Insider Threat Mitigation Guide

NOVEMBER 2020

Cybersecurity and Infrastructure Security Agency

[This page left intentionally blank]

Table of Contents

Letter from the Acting Assistant Director

America's critical infrastructure assets, systems, and networks, regardless of size or function, are susceptible to disruption or harm by an insider, or someone with institutional knowledge and current or prior authorized access. This status makes it possible for current or former employees, contractors, and other trusted insiders to cause significant damage. Insiders have compromised sensitive information, damaged organizational reputation, caused lost revenue, stolen intellectual property, reduced market share, and even harmed people.

Allowing America's critical infrastructure to be compromised by an insider could have a debilitating effect on the Nation's economic security, public health, or public safety. That is why it is important to understand this complicated threat, its many dimensions, and the concepts and practices needed to develop an effective insider threat program. To mitigate physical and cybersecurity threats, it is important to understand the risks posed by insiders and then build a comprehensive insider threat mitigation program that accounts for operational, legal, and regulatory considerations.

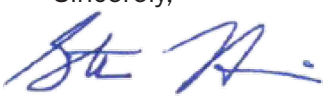
The Cybersecurity and Infrastructure Security Agency (CISA) plays an integral role in supporting public and private sector efforts to prevent and mitigate a wide range of risks, including those posed by insiders.

This *Insider Threat Mitigation Guide* is an evolution in the series of resources CISA makes available on insider threats. This *Guide* draws from the expertise of some of the most reputable experts in the field to provide comprehensive information to help federal, state, local, tribal, and territorial governments; non-governmental organizations; and the private sector establish or enhance an insider threat prevention and mitigation program. Moreover, this *Guide* accomplishes this objective in a scalable manner that considers the level of maturity and size of the organization. It also contains valuable measures for building and using effective threat management teams. Through a case study approach, this *Guide* details an actionable framework for an effective insider threat mitigation program: Defining the Threat, Detecting and Identifying the Threat, Assessing the Threat, and Managing the Threat.

On CISA.gov, visitors will find extensive tools, training, and information on the array of threats the Nation faces, including insider threats. They will also find options to help protect against and prevent an incident and steps to mitigate risks if an incident does occur. The measures you incorporate into your practices today could pay for themselves many times over by preventing an insider threat or mitigating the impacts of a successful attack in the future.

I urge you to use CISA.gov and this *Guide* to increase your own organization's security and resilience.

Sincerely,



Steve Harris
Acting Assistant Director for Infrastructure Security
Cybersecurity and Infrastructure Security Agency


Invoice

1 Introduction

Organizations of all types and sizes are vulnerable to insider threats—from family-owned small businesses to Fortune 100 corporations, local and state governments, and public infrastructure to major federal departments and agencies.

Individuals entrusted with access to or knowledge of an organization represent potential risks, and include current or former employees or any other person who has been granted access, understanding, or privilege. Trusted insiders commit intentional or unintentional disruptive or harmful acts across all infrastructure sectors and in virtually every organizational setting. These disruptions can cause significant damage (see examples below).

To combat the insider threat, organizations should consider a proactive and prevention-focused insider threat mitigation program. This approach can help an organization define specific insider threats unique to their environment, detect and identify those threats, assess their risk, and manage that risk before concerning behaviors manifest in an actual insider incident.

An effective program can protect critical assets, deter violence, counter unintentional incidents, prevent loss of revenue or intellectual property, avert sensitive data compromise, and prevent organizational reputation ruin, among many other potential harmful outcomes.

This *Insider Threat Mitigation Guide* (hereafter referred to as the *Guide*) **is designed to assist individuals, organizations, and communities in improving or establishing an insider threat mitigation program.** It offers a proven framework that can be tailored to any organization regardless of size. It provides an orientation to the concept of insider threat, the many expressions those threats can take, and offers an integrated approach necessary to mitigate the risk. The *Guide* shares best practices and key points from across the infrastructure communities

Examples of Insider Threats

- An engineer steals and sells trade secrets to a competitor
- A maintenance technician cuts network server wires and starts a fire, sabotaging operations
- An intern unknowingly installs malware
- A customer service representative downloads client contact information and emails it to a personal account for use when starting their own business
- A database administrator accesses client financial information and sells it on the dark web
- An employee brings a weapon to the office and injures or kills several of their coworkers

to assist organizations in overcoming common challenges and in establishing functional programs. It also offers case studies and statistical information to solidify the business case for establishing an insider threat mitigation program.

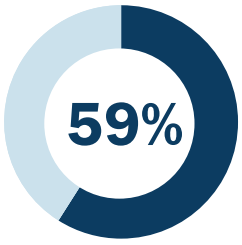
CISA recognizes that efforts to mitigate insider threats are complex. In addition, the nature of insider threats means that no two programs will be exactly alike. Flexibility and adaptability are important. The threat landscape continually evolves, technology shifts rapidly, organizations change in response to various pressures, and companies adapt to market forces. As a result, not every best practice or case study insight presented in this *Guide* will be directly applicable to every organization. Still, this *Guide* can provide value for a wide range of individuals and organizations, from the solo practitioner in a small company that requires some assistance up to and including a sizable agency that has a staff capable of operating a full complement of insider threat professionals. It offers valuable and achievable strategies, capabilities, and procedures to help organizations define their insider threats and then detect and identify, assess, and manage them in a comprehensive manner.

Ultimately, this *Guide* is designed to advance a shared, whole community approach to preparedness. Working together across infrastructure communities helps keep the Nation safe from harm and resilient when disruptions occur.

Costs of Insider Threats

Although difficult to quantify, insider threats present a complex and rapidly evolving set of challenges that organizations cannot afford to ignore. An accurate understanding of annual losses due to insider threats across all industries is elusive because of how costs are estimated and due to significant underreporting of insider threat incidents.[1] Still, the National Insider Threat Task Force (NITTF) reported that **incidents of insider threats are steadily increasing**, especially technology thefts.[2] Losses may result from physical damage to infrastructure, disruption of productivity, intellectual property theft, accidental leakage of sensitive data, or insult to an organization's reputation. Each of these may contribute to a loss of competitive advantage. Figure 1, below, presents examples of the prevalence of insider incidents across representative sectors. Figure 2 highlights potential costs that a company or organization can experience depending on the type of insider incident.

Figure 1. Insider Incidents



of surveyed **healthcare** organizations reported an insider incident in 2018[3]

Workforce-related insider disruptions:

3 per week

156 per year

were reported by surveyed **IT industry** organizations in 2019[4]

Global insider data breaches[5]

