properties of the organization's workforce management practices, including those that relate to the workforce members' job, their organization, and the people they work with.

- ***Job Engagement*** involves the extent to which workforce members are excited and absorbed by their work. Strengths-based management and professional development investments made by the organization are known to boost workforce member job engagement. Strengths-based management focuses primarily on identifying and using an individual's personal and professional strengths to direct their careers and manage their job performance [Buckingham 2010].
- ***Perceived Organizational Support*** involves the extent to which workforce members believe their organization values their contributions, cares about their well-being, supports their socio-emotional needs, and treats them fairly. Programs that promote flexibility, work/family balance, workforce member assistance, alignment of compensation with industry benchmarks, and constructive supervision that attends to workforce member needs can boost perceived organizational support [Eisenberger 2011].
- ***Connectedness at Work*** involves the extent to which workforce members want to interact with, trust, and feel close to the people they work with. Practices that involve team building and job rotation can boost workforce members' sense of interpersonal connectedness, creating an experience of being embedded in valued relationships with co-workers, managers, and the broader organization [Brien 2012, Malone 2012].

CERT research suggests that perceived organizational support is particularly important [Moore 2016]. These findings are consistent with social exchange theory and associated research on workforce member/employer relationships, which show that individuals reciprocate their employer's treatment of them, whether that treatment is perceived as good or bad.

A survey of insider risk management practitioners conducted by CyLab, Carnegie Mellon University's (CMU's) Security and Privacy Institute, found significant levels of concern over the following possible side effects of negative insider risk controls [Moore 2021]:

- infringing on workforce member rights and civil liberties
- inhibiting productivity
- undermining trust in the workforce
- reducing retention of good workforce members

These negative consequences often arise from improperly tuned negative incentives. This is where organizational supportiveness can pay big dividends; managers who (1) express appreciation of the value of their workforce members' contributions, (2) demonstrate care for their well-being, and (3) treat them fairly will help workforce members manage their work and life stress. Empathic managers that support workforce members through difficult times, both personally and professionally, can help.

Within the ***insider risk management program (IRMP)***, investigators that look for disconfirming as well as confirming evidence of wrongdoing can improve the fairness of investigations and reduce the negative impacts of false positives identified using available technology.

Extending the Traditional Information Security Paradigm (Extended from Straub's 1998 work [Straub 1998]) depicts an extension of the traditional security approach with positive incentives. The right side of Figure 15 depicts the traditional approach, which focuses on negative incentives that use workforce member restrictions and sanctions to prevent and punish abuse. This approach is based on a negative form of deterrence as promulgated in ***deterrence theory***, which says that people obey rules because they fear getting caught and being punished. In this model, restricting, monitoring, and punishing workforce members deters abuse through negative reinforcement.

The left side of Figure 15 shows organizational support (including organizational justice) as the foundation of positive deterrence. With this foundation in place, connectedness with co-workers and job engagement serve to strengthen a workforce member's commitment to the organization. Organizational support and connectedness also strengthen overall engagement in a feedback effect.

This form of positive deterrence complements the use of negative deterrence by reducing the baseline of insider risk through improving workforce members' satisfaction, performance, and commitment to the organization.

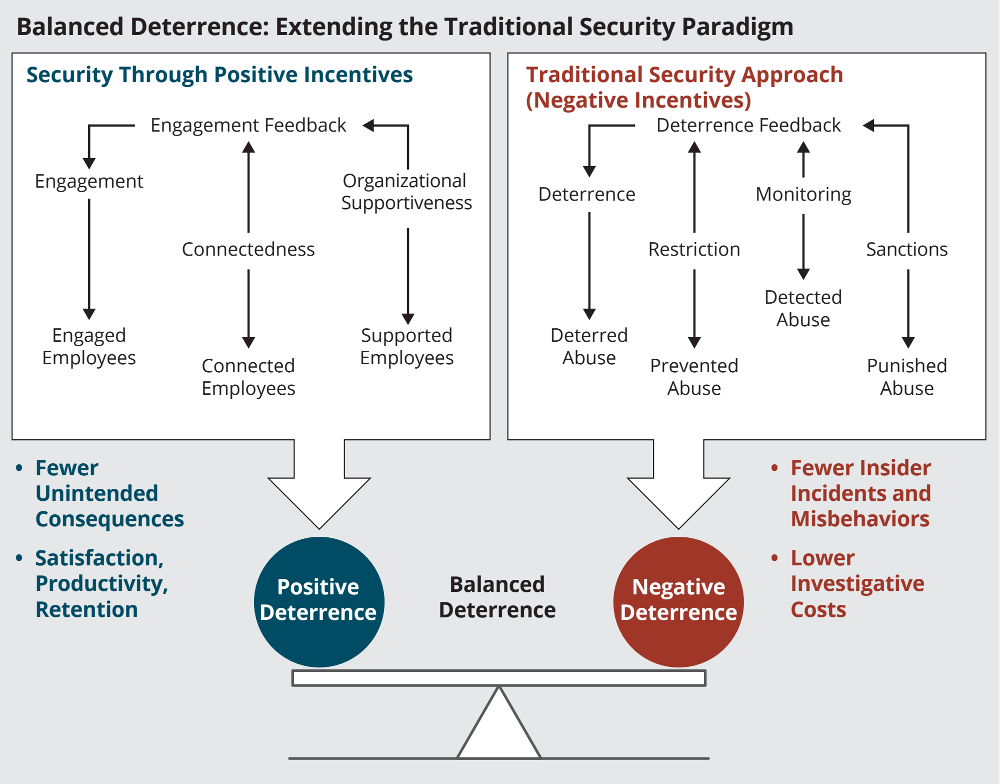

Balanced Deterrence: Extending the Traditional Security Paradigm
Security Through Positive Incentives
Engagement Feedback
Engagement
Organizational Supportiveness
Connectedness
Engaged Employees
Connected Employees
Supported Employees
Traditional Security Approach (Negative Incentives)
Deterrence Feedback
Deterrence
Monitoring
Restriction
Sanctions
Detected Abuse
Deterred Abuse
Prevented Abuse
Punished Abuse
Fewer Unintended Consequences
Satisfaction, Productivity, Retention
Positive Deterrence
Balanced Deterrence
Negative Deterrence
Fewer Insider Incidents and Misbehaviors
Lower Investigative Costs

Figure 15: Extending the Traditional Information Security Paradigm (Extended from Straub's 1998 work [Straub 1998])

The right mix and ratio of positive and negative incentives in an IRMP can create a net positive for both the workforce and the organization—moving an IRMP from a "big brother" program to a "good employer" program that actually improves workforce members' work lives.

In effect, using positive incentives can cause workforce members to view negative incentives as more legitimate and appropriate as a function of the enhanced relationship that an employer's positive incentives create. An IRMP that balances organizational incentives can become an advocate for the workforce and a means for improving an individual's work life—a welcome message to workforce members who feel threatened by programs focused on discovering insider wrongdoing.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Instituting incentives**—Positive incentives are less tangible than traditional, negative incentives. Managers might be more comfortable instituting constraints and detecting and punishing misbehaviors rather than trying to improve satisfaction and decrease disgruntlement in the workforce.
2. **Finding the balance**—Determining the right balance of positive and negative incentives can be difficult and largely depends on the organization's culture. Balance does not necessarily mean equally weighting the two approaches. An appropriate balance depends on the nature of the organization. For example, environments that require high levels of innovation and creativity can require a larger percentage of positive to negative incentives, especially when an in-demand workforce might be alienated and attracted to the competition. More regimented environments that are based on proper conduct and following rules might thrive when negative incentives dominate their positive counterparts.

The claim made by this best practice is that positive incentives, especially those that increase perceptions of organizational support, can reduce baseline insider risk by improving workforce member attitudes. In contrast to the case studies described in other practices, which focus on example insider compromises that occur when the practice is not implemented, the following case studies describe the relationship between ***workforce member*** attitudes and lower insider risk.

Although job engagement and connectedness at work have been found to negatively correlate with counterproductive work behaviors (e.g., works published by Ariani and Sulea [Ariani 2013, Sulea 2012]), an initial analysis of intentional insider threat incident data suggests that perceived organizational support is a foundational positive incentive for reducing insider threat.

CASE STUDY: INCIDENT ANALYSIS

In this project, a team of three CERT researchers rated information on real insider incidents along a five-point scale for each of three dimensions—job engagement, perceived organizational support, and connectedness with co-workers—as shown in Figure 16. The incident information came from public, non-sensitive sources (e.g., media reports, published books). The high end of the scale (+2) indicates the most positive assessment of the dimension; the low end of the scale (−2) indicates the most negative assessment.