47% breaches

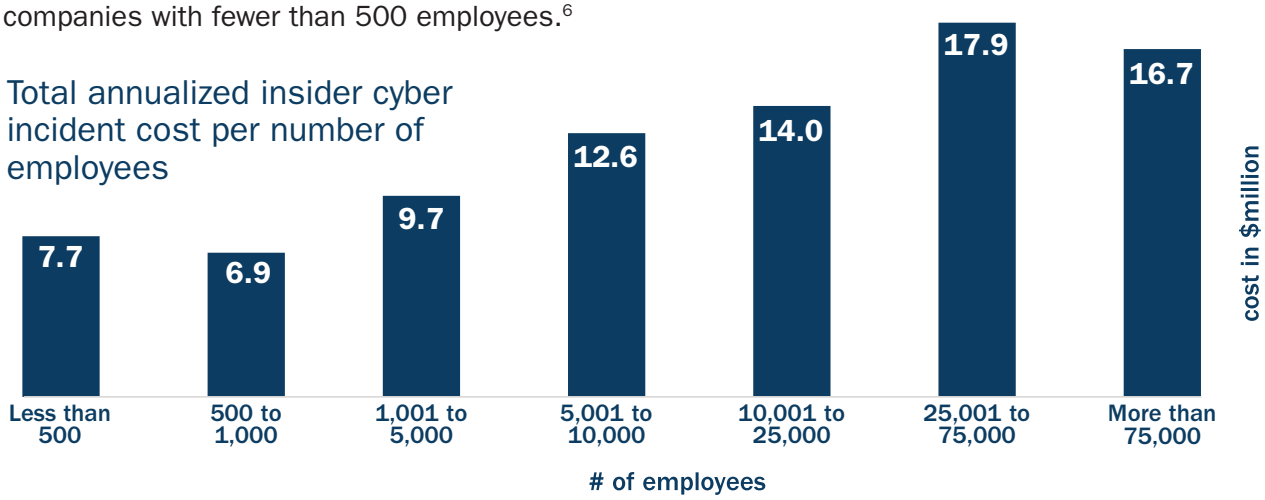
31% cost

[1]National Insider Threat Task Force. (2016). Protect Your Organization from the Inside Out: Government Best Practices. (p. 3). Retrieved from https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf
[2]National Insider Threat Task Force. (2016). Protect Your Organization from the Inside Out: Government Best Practices. (p. 6). Retrieved from https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf
[3]Verizon. (2019). 2019 Data Breach Investigations Report. (p. 44). Retrieved from https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[4]Endera. (2019). Security Executives on the Future of Insider Threat Management. Retrieved from https://endera.com/futureofinsiderthreatmanagement2019?utm_source=website&utm_medium=referral&utm_campaign=phase2 or https://endera.com/resources/
[5]ObserveIT. (2020). 2020 Cost of Insider Threats Global Report. Retrieved from https://www.observeit.com/wp-content/uploads/2020/06/The-Hidden-Costs-of-Insider-Threats-in-this-New-Infographic.pdf

Figure 2. The Costs of Insider Threats

Incident Cost

Insider threats represent a credible risk and potentially unaffordable cost for any organization, regardless of size. The financial impact on organizations can be devastating, especially for companies with fewer than 500 employees.[6]



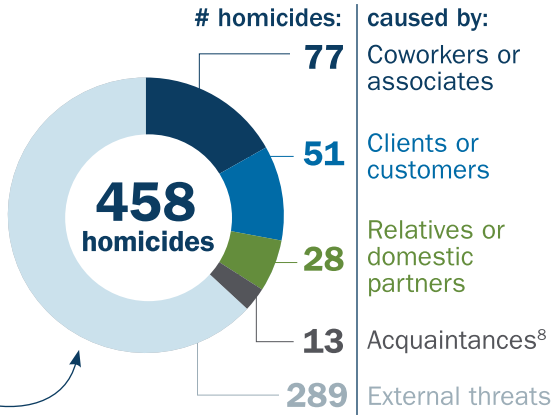
Safety

Workplace violence:

2 million people each year are directly impacted by the physical aspects

$130 billion annual financial impact[7]

In 2019, workplace violence resulted in **18,370 assaults** including



Financial Impact on Company/Organization

Research shows that there are significant financial impacts on companies and organizations when violence enters the workplace. Each occurrence of workplace violence can result in:

50% in productivity for the organization

20-40% in employee turnover following an incident

$500,000 average out-of-court settlement

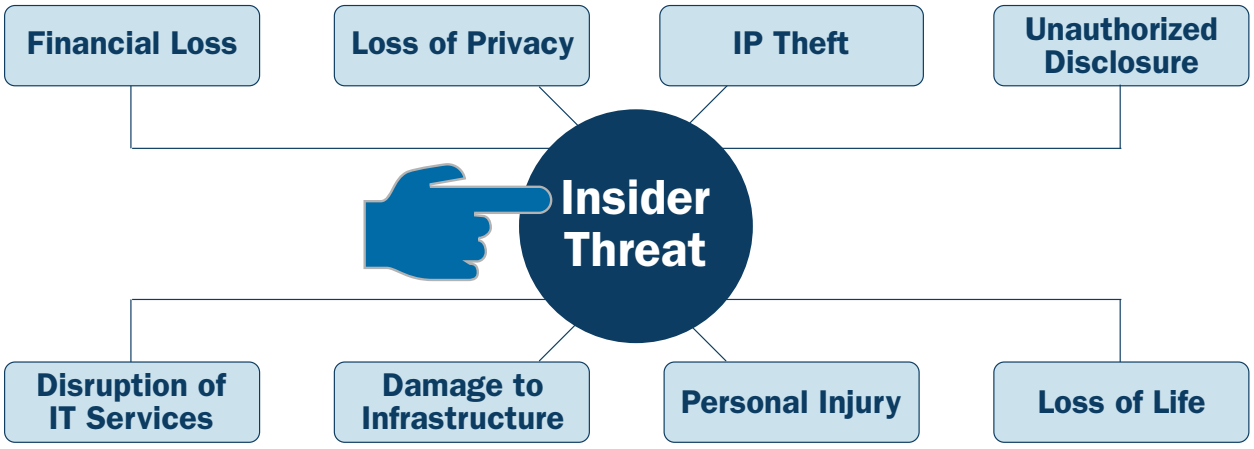
$3 million average jury award for a lawsuit[9]

[6]ObserveIT. (2020). 2020 Cost of Insider Threats Global Report. IBM Security. Retrieved from https://www.observeit.com/2020costofinsiderthreat/
[7]Ricci, D. (2018). Workplace Violence Statistics 2018: A Growing Problem. AlertFind. Retrieved from https://alertfind.com/workplace-violence-statistics/
[8]U.S. Bureau of Labor Statistics. (2019). Fact Sheet | Workplace homicides in 2019 | Injuries, Illnesses, and Fatalities. Retrieved from https://www.bls.gov/iif/oshwc/cfoi/workplace-homicides-2017.htm
[9]Frederickson, D. (n.d.). The Financial Impact of Workplace Violence. (p. 2). Workplace Violence 911. Retrieved from http://www.workplaceviolence911.com/docs/FinancialImpactofWV.pdf

Despite the significant costs associated with an insider incident, and a strong value proposition for actively working to manage this threat, many organizations have no formal insider threat program in place.[10] As demonstrated in figure 3, the consequences associated with insider threat risk are pervasive.

Beyond the financial ramifications of an insider incident, every organization has a duty to care for its members. Organizations have a responsibility to ensure that their members and those who visit or patronize their organization or business are safe. This mandate to protect members and associates from unnecessary risk of physical or virtual harm applies whether an organization's members are centrally located, mobile, or regionally, nationally, or internationally dispersed.

Figure 3. Potential Consequences of an Insider Incident



Return on Investment for Insider Threat Mitigation Programs

Typically, the cost of managing an insider incident and the recovery afterward is significantly higher than the cost of establishing and maintaining an insider threat program in the first place. **Organizations that create or enhance an insider threat mitigation program will see a return on investment (ROI)**, both intangible and tangible. ROI will be seen in the:

- Bolstering of existing security measures
- Increased number of security-minded employees or members
- Increased culture of shared responsibility and asset protection
- Early identification of threats
- Reduced time to detect threats
- Protection of organizational reputation
- Increased client approval

[10]Veriato. (n.d.). 2019 Insider Threat Program Maturity Model Report. Retrieved from https://cdn2.hubspot.net/hubfs/5260286/PDFs/Whitepapers/insider-threat-maturity-report-2019.pdf

Admittedly, some mitigation measures are cost prohibitive and projected cost savings may be a significant determinant of an insider threat mitigation program's ROI. A 2019 Ponemon Institute report concluded that organizations with active threat management programs in place averaged a cost savings of $1.2 million per incident prevented.[11]

Insider Threat Mitigation Program

What does such a program look like? An **insider threat mitigation program spans the entire organization** and should serve as a mechanism to help individuals, rather than an aggressive enforcement or a "gotcha" program. Insider threat programs should **encourage and incentivize correct behavior** with training and awareness, policy and procedure, and management practices that guide employees to act in the interest and benefit of the organization. Insider threat programs should also **deter, detect, and prevent people from wrongdoing**. When insiders do commit harmful acts—e.g., sabotage, theft, espionage, or physical harm—an insider threat program should **mitigate the impact(s) of the insider act** through appropriate management or enforcement actions. As such, it is important for organizations to balance focus, policy, processes, and messaging.

Effective Insider Threat Mitigation Programs

Tailor their insider threat program and risk appetite to the organization's unique mission, culture, critical assets, and threat landscape.

Build a culture of reporting and prevention that establishes and reinforces a positive statement of an organization's investment in the well-being of its people, as well as its overall resilience and operational effectiveness.

Employ multi-disciplinary capabilities that are enabled by technologies and/or dedicated personnel based on the organization's type, size, culture, nature, business value, and risk tolerance to acts of malicious, negligent, or unintentional insiders.

Apply the framework of detect and identify, assess, and manage for the prevention of, protection against, and mitigation of insider threats.

Establish a protective and supportive culture, protect civil liberties, and maintain confidentiality.

Assist organizations in providing a safe, non-threatening environment where individuals who might pose a threat are identified and helped before their actions can cause harm.

[11]Ponemon Institute & IBM Security. (2019). Cost of a Data Breach Report. Retrieved from https://www.ibm.com/security/data-breach

Elements of Successful Insider Threat Mitigation Programs

1. **Principles and standards that align the program with the culture and business of an organization** and describe its purpose, goals, and objectives
2. **A prioritized list of critical assets, both physical and intellectual**, that are essential to the operation or business of an organization and whose compromise, damage, or loss can have an adverse impact on its mission
3. **Definitions of the most significant and prevalent threats** and how they could affect the organization's critical assets
4. **Means to detect and identify indicators** of potential risks
5. An **Incident Response Plan** in case of an insider threat incident
6. A **committee of stakeholders** for program governance and leadership
7. An **organizational culture that encourages and provides a means of reporting**; where reporting potential threats, indicators, or concerns to a responsible party is a reasonable expectation and confidentiality is maintained
8. A **central information hub** for the collection, integration, analysis, and storage of all elements pertaining to insider threats
9. A **threat management team** for the assessment, response, and management of potential insider threats
10. An **insider threat training and awareness program** teaching the importance of identifying and reporting potential threats and how the individual is the first line of defense in protecting the organization

About this *Guide*

The recommended approaches and best practices described in this *Guide* are presented as options for consideration when developing an insider threat mitigation program; they are not definitive, applicable in all circumstances, or required by any law or regulation. Federal, state, local, tribal, and territorial governments, non-governmental and social organizations, and the private sector may at their sole discretion implement any or all of these options as considered applicable. This *Guide* is not intended to and does not create any legal rights or claims. CISA will not take any action against an entity or company that chooses not to implement these options for consideration.

Case Study

The Cost of an Insider Threat

In 2011, an American energy technology company specializing in the design and manufacture of power systems was the victim of a theft of its proprietary code by a foreign competitor. The insider threat came from the American corporation's head of automation engineering, who was convinced by two foreign competitor employees to join their organization. The insider stole product source code by secretly downloading it from a company computer.

The foreign company's market share was the second largest in the world, and it is now estimated by authorities that 20 percent of the global product operates on this stolen software. It was not until 2018 that a U.S. federal jury finally found the foreign company guilty of stealing trade secrets. According to evidence at trial, the American company suffered severe financial hardship, **losing more than $1 billion in shareholder equity and almost 700 jobs**, over half its global workforce. While the American company won a judgment in federal court, it was a hollow victory, with the judge ordering the foreign company to pay only $59 million for the theft, far short of the loss suffered.

2 Defining Insider Threats

Insider threats exist because organizations grant trust and access to individuals. Organizations rely on insiders to perform every function—from the most basic to the most sensitive functions—of a business. Understanding insider threats requires organizations to understand what constitutes an insider, and how that insider status can result in risks to an organization.

The basic disposition of an insider threat may be similar for many organizations—a trusted insider who uses their access and knowledge to harm an organization. But the expression and manifestation of the threat may be vastly different, depending on the nature of the organization, the type of work or sector, the products and services performed, and, most importantly, the organizational assets that should be protected from loss, compromise, damage, or theft. **This chapter will help characterize and categorize the range of insider threats, demonstrating the need for a comprehensive insider threat program that considers the various ways insiders can present risks to an organization**.

Before delving into the details of insider threats and how to prevent and mitigate them, it is important to provide a baseline understanding of various terms. While not inclusive of every potential insider incident, definitions provide a common vocabulary and understanding to help frame the discussion of insider threat, which is an important first step in understanding and establishing an insider threat mitigation program.

There are **two components to establishing a definition for insider threat**. The first is establishing **who is an insider**. The second, and broader component, is describing the **variety of threats presented by those insiders**. This chapter will discuss:

- The **definition of an insider**
- The **definition of an insider threat**
- The **types of insider threats**
- **How insider threats can be expressed** within an organization

Definition of an Insider

An insider is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems.

A **person the organization trusts**, to include employees, organization members, and those to whom the organization has provided sensitive information and access

A **person given a badge or access device** identifying them as someone with regular or continuous access (e.g., an employee or member of an organization, contractor, vendor, janitor, repairman)

A **person to whom the organization has provided a computer and/or network access**

A **person who develops the organization's products and services**, including those who know the secrets of the products that provide value to the organization

A **person who is knowledgeable about the organization's fundamentals**, including pricing, costs, and its strengths and weaknesses

A **person who is knowledgeable about the organization's business strategy and goals** and entrusted with future plans and the means to sustain the organization and provide for the welfare of its people

In the context of government functions, they can be **a person with access to protected information**, which, if compromised, could cause damage to national security and public safety

Definition of Insider Threat

An insider threat is the potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, facilities, and associated resources.

Many organizations have adapted this high-level definition of insider threat to reflect the specific ways insiders can present risks to their organization. Some organizations base their definitions on the types of threat actors who are considered insiders (e.g., malicious, unintentional, employee, member, or contractor). Or they use the types of assets to which insiders have access (e.g., information technology (IT), facilities, networks, or data). Another approach uses the types of harm that could be done to the organization (e.g., fraud, theft, sabotage, or violence). The key point is that the definition of insider threat is contextual in nature, and what works for one organization will not necessarily work for another.

A best practice is for an organization to **define the insider threat to address the unique nature of its operating environment, what it values, or the resources it feels are most at risk**. As a starting point, organizations can rely on or tailor a definition of insider threat that has already been created by a reputable research body, trade organization, government agency, or corporation. Remember, the threat landscape will evolve, the specific needs of the organization will change, and an organization's priorities will often shift, so an organization may need to expand or refine its definition over time.