To provide raters with a clear meaning for each of the scale's response anchors, this study provided an example at each anchor point and previously developed survey questions used in established assessments for each dimension. The final scales used for each dimension—with examples and clarifying questions—are provided in the SEI report, *The Critical Role of Positive Incentives for Reducing Insider Threat* [Moore 2016].

Because the information available for each incident is not always sufficiently detailed to answer each survey question, this activity is inexact. To increase the accuracy and consistency of the rating process, the final rating for each incident was determined through discussion and consensus by the three raters involved.

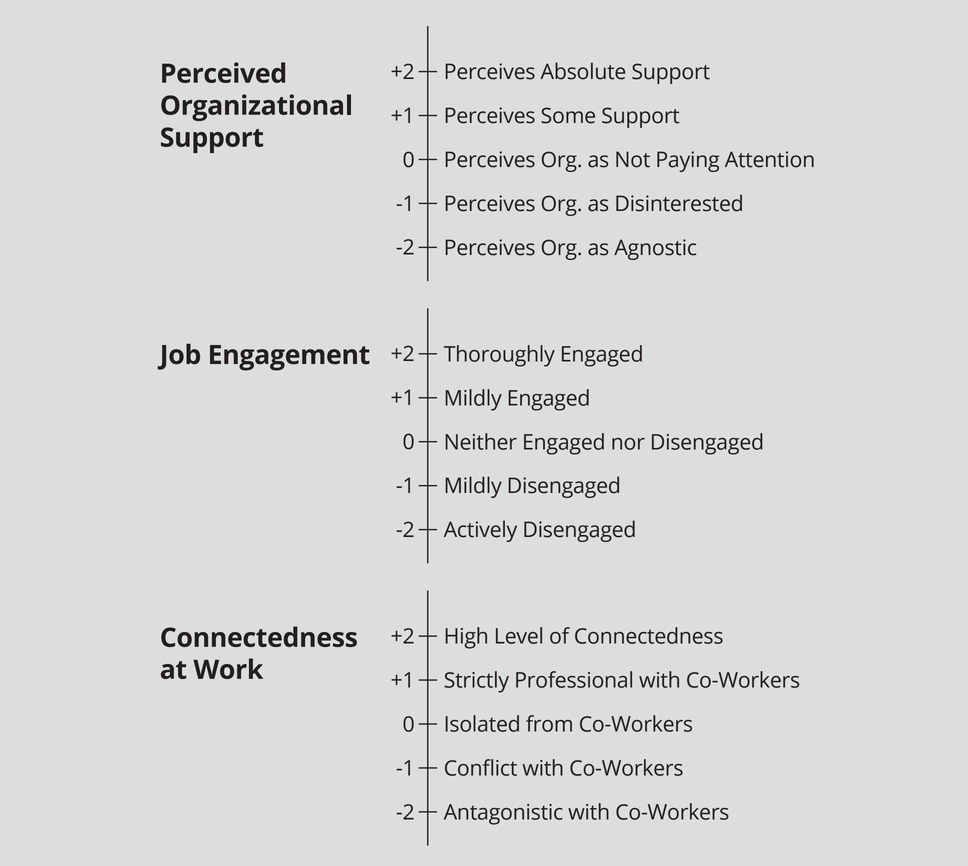

Perceived Organizational Support
+2 Perceives Absolute Support
+1 Perceives Some Support
0 Perceives Org. as Not Paying Attention
-1 Perceives Org. as Disinterested
-2 Perceives Org. as Agnostic
Job Engagement
+2 Thoroughly Engaged
+1 Mildly Engaged
0 Neither Engaged nor Disengaged
-1 Mildly Disengaged
-2 Actively Disengaged
Connectedness at Work
+2 High Level of Connectedness
+1 Strictly Professional with Co-Workers
0 Isolated from Co-Workers
-1 Conflict with Co-Workers
-2 Antagonistic with Co-Workers

Figure 16: Overview of Five-Point Scales for Interest Alignment

▸***continued on next page***

Case Study: Incident Analysis, continued

Raters considered three incidents where intentional harm was perpetrated by disgruntled insiders.[39] Figure 17 provides an overview of the raters' analysis of each of the three incidents (Case 1, Case 2, and Case 3) rated along the five-point scale, +2 to −2. The three dimensions are represented as separate graphs. Each incident is rated for each of three time periods: early, middle, and late. These time periods were specific and well defined for each incident. The raters for each case also provided their assessment of the overall score for each dimension.

As shown in Figure 17, perceived organizational support was negative in all three incidents, while Job Engagement was negative in only two of the three (Case 2 and Case 3). Connectedness at Work was negative in only one of the three cases (Case 2).

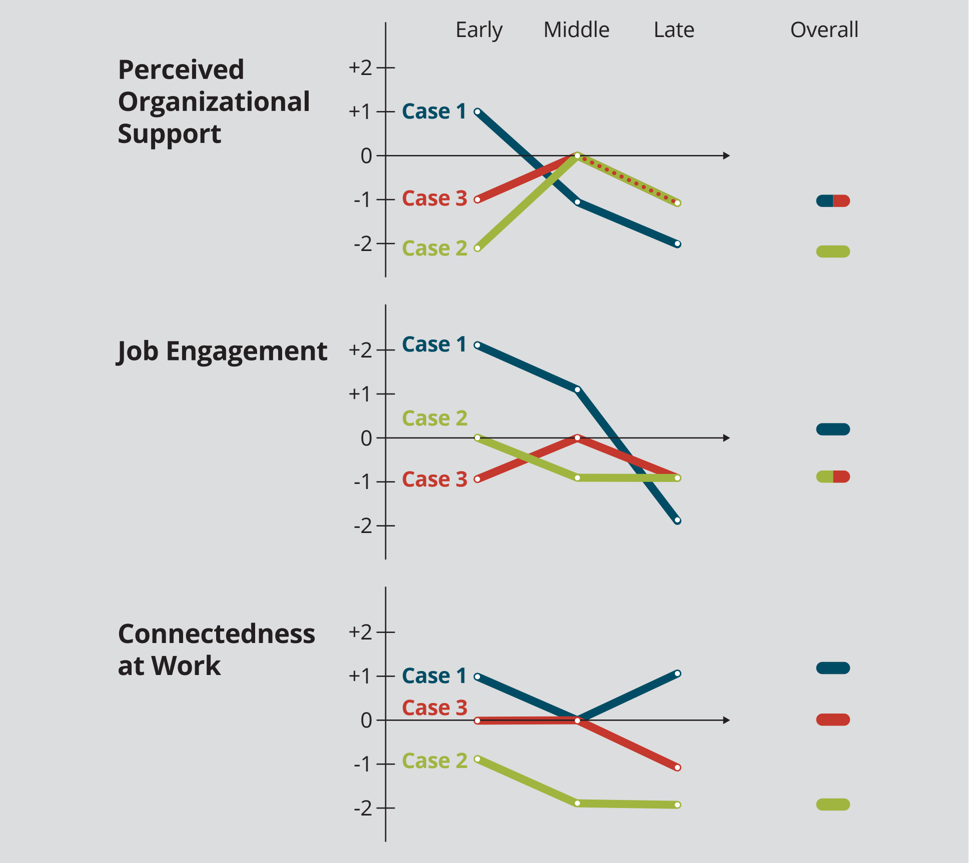


Figure 17: Incident Analysis Overview

This finding was a bit surprising. In looking at the incidents, it seemed like the individual in Case 1 could be fairly engaged in their job despite conducting activities counter to the organization. Even more surprising, the individuals in Case 2 and Case 3 maintained fairly good relations with their co-workers while engaging in activities that betrayed both their organization and the country.

Although it is impossible to draw general conclusions from this small number of cases, the results suggest that perceived organizational support is an important factor in using positive incentives to reduce insider risk. Of the three dimensions studied, the strongest negative correlation with counterproductive work behaviors found in the literature was also linked to perceived organizational support. The combination of evidence obtained from the case analysis, literature search, and survey work argues for focusing on the organizational support dimension for quick wins.

[39] This report does not identify the insiders involved in the incidents rated.

CASE STUDY: ORGANIZATIONAL SUPPORTIVENESS AND INSIDER MISBEHAVIOR

For this project, organizations were surveyed from the Open Source Insider Threat (OSIT) information sharing group—a group that meets regularly to discuss operational issues related to IRMPs in their organizations—to understand how perceptions of organizational support influence insider cyber misbehavior.

The survey used the 36 questions from the Survey of Perceived Organizational Support, which is based on a five-point Likert scale (from 1 = *strongly disagree* to 5 = *strongly agree*) and has been extensively used and validated [Eisenberger 1986, 2011]. CERT researchers developed a five-point frequency scale from 1 = *never* to 5 = *all the time* (i.e., at least once a day) for insider cyber misbehavior; this frequency scale was based on precursors in CERT insider incident data and previously reported counterproductive work behaviors [Spector 2006]. The survey included 22 questions on the frequency of cyber misbehaviors.

There were 23 responses to this survey. Figure 18 illustrates the statistically significant, negative correlation between perceived organizational support and insider misbehavior. As perceived organizational support goes up, the frequency of insider misbehavior goes down within the respondent's organization.

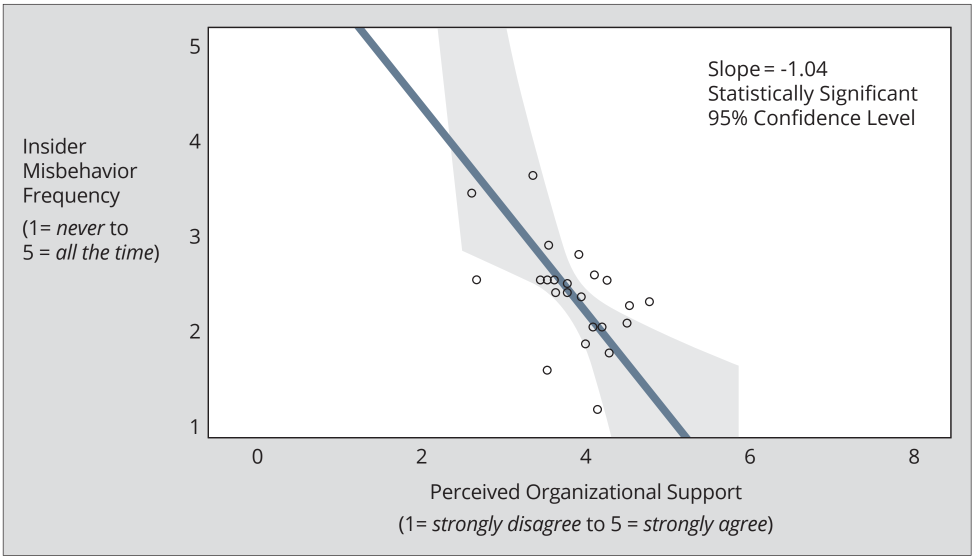


Figure 18: Negative Correlation Between Perceived Organizational Support and Insider Misbehavior

Quick Wins and High-Impact Solutions

All Organizations

The recommendations below apply to all organizations. Organizational support appears to be important for reducing insider misbehaviors and, therefore, is a good starting place for organizations that want to capitalize on the power of positive incentives.

☑ Routinely communicate organizational values and ensure organizational goals are aligned to those values.

☑ Use performance-based rewards and recognition. Ensure criteria is transparent and managers are trained to fairly measure and reward performance.

☑ Expect and model transparent and respectful communication. Maintain communication expectations within a Code of Conduct or other internal resource.

☑ Maintain an Employee Assistance Program (EAP) for employees.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	
NIST CSF	
NIST Privacy Framework	
NITTF Maturity Framework	
National Minimum Standards	G-1
CERT-RMM	Human Resources Management
ISO 27002	
CIS v7	
GDPR	

BEST PRACTICE 22

BEST PRACTICE 22

Learn From Past Insider Threat Incidents

Management	Human Resources	Legal Counsel	Physical Security	Information Technology	Information Security	Data Owners	Software Engineers
✓	✓	○	✓	✓	✓	○	○

Organizations that learn from the past are better prepared for the future. Understanding how prior incidents unfolded, whether in your organization or elsewhere, provides crucial insight into the efficacy of current insider risk management practices; potential gaps in prevention, detection, and response controls; and areas of emphasis for ***insider threat*** awareness and training efforts.

Developing the capability to collect and analyze ***insider*** incident data is a key component of an effective ***insider risk management program (IRMP)*** and should inform its operations, including risk quantification, analysis, and incident response.

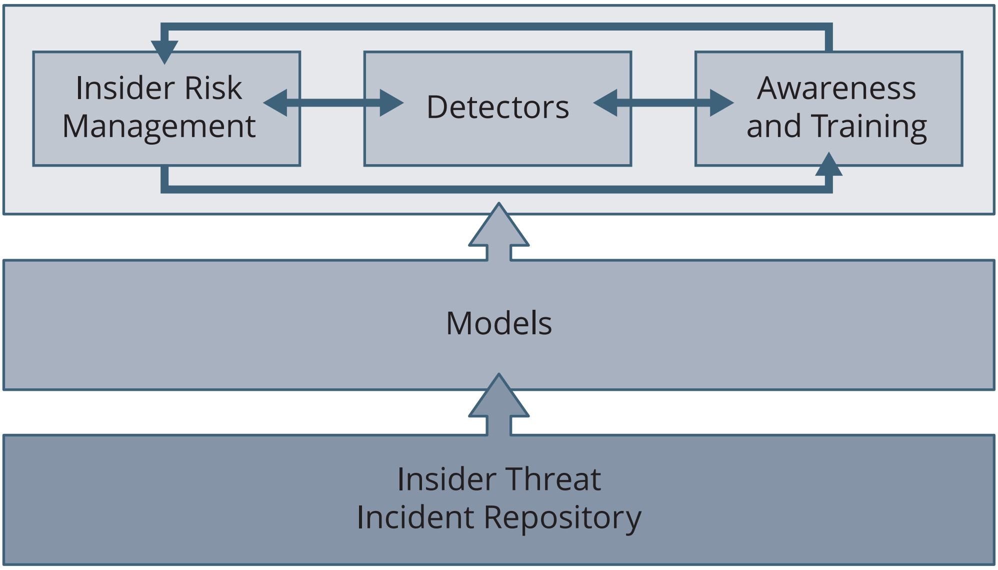


Figure 19: How Data About Prior Insider Incidents Drives Organizational Preparedness

Protective Measure—Design an Insider Incident Repository

Information available about prior insider incidents enables the organization to derive insider threat models, make risk decisions based on historical information, and use examples of insider threat incidents for awareness campaigns and training. Those who are responsible for risk management must collect this information. They typically search for examples as the need arises; however, this reactive approach is time consuming and can result in duplication of effort every time prior incident data is needed. To lessen these issues, the organization should design its own insider threat incident repository.

Internal development of an insider threat incident repository helps inform IRMP operations and, in turn, improves ***operational resilience*** more broadly. For example, supply chain security management processes can also be informed by previous incidents captured in an insider threat incident repository. Furthermore, the repository can help limit reputation risk by supporting the faster detection of incidents. Aggregated data from an insider threat incident repository can highlight potential high-risk networks or environments where ***enhanced monitoring*** or specialized tools should be deployed, or where additional mitigations should be implemented.

Developing and maintaining an insider threat incident repository can be as simple or complex as required to meet the organization's needs. In all cases, leveraging existing standards and practices to implement incident collection and information sharing makes the effort associated with those activities more manageable.

In the simplest form, an insider threat incident repository is a collection of information (e.g., files, media reports) that is organized in a repository. For example, some organizations have a de-facto incident repository of internal incidents in their case management system. A more complex repository example is when the organization uses the formal knowledge management roles and responsibilities of its ***workforce*** to collect and store information in a dedicated repository.

Regardless of its format, several knowledge management activities are involved in developing and maintaining an insider threat incident repository:

1. **Define the purpose and use cases for the insider threat incident repository.** The repository is a tool for meeting operational needs. Those needs should be documented so that the repository stewards can ensure that the repository is developed and maintained to meet those needs. Designers of the initial repository must consider both the insights needed from the data in the repository and use cases that show how users need to interact with the repository (e.g., analyze data directly on the repository platform, pull information into separate analysis tools).
2. **Build a container for an insider threat incident repository.** The repository's container can be a database, code repository, document repository, and/or incident tracker/management system. The container should have a documented structure that reflects the data needs for use cases. These use cases should be documented in a data *code book* that (1) describes the data so that users can understand what it tells them and (2) defines the data expectations for the repository. For example, if the repository is a database, then the code book should provide structural information about each field (e.g., data type). If the repository contains only files, then the code book should define expectations for different file types. The organization should also establish expectations for the repository's use and maintenance (e.g., access control, update schedules, data cleaning, and allowed and prohibited information such as whether or not personally identifiable information [PII] or disciplinary actions are permissible data points).
3. **Collect information.** To fully support the IRMP, the information collected should include both internal and external sources. Examples of external sources that are publicly available include court records, media reports, social media online forums, and/or information security bulletins. This information might include incident-specific information, or best practice or trend information that can be applied to updating repository management. For internal information, the organization should capture information from incident investigations and insights gathered from post-mortem evaluations of responses to incidents.