Examples of Insider Threat Definitions
from government agencies, industry, and academia

Department of Homeland Security (DHS)
"The threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems. This threat can manifest as damage to the Department through the following insider behaviors: espionage; terrorism; unauthorized disclosure of information; corruption, to include participation in transnational organized crime; sabotage; workplace violence; and intentional or unintentional loss or degradation of Departmental resources or capabilities."[12]

CERT National Insider Threat Center
"The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization."[13]

Computer Language Company Incorporated
"The potential risk that employees and officers of a company can cause more harm to the IT infrastructure or to the company in general than external threats such as viruses and cracker attacks. Also known as an 'authorized user threat,' disgruntled employees have easy access to confidential data, especially if their feelings are not made public."[14]

RAND Corporation
"The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization or national security."[15]

National Insider Threat Task Force (NITTF)
"The risk an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practice."[16]

Ernst & Young Global Limited (EY)
"The threat a current or former employee, contractor, or business partner, who has or had authorized access to an organization's network systems, data, or premises, uses that access to compromise the confidentiality, integrity, or availability of the organization's network systems, data, or premises, whether or not out of malicious intent."[17]

Department of Defense (DoD)/Center for Development of Security Excellence (CDSE)
"The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States or classified national security information."[18]

[12]Department of Homeland Security. (2019, October 01). Insider Threat Program. Instruction # 262-05-002, Revision 01. (p. 5). Washington, DC.
[13]Costa, D. (2017, March 7). CERT Definition of 'Insider Threat' – Updated. Retrieved from https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat—updated.html
[14]The Computer Language Company Inc. (n.d.). Encyclopedia: Definition of Insider Threat. Retrieved from https://www.pcmag.com/encyclopedia/term/45031/insider-threat
[15]Luckey, D., Stebbins, D., Orrie, R., Rebhan, E., Bhatt, S.D., et al. (2019). Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved? Santa Monica, CA: RAND Corporation. Retrieved from https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/EY-managing-insider-threat.pdf
[16]Department of Homeland Security. (n.d.). Insider Threat Mitigation: What is an Insider Threat? Retrieved from cisa.gov/insider-threat-mitigation
[17]EY. (2016). Managing Insider Threat; A Holistic Approach to Dealing with Risk from Within. (p. 1). Retrieved from https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/EY-managing-insider-threat.pdf
[18]Department of Defense. (2017, August 28). Department of Defense Directive. DoDD 5205.16. (p. 1). Washington, DC. Retrieved from https://fas.org/irp/doddir/dod/d5205_16.pdf; Department of Defense. (2016, May 18). DoD 5220.00-M National Industrial Security Program Operating Manual. Ch 2. (p. C-4). Washington, DC. Retrieved from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf

Types of Insider Threats

Broadly, insider threats originate from two primary kinds of activity: unintentional and intentional. Unintentional actions can be further broken down into negligent and accidental acts.

Unintentional

Negligent

Insiders can **expose an organization to a threat by their carelessness**. Insiders of this type are generally familiar with security and/or IT policies but choose to ignore them, creating risk to the organization. Examples include allowing someone to "piggyback" through a secure entrance point, misplacing or losing a portable storage device containing sensitive information, and ignoring messages to install new updates and security patches. Negligent insiders are usually complacent and show an intentional disregard for rules; they exhibit behaviors that can be witnessed and corrected.

Accidental

Even the best employee can be oblivious or naïve and **make a mistake causing an unintended risk to an organization**. Examples include mistyping an email address and accidentally sending a sensitive business document to a competitor, unknowingly or inadvertently clicking on a hyperlink or opening an attachment that contains a virus within a phishing email, or improperly disposing of sensitive documents. Organizations can successfully work to minimize accidents, but they will occur; they cannot be completely prevented, but those that occur can be mitigated.

Intentional

Insiders can **intentionally take actions that harm an organization for personal benefit or to act on a personal grievance**. Some intentional insiders are motivated by a disgruntlement related to a perceived grievance, ambition, or financial pressures. Others may have a desire for recognition and seek attention by creating danger or divulging sensitive information. They may even think they are acting in the public good. For example, unmet expectations due to lack of some form of recognition (e.g., promotion, bonuses, desirable travel) or even termination have motivated many insiders to "get even" by leaking sensitive information, harassing associates, sabotaging equipment, or perpetrating violence. Others have stolen proprietary data or intellectual property to advance their careers.

Other threats

In addition to insider threats involving only insiders at an organization, insider threats **may also involve individuals external to the organization**. These **collusive and third-party threats** may be either unintentional or intentional.

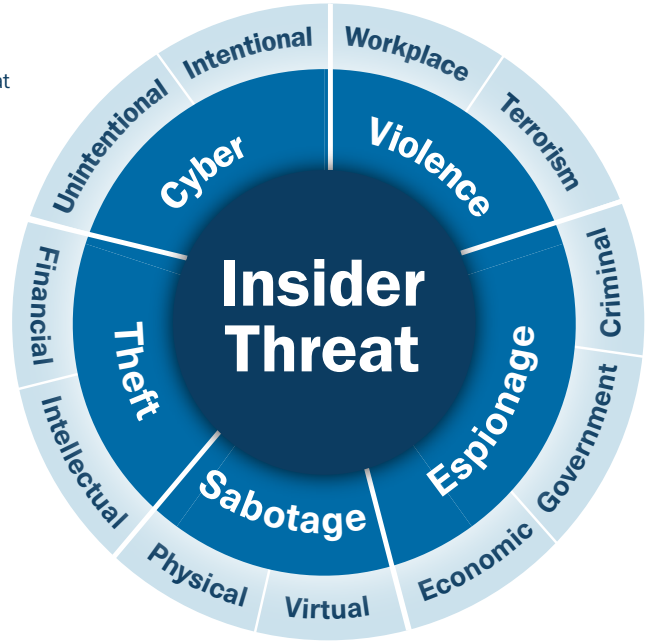
Collusive Threats: This threat sub-type manifests when one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting an insider or several insiders to enable fraud, intellectual property theft, espionage, or a combination of the three. This type of insider threat is challenging to detect, as the external actors are typically well versed in security practices and strategies for avoiding detection.

Third-Party Threats: Third-party threats are associated with contractors or vendors who are not formal members of an organization, but who have been granted some level of access to facilities, systems, networks, or people to complete their work. This threat sub-type can also include multiple third-party threats colluding. Third-party threats may be direct, where specific individuals act in a way that compromises the targeted organization, or indirect, where there may be flaws in systems that expose resources to unintentional or malicious threat actors.

Expressions of Insider Threat

Insider threats manifest in various ways. Figure 4 is a graphic representation of these expressions: violence, espionage, sabotage, theft, and those intentional or unintentional acts of harm perpetrated in the cyber domain. Each is defined in detail below.

Figure 4. Insider Threat Expressions



Violence

Violence from an insider threat consists of any act of violence, threat of violence, or other threatening behavior that creates an intimidating, hostile, or abusive environment. Insider violence includes criminal or destructive threats that precede a physical attack that damages infrastructure or threatens or harms the health and safety of an individual or group. The unique aspect associated with an insider threat involves violations of what is supposed to be a safe environment.

Workplace/Organizational Violence

Workplace/organizational violence consists of any act or threat of physical violence, harassment, sexual harassment, intimidation, bullying, offensive jokes, or other threatening behavior by a coworker or associate that occurs in a person's place of employment or while a person is working.

Terrorism

Terrorism as an insider threat is an unlawful use of, or threat to use, force and violence by employees, members, or others closely associated with an organization against that organization to promote a political or social objective. Specifically, insiders use their familiarity with an organization's structure, security, building layout, and other knowledge to maximize casualties or sabotage systems.[19]

[19]Adapted from Cybersecurity and Infrastructure Security Agency. (2019, March 3). Insider Threat – Terrorism. Retrieved from cisa.gov/terrorism

Espionage

Espionage is the practice of spying on a foreign government, organization, entity, or person to covertly or illicitly obtain confidential information for military, political, strategic, or financial advantage.

Economic Espionage

Economic espionage involves the covert practice of obtaining trade secrets from a foreign nation (e.g., all forms and types of financial, business, scientific, technical, economic, or engineering information and methods, techniques, processes, procedures, programs, or codes for manufacturing). Also referred to as commercial or industrial espionage.

Government Espionage

Government espionage consists of covert intelligence gathering activities by one government against another to obtain political or military advantage. It can also include government(s) spying on corporate entities such as aeronautics, consulting firms, think tanks, or munition companies. Also referred to as intelligence gathering.

Criminal Espionage

Criminal espionage involves a U.S. citizen betraying U.S. government secrets to foreign nations.

Sabotage

Sabotage involves deliberate actions aimed at harming an organization's physical or virtual infrastructure, including noncompliance with maintenance or IT procedures, contamination of clean spaces, physically damaging facilities, or deleting code to prevent regular operations.