4. **Share incident data as appropriate.** Since the purpose of the insider threat incident repository is to help the organization and its members make better **insider risk** decisions, it is important that the repository is used to derive insights and that those insights are shared with the people who need them. Since information from the organization is seldom enough to understand the breadth of insider threats, it is important to also gather and share incident data with the broader counter-insider threat practitioner community. In addition to providing general insider risk insights, sharing this information can lead to the exchange of indicators of compromise, tools, tactics, or procedures, and even approaches for prevention, detection, mitigation, or response.

Insight that benefits the organization can be derived from an insider threat incident repository in many ways. The most straightforward way is using incidents as case studies or examples for increasing workforce awareness of insider threat, and training the workforce to recognize and respond to insider threat. Other ways include root cause analysis, summary statistics, trend identification, and correlations. Each of these has its own use cases for the insights they provide.

Each organization should perform some foundational analyses of its repository data, especially the parts that are related to incidents inside the organization and within its information-sharing partnerships. Foundational practices for deriving insights from repository data can be qualitative or quantitative. An example of a qualitative foundational practice is creating incident repository case studies for use in training and awareness activities. A quantitative example is providing trends on how the number and severity of insider incidents are changing over time, which can influence ***threat*** likelihood and impact calculations.

Performing advanced analysis practices requires specialized knowledge or tools. These practices can enable incident data to be automatically processed (e.g., ingested) into the insider threat incident repository, or provide insights that are more complex to derive, such as complex (or hidden) correlations between data points. For organizations using technical controls, such as user activity monitoring (UAM) or user and entity behavioral analytics, advanced analyses should be used to refine and implement the threat models and risk scoring algorithms the controls provide. Many organizations that rely on out-of-the-box configurations of these controls quickly find they need to tailor them to their organization's specific risk appetite, priorities, and cultural norms. An insider threat incident repository is a vital resource that an organization can use to ensure that the IRMP's detective capability aligns (and continues to stay aligned) with the continuously changing threat landscape.

Table 5: **Foundational and Advanced Insights**

FOUNDATIONAL INSIGHTS	ADVANCED INSIGHTS
Summary statistics for each metric/category • statistical distributions and expected values • outliers Year-over-year trends for each metric Case studies and lessons learned	Machine learning (ML) that pre-processes or "codes" incident data into the repository Statistically significant correlations • alternatively, identifying co-occurrences approaching statistical significance to continue collecting data on Named-entity recognition and other natural language processing (NLP) to analyze unstructured text associated with an incident Incorporation of external data sources • comparing trends and performing baselining • identifying potential "macro" influences (outside the organization) on insider incidents

The creation, maintenance, and analysis of incident data can quickly become a full-time role or a source of scope creep. For the successful implementation of these processes, the organization should identify and assign someone to the role of incident repository project manager. This position can be full time or part time and should have the following responsibilities:

- Define the scope for what will and will not be included in the repository, both in terms of incidents generally and data points (e.g., fields) specifically.
- Collaborate on requirements and use cases.
- Acquire and allocate a budget for activities.
- Decide on standards and procedures to be leveraged when developing and maintaining the repository, and if necessary, a ***data dictionary***.
- Identify potential stakeholders.
- Identify the knowledge, skills, and abilities (KSAs) needed for the various roles that will interact with the repository (e.g., data entry, analysis, platform maintenance, administration).
- Ensure that the responsibilities for maintenance, analysis, and updates of the repository are assigned to the appropriate individuals.
- Develop documentation for data collection, incident data curation, and analysis.
- Establish a plan and process for change management.
- Set expectations for ongoing repository stewardship and updates.

Protective Measure—Engage in Information Sharing

Sharing insider incident information not only improves the insights of an individual organization, it also helps to more generally improve insider risk management and operational resilience. Information sharing can be done informally through industry connections or in a more organized manner by participating in information-sharing groups, which has several benefits, including the following:

- The organization establishes formal agreements concerning how the data may be used and shared further.
- The organization receives timely and relevant information on a regular basis.
- The information the organization (typically) receives is in structured or standardized forms.
- Engagement with the organization's industry or insider threat community allows opportunities to "give back."

In addition to incident data, information-sharing groups can be a source of best practices and other relevant information, such as experiences with specific tools or techniques, or challenges and solutions related to regulatory compliance. Information-sharing groups provide information that is relevant to IRMPs and other parts of the organization (e.g., supply chain security management).

Engagement with information-sharing groups can also help the organization stay attuned to potential changes in its environment, which data sources to monitor, and useful tool configurations. Information-sharing groups, especially those that are free or low cost, can have a good return on investment for the organization in terms of securing best practices for resource management instead of figuring them out alone.

The organization should consider joining several types of information-sharing groups, including geographically focused (e.g., national, state, local, international), sector-specific, and formal collaborative structures. The most notable of these groups are the Information Sharing and Analysis Organizations Standards Organization (ISAO SO) and the Global Resilience Federation.

Table 6: **ISACs vs. ISAOs**

INFORMATION SHARING AND ANALYSIS CENTERS (ISACS)	INFORMATION SHARING AND ANALYSIS ORGANIZATIONS (ISAOS)
They apply to critical infrastructure/key resources (CI/KRs). They conduct bidirectional sharing with government and industry (in theory). Many work within the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The National Council of ISACs has 21 of the 33 sector-specific ISACs.	They were established by Executive Order (EO) 13691 [Obama 2015]. They are private sector (original intent) organizations. • While some can fall within CI/KR (i.e., could reflect a subsector), they are not obligated to share with government or other ISAOs. • Many still work with Cyber Information Sharing and Collaboration Program (CISCP), Automated Indicator Sharing (AIS), Enhanced Cybersecurity Services (ECS), and CISA Integrated Operations Coordination Center (CIOCC). ISAO SO provides documentation and guidance. • Many geographically based groups use the term *ISAO*.

There are other information-sharing groups where member organizations rely on a similar resource, vendor, or supply stream. These organizations join together to address issues that can affect their bottom line. Perhaps the most common kind of informal group is one that focuses on a common interest. Different options exist for organizations that are interested in engaging around the topic of insider threat.

The Software Engineering Institute (SEI) operates the Open Source Insider Threat (OSIT) information sharing group, an industry-only group that focuses on vendor-free discussions about policies, procedures, tools, and analytic techniques. The Intelligence National Security Alliance (INSA)[40] manages an Insider Threat Subcommittee that includes representation from public and private sectors. For organizations considering workplace violence as an insider risk use case, the Association for Threat Assessment Professionals (ATAP)[41] is a valuable resource.

Challenges

The organization can face the following challenges when implementing this best practice:

1. **Hesitating to share information**—Insider incident information is often viewed as highly sensitive, and decision makers might be hesitant to share relevant information, even internally. Good data anonymization, nondisclosure agreements (NDAs), and terms of use can help alleviate some of the hesitancy.[42]
2. **Conforming with data regulations**—Some environments must consider protected information, such as PII or United States (U.S.) security classified data or systems, which can limit what and to whom information related to incidents involving that data or those systems can be shared. The organization must ensure that data related to incidents that involve protected ***assets*** requires the involvement of legal counsel and ethics and compliance teams.
3. **Obtaining the needed support**—Maintaining an insider threat incident repository and engaging in information sharing requires support in the form of (1) time to participate and (2) funding for effort, tools, and fees. While there are free options for both information-related tools and information-sharing groups, they still require workforce resources to attend and consequently require financial support.
4. **Recognizing the limits of insight from the past**—Information about past incidents cannot provide all the insight an organization needs for its IRMP. Even robust incident repositories and incident sharing have limits in both the breadth and depth of detail from global or even internal sets of insider incidents. The information available is limited to incidents that were both detected and that could be effectively investigated (e.g., where investigators could learn

[40] Learn more about INSA at **https://www.insaonline.org**.