Physical Sabotage

Physical sabotage consists of deliberate actions aimed at harming an organization's physical infrastructure (e.g., facilities or equipment).

Virtual Sabotage

Virtual sabotage consists of malicious actions using technical means to disrupt or stop an organization's normal business operations.

Theft

Theft includes multiple subcategories of stealing. The two subcategories most perpetrated by insiders involve finance and intellectual property. Financial gain is an age-old motive, made all the more appealing by digitized systems that lend themselves to the theft of vast quantities of customer data or intellectual property for use in larger fraud schemes.

Financial Crime

Financial crime is the unauthorized taking or illicit use of a person's, business', or organization's money or property with the intent to benefit from it. Typically, this theft involves some form of deceit, subterfuge, or abuse of a position of trust. Examples of financial crimes include personal or business identity theft, money laundering, forgery, tax evasion, bribery, embezzlement, and fraud (e.g., credit card, mortgage, wire, or securities).[20]

Intellectual Property

Intellectual property theft is the theft or robbery of individuals or organizations of their ideas, inventions, and/or creative expressions, including trade secrets and proprietary products from individuals or organizations, even if the concepts or items being stolen originated from the thief.

Cyber

Cyber is a range of expressions, including theft, espionage, violence, and sabotage, dealing with anything related to technology, virtual reality, computers, devices, or the internet. These expressions are undertaken using a variety of vectors to include viruses, data breaches, Denial of Service attacks, malware, and unpatched software, and are considered either unintentional or intentional.

Unintentional Threats

Unintentional threats consist of non-malicious (oftentimes accidental or inadvertent) exposure of an organization's IT infrastructure, systems, and data that causes unintended harm to an organization. Often, the insider may not know they are participating in the disruption (i.e., an unwitting insider). Examples include phishing emails, rogue software, and malvertising.

Intentional Threats

Typically, intentional threats are malicious actions performed by hostile insiders using technical means intended to disrupt or cease an organization's regular business operations, identify IT weaknesses, gain protected information, or otherwise further an attack plan via access to IT systems. This action can involve changing data or inserting malware or other pieces of offensive software to disrupt systems and networks.

[20]FindLaw.com. (n.d.). Fraud and Financial Crimes. Retrieved from https://criminal.findlaw.com/criminal-charges/fraud-financial-crimes.html

Case Study

When an Insider Becomes an Insider Threat

The case that follows demonstrates how the trusted employee and the use of their authorized access or knowledge to do harm come together and manifest as an insider threat. It outlines several indicators of the often-observable progression from trusted insider to insider threat, including stressors, personal predispositions, and concerning behaviors that were helpful in identifying the insider, facilitating the investigation, and ultimately disrupting a malicious act of espionage.

THE INSIDER

An engineer at an aerospace manufacturing company working on commercial and military satellites sold to the Air Force, Navy, and the National Aeronautics and Space Administration. He had access to closely held trade secrets, including anti-jamming technology and encryption plans for communication with satellites.

INDICATORS

Stressors

- Feeling of underappreciation at work and was frustrated that he could not get promoted
- Wife's deteriorating health and mounting medical bills

Personal Predispositions

- Problems with judgment: Sent gifts of $21,000+ to an online romantic interest he had never met

Concerning Behaviors

- User Activity Monitoring (UAM) revealed he had inserted a USB device and copied five folders with detailed mechanical drawings and design information for a satellite program to which he was entrusted

THE MALICIOUS ACT OF ESPIONAGE

Frustrated with financial problems and his inability to get promoted, the engineer sent notes to the Russian embassy and consulate soliciting funds in exchange for sensitive and proprietary software technology and other satellite information. Over the course of a year, he met several times with an undercover Federal Bureau of Investigation (FBI) agent who he thought was a Russian intelligence officer and collected $3,500 for the information he passed. His actions violated the Arms Export Control Act and International Traffic in Arms Regulations and posed a threat to national security and potentially significant financial harm to his company.

HOW IT WAS DISRUPTED

In cooperation with his company's insider threat team, law enforcement intervened to prevent the compromise. This intervention led to the insider's conviction for the attempted illegal sale of proprietary trade secrets to a foreign government's intelligence service. He was sentenced to five years in prison.

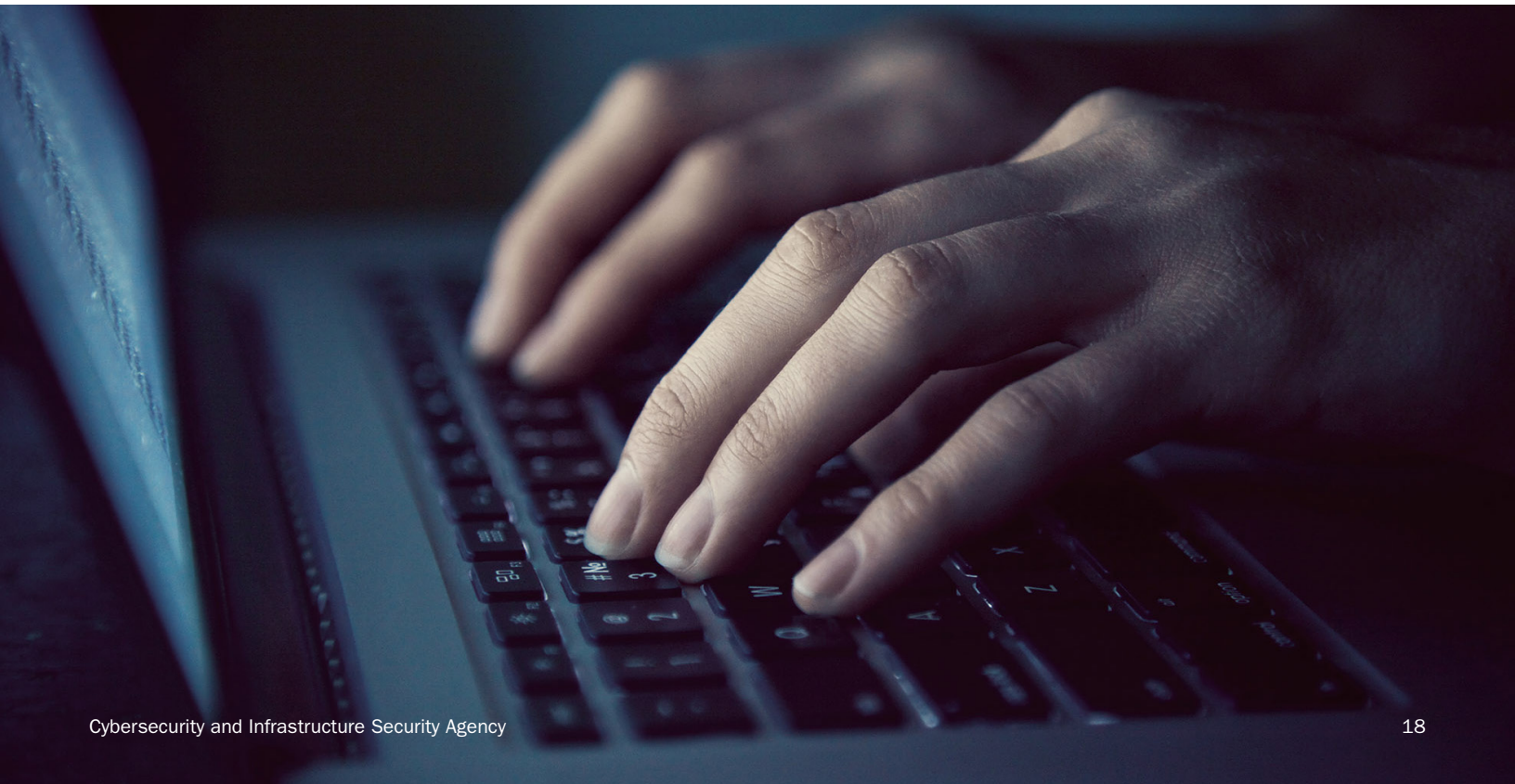
Concluding Thoughts

This chapter is designed to help characterize and categorize the range of insider threats to better structure insider threat programs and approaches. An insider is any person who has or had authorized access to an organization's resources, including personnel, facilities, information, equipment, networks, and systems. These people are trusted by the organization and only become a threat when they act outside the expectations of that trust relationship.

This chapter helps to demonstrate the breadth of the challenge organizations face and the varying typologies and expressions of the insider threat. It includes those with a specific intent to do harm, and helps to illuminate the challenge presented by those who may be the unwitting or unintentional insiders who, through acts of negligence or through manipulation, cause harm to the organization.

This chapter provides organizations with an understanding of the variety of insider threat expressions for which they must prepare. It provides a full listing of the range of threats and helps to demonstrate the need for a comprehensive insider threat program. Each threat may present risks to some degree, and each organization should understand how the risks apply to their organization when making their planning and investments choices.

Finally, while there are a variety of insider threat definitions referenced, the commonalities are important to note—these threats will manifest from those the organization trusts and for whom access has been granted and information has been shared. How that harm is realized will depend on the nature of the organization's operating environment, its critical assets, risk appetite, and what it values.



Key Points

- **The insider threat is similar for many organizations in terms of the nature of the threat**—a trusted insider who takes advantage of his or her access to do harm to the organization's mission, products, resources, personnel, facilities, information, equipment, network, or systems.
- **The character and conduct of the threat will manifest in various ways** depending on the nature of the organization, the type of work or sector, the products and services performed, and the assets that should be protected from loss, compromise, damage, or theft.
- **Each insider threat will have or have had some level of a trust relationship with their victim** and act in a way that is outside the expectations of that trust relationship.
- **Organizations should tailor their approach to the insider threat** to address the unique nature of their operating environment and what they value.
- **Insider threats are intentional and unintentional**. A significant portion of insider threats involve negligent or accidental behaviors.
- **Not all intentional insider threats are malicious**. An insider threat can occur when an individual commits a dangerous act for any number of reasons outside of an intent to harm an organization.

3 Building an Insider Threat Mitigation Program

The people within an organization are simultaneously the strongest elements of a security program and its greatest vulnerability. Without legitimate and trusted access to facilities, resources, systems, intellectual property, data, and other people, each of which creates vulnerabilities, organizations cannot function. The disruptive impacts of insider-related incidents jeopardize safety, undermine value, and degrade operations.

Despite these realities, a significant number of organizations have not established formal insider threat mitigation programs[21] to manage this risk and, if they have, many do not take a holistic view of the insider threat, often excluding expressions of the threat such as violence and sabotage. Some do have procedures in place to monitor access to or activity in specific locations. However, it is more likely that insider threat programs limit their tools and procedures to those that detect external attacks or intrusions on IT systems and company networks. Many do not have an equivalent capability to monitor and respond to insider activities, especially the malicious disruptions that are a frequent expression of insider threats.

This chapter provides a structured approach to **help an organization establish and tailor an insider threat mitigation program**. It will:

- Outline the **characteristics of an effective insider threat mitigation program**
- Describe **core principles** and **keys for success** that organizations can use to address their specific needs regardless of program maturity
- Provide guidance for **establishing an insider threat mitigation program**, aiding in an understanding of how to grow and scale a program with considerations for the size of the entity, its budget, the nature of its mission and culture, and its tolerance for risk associated with insider threats

[21]Veriato. (2019). 2019 Insider Threat Program Maturity Model Report. Retrieved from https://cdn2.hubspot.net/hubfs/5260286/PDFs/Whitepapers/insider-threat-maturity-report-2019.pdf

Characteristics of an Effective Insider Threat Mitigation Program

Successful insider threat mitigation programs employ practices and systems that limit or monitor access across organizational functions. Those practices and systems, in turn, limit the amount of damage an insider can do, whether the act is intentional or unintentional.

Even still, some organizations view insider threat programs as expensive and resource-intensive investments, with privacy, legal, and labor relations challenges. Taking advantage of established capabilities and resources can reduce these burdens. Most organizations have people and teams with similar program objectives or currently address related functions. Existing workplace harassment and violence policies and cybersecurity programs are candidates that can serve as productive starting points. Leveraging those resources can help reduce costs and the level of effort required.

In every case, **effective insider threat mitigation programs** need to be able to **detect and identify improper or illegal actions**, **assess threats** to determine levels of risk, and **implement solutions to manage and mitigate** the potential consequences of an insider incident.

An Effective Insider Threat Mitigation Program

- **Identifies and focuses on those critical assets, data, and services** that the organization defines as valuable
- **Monitors behavior** to detect and identify trusted insiders who breach the organization's trust
- **Assesses threats** to determine the individual level of risk of identified persons of concern
- **Manages the entire range of insider threats**, including implementing strategies focused on the person of concern, potential victims, and/or parts of the organization vulnerable to or targeted by an insider threat
- **Engages individual insiders** who are potentially on the path to a hostile, negligent, or damaging act to deter, detect, and mitigate

Case Study

The Case for an Insider Threat Mitigation Program

WHAT HAPPENED

During the night shift beginning on March 31, 2011, an employee at a water reclamation plant intentionally disabled controls and shut multiple valves to critical components of the water reclamation systems at the facility. This included deactivating pumps that controlled the flow of sewage through the facility and flares that burn off methane gas produced by the plant. The individual closed the valves manually so that the remote-control systems in place at the facility could not override his actions. The employee also disabled alarm systems, which would have alerted other staff at the facility, and he disabled the entry gates to the plant to delay emergency response to the facility. Once these actions were completed, the individual went to the top of one of the buildings within the compound, sat in a folding chair, and called 9-1-1. While waiting for emergency responders, he took his prescribed psychostimulant medication with multiple alcoholic beverages so that he would be "brave enough to face what was coming."

When law enforcement arrived at the plant, the individual spray-painted a bullseye on his shirt and placed a bandage on his head so that the police would "know where to aim." The employee was eventually taken into custody by local law enforcement, where he was found to be armed with a handgun, five rounds of ammunition, and a knife.

INDICATORS

The subsequent investigation revealed that the individual had shown his peers, coworkers, and supervisors a clear pattern of increased stress and concerning behaviors. The employee had financial problems and multiple failed attempts to obtain assistance for his depression and suicidal thoughts. The employee had previously engaged the human resources (HR) department on several occasions about his health concerns and requested removal from the night shift. In addition to his financial and health concerns, the employee became increasingly disgruntled at work, expressing multiple grievances about the lack of municipal investment in compensation for employees at the water reclamation plant.

COST OF THE THREAT

The water reclamation plant sustained $60,000 in damages from this incident. The individual was immediately fired from the plant and was charged with terrorism, burglary, criminal damage, and the use of a handgun in the act of terrorism. He was sentenced to four years of probation.

LESSON LEARNED

With a trained and sensitized workforce, a threat management team in place, and a positive culture of reporting, the damage and disruption to plant operations could have been prevented, and the employee could have received the help he needed.

Core Principles

A holistic insider threat mitigation program combines physical security, personnel assurance, and information-centric principles. Its objectives are to understand the insider's interaction within an organization, monitor that interaction as appropriate, and intervene to manage that interaction when it poses a threat to the organization.