[41] Learn more about ATAP at **https://www.atapworldwide.org**.

[42] For more in-depth guidance on participating in information sharing, see the National Institute of Standards and Technology's (NIST's) *Guide to Cyber Threat Information Sharing* (**https://csrc.nist.gov/publications/detail/sp/800-150/final**) **[NIST 2016]**.

the answers to how, why, and to what effect). The answers to these questions are highly dependent on the tools and data available for analysis as well as the skills (e.g., analysis skills, the ability to communicate relevant findings) of those investigating the incident. Both incident repositories and information sharing can help lessen the number of items in the "you don't know what you don't know" category; they cannot eliminate that problem.

The claim made by this best practice is that establishing an insider threat incident repository improves the organization's insider risk management, its ability to respond to insider threat, and its awareness and training programs. In contrast to the case studies described in other practices, which focus on example insider compromises that occur when the practice is not implemented, and similar to the case studies in **Best Practice 21**, these case studies describe evidence that reflects the benefits of maintaining and sharing insider incident information.

CASE STUDY: COLLABORATE TO LEARN ABOUT THREATS

A 2019 Ponemon Institute report presents survey results related to the value of shared threat intelligence [Ponemon 2019]. From the survey results, 61% of respondents believe that a benefit of participating in an ISAC/ISAO (e.g., information-sharing organization) is the ability to learn about threats affecting similar organizations. Of the respondents, 57% believe that collaboration is a benefit.

CASE STUDY: SHARING TO PREVENT INCIDENTS

The College of Emergency Preparedness, Homeland Security, and Cybersecurity at the State University of New York at Albany continually collects success stories related to information sharing. In 2020, it released a report that includes examples where information sharing, both formal and informal, helped to prevent or detect incidents [Turetsky 2020]. For example, the second success story (Cozy Bear and a Financial Institution) describes how information sharing on a community forum allowed an institute to detect a spear-phishing email message before the recipient opened it. This detection prevented an inadvertent insider risk incident.

CASE STUDY: INTEGRATED DATA CAPTURE TO LEARN MORE

In his master's thesis, Andrew Baze proposes a tagging method for documenting lessons learned information within a case-tracking system [Baze 2021]. During a three-month case study, he illustrated how changes in policies and making capturing data an integrated part of case management (as opposed to something done at the end of a case) increased the amount of lessons-learned data collected and the corresponding changes or training they implied.

Quick Wins and High-Impact Solutions

All Organizations

The recommendations in this subsection apply to all organizations.

- ☑ Collect case studies from inside your organization or industry to use in workforce awareness and training.
- ☑ Clarify goals for information sharing (e.g., how it fits into your organization's overall information security, situational awareness, or IRMP strategy).
- ☑ Dedicate time and resources for your organization to participate in information-sharing groups.
- ☑ Incorporate information sharing (whether with external partners or forums) into your organization's incident response process.

Mapping to Standards

STANDARDS	MAPPINGS
NIST SP 800-53 Rev. 5	IR-4 Incident Handling PM-16 Threat Awareness Program RA-3 Risk Assessment
NIST CSF	DE DP ID RA ID RM ID SC PR AT PR IP RS AN RS CO RC IM RS MI
NIST Privacy Framework	
NITTF Maturity Framework	ME-2 ME-9 ME-10 ME-16
National Minimum Standards	G-1
CERT-RMM	Communications Risk Management
ISO 27002	
CIS v7	Control 17 Control 19 Control 20
GDPR	

APPENDICES

APPENDIX A

Glossary

Assets
The raw materials that services need to operate, falling into the categories of people, information, technology, and facilities [Caralli 2016]

Backdoor
A secret way to take control of a computer [PC Magazine 2021]

Change Controls
Security controls that ensure the accuracy, integrity, and authorization of all changes made to computer and network systems by ensuring that all changes are documented and approved by all appropriate stakeholders

Cloud Computing
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 2011]

Community Clouds
Cloud computing service typically consisting of several organizations that have the same needs [GAO 2010]

Connectedness at Work
The extent to which workforce members want to interact with, trust, and feel close to the people they work with [Moore 2016]

Critical Asset
The organizational resources essential to maintaining operations and achieving the organization's mission [CISA 2021c]

Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed

Data Dictionary
Documentation describing data sources and the data fields they contain

Data Protection Impact Assessments (DPIA)
A process required under the [General Data Protection Regulation] GDPR that identifies and assesses data protection risks [ICO 2021a]

Data Subject
A living individual to whom personal data relates [CSRC-NIST 2021]

Detective Monitoring
Continual observation to identify a target observable or indicator

Deterrence Theory
Theory that people obey rules because they fear getting caught and being punished

Digital Access Log
A chronological record of information system access in a given period

Enhanced Monitoring
Monitoring that is implemented beyond the baseline of the organization to mitigate increased risk due to role, position, or observed behavior

Hybrid Clouds
Two or more clouds (private, community, or public) that are connected

Insider
Individual who has or had authorized access to an organization's critical assets

Insider Risk
The impact and likelihood associated with the realization of an insider threat

Insider Risk Management Program (IRMP)
A designated set of capabilities and resources purposefully allocated to mitigate insider threat and manage insider risk

Insider Threat
The potential for an individual who has or had authorized access to an organization's critical assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization

Insider Threat Actor (or Insider)
Individual who has or had authorized access to an organization's critical assets

Insider Threat Behavior
Measurable and detectable sequences of events that relate to a known or suspected insider threat scenario

Insider Threat Scenario
Sequences of events by which an insider threat actor could negatively affect the organization

Intellectual Property (IP)
Broad reference to "intangible creations of the mind—inventions, literary and artistic works, unique business names and symbols, and internal secret information [Gross 2014]

Intrusion Detection System (IDS)
A security service that monitors and analyzes network or system events for the purpose of finding and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner

Intrusion Prevention System (IPS)
A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets [NIST 2015c]

Job Engagement
The extent to which workforce members are excited and absorbed by their work [Moore 2016]

Jump Box
A system on a network used to access and manage devices in a separate security zone that is hardened and monitored to provide a controlled means of access between two dissimilar security zones; sometimes referred to as a *jump server* or *jump host* [Wikipedia 2021]

Least Privilege
A security principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges) to the minimum necessary to perform their jobs[43]

Logic Bomb
A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met [CSRC-NIST 2021]

Malicious Insider
An insider threat actor who has intent to harm

Multifactor Authentication (MFA)
Using two or more authentication methods of different types (e.g., passwords and tokens) to verify a user's identity [CISA 2021b]

[43] NIST SP 800-57 Part 2, under Least privilege (**https://doi.org/10.6028/NIST.SP.800-57p2**) [archived]

Network Enclave
An information system environment that is end-to-end under the control of a single authority and that has a uniform security policy, including personnel and physical security [Gezelter 2002]

Non-Repudiation
Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information [CSRC-NIST 2021]

Non-Technical Observables
Inferences from a socio-behavioral data source that reflect a measurable phenomenon (Non-technical observables can be filtered and analyzed to identify potential risk indicators [PRIs].)

Operational Resilience
The ability of an organization to continue to carry out its mission in the presence of operational stress and disruption

Perceived Organizational Support
The extent to which workforce members believe their organization values their contributions, cares about their well-being, supports their socio-emotional needs, and treats them fairly [Eisenberger 2011]

Positive Incentives
Workforce management practices that increase perceived organizational support because they attempt to entice (rather than force) a workforce member to act in the interests of the organization [Moore 2016]

Potential Risk Indicators (PRIs)
Inferences from non-technical and technical observables that reflect a measurable and detectable phenomenon (PRIs can be aggregated and analyzed to identify evidence of insider threat behavior.) [Moore 2016]

Privacy Impact Assessments (PIAs)
A process that evaluates how information is handled to ensure the handling conforms to applicable legal, regulatory, and policy requirements regarding privacy [CSRC-NIST 2021]

Private Clouds
Cloud computing services that are operated by the organization itself or by another entity on behalf of the organization [GAO 2010]

Privileged User
A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform [CSRC-NIST 2021]

Public Clouds
Cloud computing service open to any customers, who often have diverse needs [GAO 2010]

Remote Workforce Members
Teleworkers, remote workers, or any workforce member not working at the physical facility

Right to Erasure (i.e., Right to Be Forgotten)
The right of individuals to have their personal data erased [ICO 2021b]

Security Controls
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 2015a]

Service-Based Inventory
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, etc.