Successful insider threat mitigation programs accomplish these objectives while addressing three core principles, which apply to organizations of all sizes and maturity levels:

1. **Promoting a protective and supportive culture** throughout the organization
2. **Safeguarding organizational valuables** while protecting privacy, rights, and liberties
3. **Remaining adaptive** as the organization evolves and its risk tolerance changes

1 Promote a Protective and Supportive Culture

A strong foundation for insider threat prevention and mitigation comes from a set of values that are shared and acted upon by everyone in an organization. Such a foundation helps to shape the way people think about these threats to people, assets, and information, and the approach they should take when observing indicators in their environment.

A protective culture gives people confidence that an insider threat mitigation program is supportive in nature. To support this approach, **organizations should promote a climate of accountability and mutual respect, generating a positive community-focused culture and one that encourages reporting** rather than unintentionally inhibiting it. As figure 5 exemplifies, successful programs focus on helping members of an organization in order to deter and prevent an insider incident rather than seeking to punish or discipline following a negligent or intentional act.

Figure 5. A Protective Culture Supports a Successful Insider Threat Mitigation Program

A Protective Culture...

Establishes an environment where all members of an organization are collectively responsible for participating in the detection and mitigation of insider threats

Enables employees to speak openly regarding threats by encouraging reporting and instilling confidence that the organization will act while protecting the privacy of those who do report

Empowers members of an organization, inspiring them to focus on acting for the benefit of the organization while helping the individual

Determining organizational expectations and conveying them effectively is vital to creating and sustaining a protective and supportive culture. Key guidelines include:[22]

- The **behaviors expected from members** to keep themselves and organizational assets safe and secure
- **How these behaviors differ depending on the role or responsibilities of an individual or group** in the organization
- The **behaviors expected from vendors, contractors, or visitors** when they are physically or virtually engaged with the organization so they do not jeopardize security
- The **behaviors expected from partners or suppliers** when handling or accessing organizational information or equipment to protect them from compromise

Ensuring that members are educated about the dynamics of insider threats is critical to setting a culture of reporting. It starts with letting members know that they will likely be in a position to detect the threats. For example, a study in the banking and finance sector conducted by the National Insider Threat Center found that, in 85 percent of incidents, someone other than the insider had full or partial knowledge about the insider's intentions, plans, and activities.[23] Still, the incidents were not thwarted. Training should include this key understanding. Train members to whom they can report—including anonymous reporting—and emphasize that reporting will help individuals and potentially prevent an incident. Sharing the details on the investigative process once a report is made can also help to overcome reporting barriers, increase organizational trust, and alleviate fears or misinformation.[24]

Establishing a focus on accountability versus blame also plays a role in establishing a protective culture. Assigning blame can be counter-productive, and can discourage reporting, even when the potential consequences of an event are high. Still, a blame-free environment does not mean that individuals are not accountable for their actions. Providing individuals an opportunity to acknowledge their responsibility in an incident while involving them in addressing the consequences can reduce the potential for recurrence.

2 Safeguard the Organization's Valuables while Protecting Privacy, Civil Rights, and Personal Liberties

Insider threat mitigation programs have insight into sensitive information regarding an organization's people and their behavior. With great authority comes an equal responsibility. Organizations must strike a balance between the need to protect assets and the need for transparency on monitoring policies and privacy expectations.

All insider threat programs touch on multiple complex legal considerations including privacy and civil liberties, whistleblower protection, employment law, health and educational privacy, liability and management, and individual due process rights, among many others. **An insider threat**

[22]Adapted from Centre for the Protection of National Infrastructure. (n.d.). Identifying Security Behaviours. Retrieved from www.cpni.gov.uk/identifying-security-behaviours

[23]Randazzo, M.R., Keeney, M., Kowalski, E., United States Secret Service's National Threat Assessment Center, Cappelli, D. (2005, June). "Illicit Threat Study: Illicit Cyber Activity in the Banking and Finance Sector." (p. 15). Software Engineering Institute. Technical Report CMU/SEI-2004-TR-021. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14420.pdf

[24]Jaros, S. L. (2018, October). A Strategic Plan to Leverage Social & Behavioral Sciences to Counter the Insider Threat. | OPA-2018-082 | (p. 13). Defense Personnel and Security Research Center, Office of People Analytics. Washington, D.C.

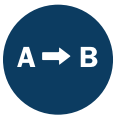
mitigation program that protects privacy, civil rights, and civil liberties can reinforce a protective culture, positively impacting morale, and potentially avoiding civil or criminal penalties.

In some cases, an improper organizational response may provide a triggering event, transforming a potential insider threat into an actual one.[25] Conversely, insider threat mitigation programs that protect privacy and civil liberties and comply with laws, regulations, and standards will have an enhanced ability to accomplish their mission and enable greater protection for their organization.

> "Addressing privacy, civil rights, and civil liberties early in the planning of any new initiative (or in the redesign of existing systems and processes) allows these information protections to be considered, built-in, managed, and monitored enterprise-wide."
>
> *2012 National Strategy for Information Sharing and Safeguarding*[26]

3 Remain Adaptive as the Organization and Its Risk Tolerance Evolves

Insider threat is an evolving challenge, requiring adaptive and resilient practices to address a dynamic environment. It involves rapidly changing technologies and organizational priorities.[27] Varying degrees of access and understanding, new and evolving capabilities, and continuous evolution in most organizations make apparent the requirements for a dynamic and responsive program. Best practices include:



Adaptation of insider threat mitigation programs as the organization evolves and adapts

Continuous improvement from best practices and lessons learned from the broader insider threat management community

A dynamic insider threat risk registry with regular risk assessments and risk ratings informing a more current and accurate risk picture, which enables proactive solutions to prevent and mitigate more broadly across the organization as opposed to just making changes following incidents

Leveraging information sharing, lessons learned, and best practices from authoritative agencies and non-governmental organizations who can provide a deep well of (often publicly available) insider threat reference and advisory material, allowing the collective experience of others to inform program improvements[28]

[25]Shaw, E. & Sellers, L. (2015, June). Application of the Critical-Path Method to Evaluate Insider Risks. Internal Security and Counterintelligence. Studies in Intelligence 59(2) pp. 1-8. Retrieved from https://static1.squarespace.com/static/596a623ba5790afcec9c024e/t/59c9e849cd39c3877ffc5098/1506404436555/Shaw-Critical+Path-June-2015.pdf

[26]Office of the President of the United States. (2012, December). National Strategy for Information Sharing and Safeguarding. (p. 13). Retrieved from https://www.dhs.gov/sites/default/files/publications/15_1026_NSI_National-Strategy-Information-Sharing-Safeguarding.pdf

[27] National Insider Threat Task Force. (2018, November). Insider Threat Program Maturity Framework. Retrieved from https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

[28]Adapted from the Transportation Security Administration. (2020). Insider Threat Roadmap 2020. (p. 8). Retrieved from https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf

Keys for Success

An insider threat mitigation program is designed to help organizations intervene before an individual with privileged access to or understanding of the organization makes a mistake or commits a harmful or hostile act. In addition to the foundational concepts and core principles described above, there are several keys to program success, each of which applies to organizations of all sizes and maturity levels.

Know Your People

To achieve an effective level of personnel assurance, an organization must know and engage its people. Accordingly, it must vet them prior to hiring and incorporate continuous accountability processes as a part of the protective culture. And it must engage them with regular and continuous awareness, education, and training. This final piece is of particular importance since many insider incidents are unintentional, resulting from falling victim to social engineering, noncompliance with company policies and protections, or other negligent activities.

Identify the Organization's Assets and Prioritize Risks

Understanding what an organization values, and what could possibly damage or disrupt those assets is essential for an effective insider threat mitigation program. A full understanding of an organization's assets will allow the proper alignment and management of potential risk to those assets. A proven approach begins with determining where an organization's assets are located and who has access to them. This will allow a broader classification of the risk to each asset and enable the development of risk-based mitigation strategies.