Social Engineering
Using deception to manipulate others into disclosing personal or confidential information, such as passwords, access to personal computers, and bank information [CSRC-NIST 2021]

Technical Observables
Inferences from an information technology (e.g., application logs, mobile device logs, VPN logs) data source that reflect a measurable phenomenon (Technical observables can be filtered and analyzed to identify PRIs.) [Greitzer 2009]

Threat
A negative impact that could potentially occur

Threat Scenario
An event that could result in a specific harm to an organization or its assets [CSRC-NIST 2021]

Threat Scenario Impact
Measure of direct and indirect costs associated from recovering from the potential loss and for returning to the pre-incident state [CSRC-NIST 2021]

Trusted External Entity (TEE)
External entities (i.e., not direct employees of the organization) who are given authorized access to the organization's critical assets

Two-Person Rule
Policy requiring the presence of at least two authorized persons who are capable of detecting incorrect or unauthorized procedures with respect to the task to be performed [USLegal 2021]

Workforce/Workforce Member
A human person that formerly had or currently has authorized access to an organization's critical assets (The nature of the relationship is generally categorized as an employee, contractor, consultant, or trusted external entity.)

Zero-Day Exploits
Exploits that have never been seen before

APPENDIX B

Acronyms

ACL—Access Control List

ADM—Asset Definition and Management

AfriNIC—African Network Information Centre

AI—Artificial Intelligence

AIS—Automated Indicator Sharing

APNIC—Asia Pacific Network Information Centre

ARIN—American Registry for Internet Numbers

ATAP—Association for Threat Assessment Professionals

AUP—Acceptable Use Policy

C2M2—Cybersecurity Capability Maturity Model

CAO—Chief Administrative Officer

CCPA—California Consumer Privacy Act

CD—Compact Disk

CD-RW—Compact Disc-Rewritable

CEO—Chief Executive Officer

CERT-RMM—CERT Resilience Management Model

CFO—Chief Financial Officer

CI/KR—Critical Infrastructure/Key Resources

CIO—Chief Information Officer

CIOCC—CISA Integrated Operations Coordination Center

CIS—Center for Internet Security

CISA—Cybersecurity and Infrastructure Security Agency

CISCP—Cyber Information Sharing and Collaboration Program

CISO—Chief Information Security Officer

CMMC—Cybersecurity Maturity Model Certification

CMU—Carnegie Mellon University

COO—Chief Operating Officer

CRO—Chief Revenue Officer

CRO—Chief Risk Officer

CSA—Cloud Security Alliance

CSF—Cyber Security Framework

CSIRT—Computer Security Incident Response Team

CSO—Chief Security Officer

CSRC—Computer Security Resource Center

CTO—Chief Technical Officer

DARPA—Defense Advanced Research Projects Agency

DBA—Database Administrator

DDoS—Distributed Denial of Service

DHS—Department of Homeland Security

DLP—Data Loss Prevention

DMV—Department of Motor Vehicles

DNS—Domain Name System

DoS—Denial of Service

DPIA—Data Protection Impact Assessment

DPO—Data Protection Officer

DVD—Digital Video Disc

DVD-RW—DVD-Rewritable

EAP—Employee Assistance Program

EDM—External Dependencies Management

EEOC—Equal Employment Opportunity Commission

EO—Executive Order

ERM—Enterprise Risk Management

EU—European Union

FBI—Federal Bureau of Investigation

FIPS—Federal Information Processing Standards

FTP—File Transfer Protocol

GAO—Government Accountability Office

GDPR—General Data Protection Regulation

HC—Human Capital

HR—Human Resources

HVAC—Heating, Ventilation, and Air Conditioning

IA—Information Assurance

IDPS—Intrusion Detection and Prevention Systems

IDS—Intrusion Detection System

INSA—Intelligence National Security Alliance

InTP—Insider Threat Program

IP—Intellectual Property

IP—Internet Protocol

IPS—Intrusion Prevention System

IRMP—Insider Risk Management Program

ISAC—Information Sharing and Analysis Center

ISAO—Information Sharing and Analysis Organization

ISO—International Organization for Standardization

ISP—Internet Service Provider

ISSO—Information Systems Security Officer

IT—Information Technology

ITPE—Insider Threat Program Evaluator

ITPM—Insider Threat Program Manager

ITVA—Insider Threat Vulnerability Assessor

KSA—Knowledge, Skills, and Abilities

LACNIC—Latin America and the Caribbean

LDAP—Lightweight Directory Access Protocol

M&A—Measurement and Analysis

M&A—Mergers and Acquisitions

MDM—Mobile Device Management

MFA—Multifactor Authentication

ML—Machine Learning

MOA—Memoranda of Agreement

NDA—Nondisclosure Agreement

NISPOM—National Industrial Security Program Operating Manual

NIST—National Institute of Standards and Technology

NITTF—National Insider Threat Task Force

NLP—Natural Language Processing

NLRB—National Labor Relations Board

OCTAVE—Operationally Critical Threat, Asset, and Vulnerability Evaluation

OMB—Office of Management and Budget

OPSEC—Operational Security

OSHA—Occupational Safety and Health Act

OSIT—Open Source Insider Threat (information sharing group)

PDF—Portable Document Format

PGP—Pretty Good Privacy

PIA—Privacy Impact Assessment

PII—Personally Identifiable Information

PRI—Potential Risk Indicator

RFC—Request for Comments

RIPE—Reseaux IP Européens

RIPE NCC—RIPE Network Coordination Centre

SaaS—Software as a Service

SAN—Storage Area Network

SAPM—Shared Account Password Management

SCP—Secure Copy Protocol

SEI—Software Engineering Institute

SFTP—SSH File Transfer Protocol

SIEM—Security Information and Event Management

SLA—Service Level Agreement

SME—Subject Matter Expert

SMTP—Simple Mail Transfer Protocol

SO—Standards Organization

SOC—Security Operations Center

SP—Special Publication

SSH—Secure Shell

SSL—Secure Sockets Layer

SSN—Social Security Number

TEE—Trusted External Entity

U.S.—United States

UAM—User Activity Monitoring

USB—Universal Serial Bus

USDA—United States Department of Agriculture

USSS—United States Secret Service

VPN—Virtual Private Network

APPENDIX C

Bibliography

URLs are valid as of August 2021.

[Alberts 2004]
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. **https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153**

[Ariani 2013]
Ariani, Dorothea Wahyu. The Relationship between Employee Engagement, Organizational Citizenship Behavior, and Counterproductive Work Behavior. *International Journal of Business Administration*. Volume 4. Number 2. 2013.

[AXELOS 2015]
AXELOS. *What Is ITIL?* AXELOS Information Technology Infrastructure Library. 2015. **https://www.axelos.com/best-practice-solutions/itil/what-is-itil**

[Baze 2021]
Baze, Andrew. *Improving Incident Response Through Simplified Lessons Learned Data Capture*. SANS Institute. February 2021. **https://www.sans.org/white-papers/40145/**

[Bishop 2010]
Bishop, Dave. *Step-By-Step Guide to Controlling Device Installation Using Group Policy*. May 2010. **http://msdn.microsoft.com/en-us/library/bb530324.aspx**

[Brien 2012]
Brien, M.; Forest, J.; Mageau, G. A.; Boudrias, J.; Desrumaux, P.; Brunet, L.; & Morin, E. M. The Basic Psychological Needs at Work Scale: Measurement Invariance between Canada and France. *Applied Psychology: Health and Well-Being*. Volume 4. Number 2. July 1, 2012. Page 167. **https://iaap-journals.onlinelibrary.wiley.com/doi/full/10.1111/j.1758-0854.2012.01067.x**

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

[BSI Group 2015]
British Standards Institute. 2015. **http://www.bsigroup.com**

[Buckingham 2010]
Buckingham, M. *Go Put Your Strengths to Work: 6 Powerful Steps to Achieve Outstanding Performance*. Simon and Schuster. 2010. **https://www.simonandschuster.com/books/Go-Put-Your-Strengths-to-Work/Marcus-Buckingham/9780743261685**

[Butler 2009]
Butler, J. Michael. *Benchmarking Security Information Event Management (SIEM)*. SANS. February 2009.

[Caralli 2016]
Caralli, Richard; Allen, Julia; Curtis, Pamela; White, David; & Young, Lisa. *CERT Resilience Management Model (CERT-RMM), Version 1.2*. Software Engineering Institute, Carnegie Mellon University. 2016. **http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=508084**

[CIS 2021]
Center for Internet Security (CIS). *CIS Controls v7.1*. August 2021 [accessed]. **https://www.cisecurity.org/controls/v7**

[CISA 2021a]
Cybersecurity & Infrastructure Security Agency. *CRR Supplemental Resource Guide: Volume 8 External Dependencies Management*. Retrieved from CRR Supplemental Resource Guides. July 2021[accessed]. **https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-EDM_0.pdf**

[CISA 2021b]
Cybersecurity & Infrastructure Security Agency. *Multi-Factor Authentication (MFA)*. August 2021 [accessed]. **https://www.cisa.gov/publication/multi-factor-authentication-mfa**

[CISA 2021c]
Cybersecurity & Infrastructure Security Agency. *What Is a Critical Asset?* August 2021 [accessed]. **https://www.cisa.gov/rbps-12-personnel-surety**

[CISCO 2012]
CISCO. Supplier Information: Diversity Business Practices. 2015. **http://www.cisco.com/c/en/about/supplier-information.html**

[CISWG 2005]
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.

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

[Conway 2005]
Conway, Tara; Keverline, Susan; Keeney, Michelle; Kowalski, Eileen; Williams, Megan; Cappelli, Dawn; Moore, Andrew P.; Rogers, Stephanie; Shimeall, Timothy J. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. May 2005. **https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=51934**

[Costa 2017]
Costa, Dan. CERT Definition of 'Insider Threat'—Updated [blog post]. *SEI Blog*. March 2017. **https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/**

[CSA 2010]
Cloud Security Alliance. *Top Threats to Cloud Computing, Version 1.0*. 2010.

[CSO Magazine 2017]
CSO Magazine. *State of Cybercrime 2017: Security Events Decline, but Not the Impact*. 2017. **https://www.csoonline.com/article/3211491/security/state-of-cybercrime-2017-security-events-decline-but-not-the-impact.html**

[CSRC-NIST 2021]
Computer Security Resource Center, NIST. Glossary. August 2021 [accessed]. **https://csrc.nist.gov/glossary/**

[DARPA 2004]
Defense Advanced Research Projects Agency. *The Grand Challeng*e. 2004. **https://www.darpa.mil/about-us/timeline/-grand-challenge-for-autonomous-vehicles**

[Deloitte 2021]
Deloitte. *Managing Potential Insider Threat During COVID-19*. August 2021 [accessed]. **https://www2.deloitte.com/us/en/pages/public-sector/articles/managing-potential-insider-threat-during-covid-19.html**

[Deschenaux 2012]
Deschenaux, Joanne. Maryland Enacts Country's First Social Media Password Law [blog post]. *The SHRM Blog*. 2012. **https://blog.shrm.org/public-policy/maryland-enacts-countrys-first-social-media-password-law**

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

[DHS 2021]
Department of Homeland Security (DHS). *Security of Cloud-Based Systems*. August 2021 [accessed]. **https://www.dhs.gov/science-and-technology/csd-cloud**

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

[Eisenberger 1986]
Eisenberger, R.; Huntington, R.; Hutchison, S.; & Sowa, D. Perceived Organizational Support. *Journal of Applied Psychology*. Volume 71. Number 3. 1986. Page 500.

[Eisenberger 2011]
Eisenberger, R. & Stinglhamber, F. ***Perceived Organizational Support: Fostering Enthusiastic and Productive Employees***. American Psychological Association. 2011. **https://psycnet.apa.org/record/2010-19901-000**

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

[FIPS 2004]
Federal Information Processing Standards Publication. ***Standards for Security Categorization of Federal Information and Information Systems***. FIPS PUB 199. February 2004. **http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf**

[Gallup 2013]
Gallup. State of the American Workplace: Employee Engagement Insights for U.S. Business Leaders. 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**

[GDPR 2021]
General Data Protection Regulation, European Union. *Data Protection Impact Assessment*. July 2021 [accessed]. **https://www.privacy-regulation.eu/en/article-35-data-protection-impact-assessment-GDPR.htm**

[Gezelter 2002]
Gezelter, Robert. Mobile Code. In *Computer Security Handbook, 4th Edition*. 2002.

[Greitzer 2009]
Greitzer, Frank L.; Paulson, Patrick R.; Kangas, Lars J.; Franklin, Lyndsey R.; Edgar, Thomas W.; & Frincke, Deborah A. ***Predictive Modeling for Insider Threat Mitigation***. United States Department of Energy. April 2009.

[Grim 2014]
Grim, Lawrence. *IDS: File Integrity Checking*. August 2014. **https://www.sans.org/white-papers/35327/**

[Gross 2014]
Gross, Charlene. *Development of an Intellectual Property Strategy: Research Notes to Support Department of Defense Programs*. CMU/SEI-2014-SR-036. Software Engineering Institute, Carnegie Mellon University. **https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=311938**

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

[Hanley 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. **https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9807**

[Hanley 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. **https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9875**

[Hurlburt 2011]
Hurlburt, G.; Voas, J.; & Miller, K. W. MobileApp Addiction: Threat to Security? *IT Professional*. Volume 13. Number 6. January-February 2011. Pages 9-11. **https://doi.org/10.1109/MITP.2011.104**

[ICO 2021a]
Information Commissioner's Office. *Data Protection Impact Assessments*. August 2021 [accessed]. **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/**

[ICO 2021b]
Information Commissioner's Office. *Right to Erasure*. August 2021 [accessed]. **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/**

[Infosecurity 2010]
Infosecurity. Air Force's Banning of Thumb Drives Temporary Solution to WikiLeaks. *Infosecurity*. December 2010.

[INSA 2013]
Intelligence and National Security Alliance (INSA). *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector*. September 2013. **https://www.insaonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/**

[ISACA 2015]
Information Systems Audit and Control Association. 2015. **http://www.isaca.org**

[ISF 2015]
Information Security Forum. *The Standard of Good Practice*. 2015. **https://www.securityforum.org/**

[ISO 2013a]
International Organization for Standardization. *Information Technology—Security Techniques—Information Security Management Systems—Requirements*. ISO/IEC 27001:2013. **https://www.iso.org/standard/54534.html**

[ISO 2013b]
International Organization for Standardization. *Information Technology—Security Techniques—Code of Practice for Information Security Management*. ISO/IEC 27002. 2013. **https://www.iso.org/standard/54533.html**

[ISO 2014]
International Organization for Standardization. *Asset Management—Overview, Principles and Terminology*. ISO 55000. 2014. **https://www.iso.org/standard/55088.html**

[Johnson 2009]
Johnson, David J.; Takacs, Nicholas; & Hadley, Jennifer. Securing Stored Data. In *Computer Security Handbook, Fifth Edition*. 2009.

[Kessel 2021]
Kessel, Emily, Miller, Sarah, & Gardner, Carrie. Potential Implications of the California Consumer Privacy Act (CCPA) for Insider Risk Programs [blog post]. *SEI Blog*. May 2021. **https://insights.sei.cmu.edu/blog/potential-implications-of-the-california-consumer-privacy-act-ccpa-for-insider-risk-programs/**

[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.

[Malone 2012]
Malone, G. P.; Pillow, D. R.; & Osman A. The General Belongingness Scale (GBS): Assessing Achieved Belongingness. *Personality and Individual Differences*. Volume 52. Number 3. February 2012.

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

[Mell 2011]
Mell, Peter & Grance, Timothy. *The NIST Definition of Cloud Computing*. (SP 800-14). National Institute of Standards and Technology. 2011. **http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf**

[Moore 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**

[Moore 2016]
Moore, Andrew P.; Perl, Samuel J.; Cowley, Jennifer; Collins, Matthew L.; Cassidy, Tracy M.; Van-Houdnos, Nathan; Buttles-Valdez, Palma; Bauer, Daniel; Parshall, Allison; Savinda, Jeff; Monaco, Elizabeth A.; Moyes, Jaime L.; & Rousseau, Denise M. *The Critical Role of Positive Incentives for Reducing Insider Threat*. CMU/SEI-2016-TR-014. December 2016. **https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484917**

[Moore 2017]
Moore, Andrew P. Modeling the Influence of Positive Incentives on Insider Threat Risk Reduction. In *Proceedings of the International Conference of the System Dynamics Society*. July 2017.

[Moore 2018]
Andrew P.; Cassidy, Tracy M.; Theis, Michael C.; Rousseau, Denise M.; Bauer, Daniel; & Moore, Susan B. Balancing Organizational Incentives to Counter Insider Threat. In *Proceedings of the Workshop on Research for Insider Threats*. IEEE Symposium on Security and Privacy. May 2018.

[Moore 2021]
Moore, Andrew P.; Miller, Sarah; & Horneman, A. *Insider Risk Management Program Building: Summary of Insights from Practitioners*. CyLab, Carnegie Mellon University's Security and Privacy Institute. May 2021.

[NCSL 2015]
Conference of State Legislators. *Access to Social Media Usernames and Passwords*. 2015.

[NISPOM 2006]
National Industrial Security Program. *National Industry Security Program Operating Manual (NISPOM) Change 2*. DoD 5220.22-M. February 2006.

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

[NIST 2008]
National Institute of Standards and Technology. ***Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices***. SP 800-60 Vol. 2 Rev 1. 2008. **https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final**

[NIST 2009]
National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems and Organizations*. SP 800-53, Rev. 3. 2009. **https://csrc.nist.gov/publications/detail/sp/800-53/rev-3/archive/2010-05-01**

[NIST 2015a]
National Institute of Standards and Technology. ***Security and Privacy Controls for Federal Information System and Organizations***. NIST SP 800-53, Rev. 4. 2015. **https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final**

[NIST 2015b]
National Institute of Standards and Technology. *Special Publications (800 Series)*. 2015. **http://csrc.nist.gov/publications/sp800**

[NIST 2015c]
National Institute of Standards and Technology. ***Guide to Industrial Control Systems (ICS) Security***. NIST SP 800-82, Rev. 2. May 2015. **https://doi.org/10.6028/NIST.SP.800-82r2**

[NIST 2016]
National Institute of Standards and Technology. *Guide to Cyber Threat Information Sharing*. SP 800-150. October 2016. **https://csrc.nist.gov/publications/detail/sp/800-150/final**

[NIST 2018a]
National Institute of Standards and Technology. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. SP 800-37, Rev. 2.2018. **https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final**

[NIST 2018b]
National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. April 2018. **https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf**

[NIST 2020]
National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. SP800-53, Rev. 5. 2020. **https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final**

[NIST 2021a]
National Institute of Standards and Technology. *Digital Identity Guidelines*. SP-800-63B. July 2021. **https://pages.nist.gov/800-63-3/sp800-63b.html**

[NIST 2021b]
National Institute of Standards and Technology. *Privacy Framework*. July 2021 [accessed]. **https://www.nist.gov/privacy-framework**

[NITTF 2013]
National Insider Threat Task Force (NITTF). *National Insider Threat Policy*. 2013. **https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.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**

[Obama 2015]
Obama, Barack. *Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing.* The White House. Office of the Press Secretary. 2015. **https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari**

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

[PC Magazine 2021]
PC Magazine Encyclopedia. July 2021 [accessed]. **https://www.pcmag.com/encyclopedia/**

[PCI 2018]
PCI Security Standards Council. *Payment Card Industry Data Security Standard*. 2018.

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

[Ponemon 2019]
Ponemon Institute. *The Value of Threat Intelligence: Annual Study of North American and United Kingdom Companies*. 2019. **https://stratejm.com/wp-content/uploads/2019/08/2019_Ponemon_Institute-Value_of_Threat_Intelligence_Research_Report_from_Anomali.pdf**

[Ponemon 2020]
The Ponemon Institute, IBM, and Observe IT. *The Cost of Insider Threats*. 2020. **https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/?_ga=2.197333487.1717092372.1625578540-1156939784.1625578540#/**

[Ponemon 2021]
Ponemon Institute. *2021 Ponemon Report: The Cost of Cloud Compromise and Shadow IT*. 2021. **https://www.proofpoint.com/us/resources/analyst-reports/cost-of-cloud-compromise-and-shadow-it**

[Purcell 2012]
Purcell, Anne. *Report of the Acting General Counsel Concerning Social Media Cases*. OM 12-59. Office of the General Counsel. 2012.

[PWC 2015]
Deloitte. *2015 CyberSecurity Watch Survey*. 2015. **https://www2.deloitte.com/ca/en/pages/risk/articles/cybersecurity-survey-2015.html**

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

[SEI 2007]
Software Engineering Institute. *Over-Confidence Is Pervasive Amongst Security Professionals: 2007 E-Crime Watch Survey*. Software Engineering Institute, Carnegie Mellon University. 2007. **http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52340**

[SEI 2014a]
CERT Insider Threat Center. *Unintentional Insider Threats: A Foundational Study*. CMU/SEI-2013-TN-022. Software Engineering Institute, Carnegie Mellon University. 2014. **http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58744**

[SEI 2014b]
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**

[SEI 2015]
Software Engineering Institute. *Survivability and Information Assurance Curriculum (SIA)*. Software Engineering Institute, Carnegie Mellon University. 2015. **https://www.sei.cmu.edu/education-outreach/curricula/survivability-information-assurance**

[Shaw 2015]
Shaw, Eric; Sellers, Laura Application of the Critical-Path Method to Evaluate Insider Risks. *Studies in Intelligence*. Volume 59. Number 2. June 2015.

[Shin 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*. Volume 2. Number 3. December 2011. Pages 243-255.

[Shin 2012]
Shin, Dongwan; Wang, Ying; & Claycomb, William. A Policy-Based Decentralized Authorization Management Framework for Cloud Computing. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*. March 2012. ACM. 2012.

[SHRM 2021]
Society for Human Resources Management (SHRM). *Social Media Policy*. August 2021 [accessed]. **https://www.shrm.org/resourcesandtools/tools-and-samples/policies/pages/socialmediapolicy.aspx**

[Spector 2006]
P. E. Spector, S. Fox, L. M. Penney, K. Bruursema, A. Goh, and S. Kessler. The Dimensionality of Counterproductivity: Are All Counterproductive Behaviors Created Equal? *Journal of Vocational Behavior*. Volume 68. Number 3. 2006. Pages 446–60.

[Straub 1998]
D. W. Straub and R. J. Welke. Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*. 1998. Pages 441–469.

[Strozer 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 2012]
Sulea, Coralia; Virga, Delia; Maricutoiu, Laurentiu, P.; Schaufeli, Wilmar; Dumitru, Catalina Zaborila; & Sava, Florin A. Work Engagement as Mediator between Job Characteristics and Positive and Negative Extra-Role Behaviors. *Career Development International*. Volume 17. Number 3. 2012. Pages 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.ojp.gov/ncjrs/virtual-library/abstracts/prevalence-and-incidence-arrest-among-adult-males-california**

[Tucker 2020]
Tucker, Brett. *Advancing Risk Management Capability Using the OCTAVE FORTE Process*. CMU/SEI-2020-TN-002. Software Engineering Institute, Carnegie Mellon University. 2020. **http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=644636**

[Turetsky 2020]
Turetsky, David S.; Nussbaum, Brian H.; & Tatar, Unal. *Success Stories in Cybersecurity Information Sharing*. July 2020.

[USDA 2001]
United States Department of Agriculture. *The USDA Handbook on Workplace Violence Prevention and Response*. October 2001. **http://www.dm.usda.gov/workplace.pdf**

[USLegal 2021]
USLegal. *Two Person Rule Law and Legal Definition*. July 2021 [accessed]. **https://definitions.uslegal.com/t/two-person-rule/**

[Verizon 2021]
Verizon. *Data Breach Investigation Report*. 2021. **https://www.verizon.com/business/resources/reports/dbir/**

[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/**

[Wikipedia 2021]
Wikipedia. August 2021 [accessed]. **https://en.wikipedia.org/wiki/**

[Wikoff 2004]
Wikoff, Darrin. How to Effectively Manage Assets by Criticality. *ReliablePlant*. Noria Corporation. January 4, 2004. **http://www.reliableplant.com/Read/15166/manage-assets-criticality**

[Working Party 2002]
Working Party. Article 29—Data Protection Working Party. *On Surveillance and Monitoring of Electronic Communications in the Workplace*. 2002.

[Working Party 2017]
Working Party. *Opinion 2/2017 on Data Processing at Work—WP249*. 2017. **https://ec.europa.eu/newsroom/article29/items/610169**

[Wrubel 2009]
Wrubel, Jim; White, David W.; & Allen, Julia H. *High-Fidelity E-Learning: The SEI's Virtual Training Environment (VTE).* Software Engineering Institute, Carnegie Mellon University. 2009. **http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9079**

[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/**