Establish the Proven Operational Approach of *Detect & Identify—Assess—Manage*

Best practices for insider threat mitigation employ an operational approach that is built in concert with existing security programs to enable detection and identification of a potential threat, assessment of that threat, and then both active and passive techniques to manage that threat. All three are necessary to proactively mitigate the insider threat. This approach is best employed and supported with a multi-disciplinary team from across an organization, with organizational leaders, human resources, information technology, legal counsel, security, and others each supporting the effort to detect and identify, assess, and manage threats. This approach gathers and investigates incident and threat information, assesses and categorizes those risks, and implements management strategies to mitigate threats. Those solutions will also employ a range of proactive and protective measures focused on reducing the risk from the person of concern, protecting potential victims or assets, or improving the overall protective posture in the organization. Smaller

organizations or those with nascent insider threat programs can leverage existing functions to support this activity.

The insider threat mitigation framework allows for consistent, systematic mitigation of insider threats, encouraging engagement across all organizational operations and functions. The combination of cultural and systemic action will fulfill **five core functions**:

1. **Establish and maintain a safe environment** to prevent violence and other hostile acts from occurring
2. **Deter potential insider threats** by instituting policies, security controls, procedures, and programs to protect the organization
3. **Detect threatening or concerning behaviors** and identify individuals at risk of becoming an insider threat
4. **Assess information about actual or potential insider threats**
5. **Manage potential insider threats before they escalate** to violence, espionage, sabotage, or theft

Establishing an Insider Threat Mitigation Program

Building and maintaining an insider threat mitigation program takes careful conceptualization, planning, and oversight. Insider threat mitigation programs are multi-disciplinary, and because they intersect with multiple business functions they require executive level sponsorship and commitment to improve an organization's ability to detect and identify, assess, and manage insider threats.

Organizations do not need to create an insider threat mitigation program from the ground up. Rather, organizations that have existing violence prevention policies and procedures, or IT or cybersecurity programs can use their existing infrastructure as the foundation for insider threat mitigation.

Just as there are key principles for a successful insider threat mitigation program, there are some recognized best practices, concepts, tools, and processes for establishing such a program. The NITTF created a list of guidelines for federal agencies and departments to develop insider threat management programs.[29] This guidance provides a sound starting point for all public and private sector organizations to consider in developing a new program, implementing a more fully functioning program, or measuring the maturity of an existing program.

NITTF Guidelines for Establishing an Insider Threat Program

1. Designate a Senior Official
2. Form an Insider Threat Working Group
3. Establish Governance and Publish Insider Threat Policy
4. Implement a Formal Training and Awareness Program
5. Create an Insider Threat Program Office

For this *Guide*, those practices have been adapted for application across both the public and private sectors in **four mission areas**:[30]

I. Plan

- Secure Executive Engagement
- Determine the Best Fit
- Determine Program Ownership
- Establish a Multi-Disciplinary Governance Group
- Establish Guiding Principles
- Develop Policy
- Address Legal Obligations
- Identify Crown Jewels

II. Organize & Equip

- Integrate Information, Analysis, and Response
- Develop an Incident Response Plan
- Establish Reporting Pathways
- Employ Technology and Tools to Identify Concerning Behaviors
- Establish a Risk Rubric and Threat Assessment Methodology
- Establish a Multi-Disciplinary Threat Management Team

III. Train & Execute

- Sell the Program
- Encourage a Culture of Reporting
- Implement a Formal Training and Awareness Program

IV. Evaluate & Improve

- Conduct Exercises
- Maintain the Program
- Provide Oversight and Compliance

[29] National Insider Threat Task Force. (2017). Insider Threat Guide; A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards. Retrieved from https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

[30] Adapted from National Insider Threat Task Force. (2017). Insider Threat Guide; A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards. Retrieved from https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

I. Plan

☐ Secure Executive Engagement

Insider threat programs require support from executive or senior leadership. Best practices from various insider threat programs demonstrate that programs that are directly aligned with the senior leadership of an organization are the most effective and have fewer impediments. Executive engagement assures commitment to the program, encourages cooperation from managerial staff, and can enhance access to essential information. Most importantly, when an executive or senior leader is visibly involved or seen emphasizing the program to the personnel, it drives positive support for the program.

☐ Determine the Best Fit

Where does the program fit into the organization? Should it be an independent entity or fall under one of the already-established offices?

Some organizations have an independent program organized laterally from senior leadership. These organizations appoint a Senior Official, who reports directly to a senior leader. Other organizations align the program under their security, loss prevention, or investigative offices. These offices are already working to resolve threat incidents and can lend valuable experience to program implementation. Specialty organizations, generally large manufacturing companies or national security agencies, place the program within a counterintelligence function, an entity that is the existing focal point for handling incidents of suspected espionage. There are many options and applications in practice; the key is to decide the approach that is best for each organization.

☐ Determine Program Ownership – Identify a Responsible and Accountable Senior Official

The program should be headed by a single individual, commonly called the Senior Official, who is appointed by the executive leadership and supported by a multi-disciplinary governance group. This official will be principally responsible for the overall management and oversight of the insider threat program. The individual needs to have proper seniority and the ability to bring together multiple organizational activities. The official will be a visible symbol for the program and will serve as a program advocate. Consider an individual with security or investigative experience, someone with excellent communication skills, and someone whose character is above reproach.

Organizationally, the Senior Official should be aligned to allow for direct, unfettered access to executive leadership for program support, resource requests, budgeting, and case updates. At the same time, executive leadership

Figure 6. Senior Official Best Practices

should be visible in their support of the Senior Official to enhance program success. The Senior Official will be singularly responsible for:

- Establishing program policies, procedures, practices, and processes to gather, integrate, and centrally analyze information
- Publishing an insider threat response plan
- Ensuring the program protects privacy and civil liberties
- Establishing oversight mechanisms and reviews to ensure the program has rigorous accountability
- Creating procedures for the proper handling, analysis, and retention of records
- Responding to relevant information indicative of a potential insider threat
- Serving as the primary communicator, negotiator, and resource advocate with senior leadership (see figure 6 for some Senior Official best practices)

☐ Establish a Multi-Disciplinary Governance Group

Form a governance group consisting of stakeholders or personnel from each component or office in the organization whose discipline places them in a position to receive information pertinent to the background, conduct, and activities of trusted insiders. Stakeholders may include representatives from:

- Physical Security
- Law Enforcement, Loss Prevention, or Investigative Offices
- Human Resources
- Counterintelligence
- Data Owners
- Information Technology
- Information Security
- Software Engineering
- Contracting
- General Counsel
- Privacy, Civil Rights, and Civil Liberties
- Employee Assistance Program (EAP) or Behavioral Scientist
- Equal Opportunity and Diversity Management
- Enterprise Risk Management

Each of these disciplines will play a role in an effective insider threat mitigation program. Moreover, each has access to information that others in the organization typically do not have or a perspective that can help find and contextualize anomalous behavior. If an organization lacks a needed discipline, consider creating a memorandum of agreement with an external entity for specialized support and specific response actions.

The governance group is responsible for reviewing the organization's existing policies, standards, procedures, and environment for threat program compliance. It should make modifications to existing documentation or programs when needed or create new policies and standards tailoring the organization to comply with the insider threat program and required legal constraints.

The governance group should be empowered with clear roles and authorities, including oversight of major program elements, including the program budget, resource allocation, compliance with legal obligations, training and exercises, and the development of the Incident Response Plan, which describes the processes for making insider threat case assessments and interventions.

☐ Establish Guiding Principles

Organizations should identify principles that will guide the development of its program and ensure that they match the security challenge, as well as fit within the organization's structure, function, and culture. These principles should express the function of an insider threat program in the organization. They should align to how the program describes its purpose, goals, and objectives, as well as how the threat management team will operate. Figure 7 below is an example of a major defense company's guiding principles. Notice that the principles reflect how the company aligned its insider threat program to its culture and business.

Figure 7. Sample Guiding Principles

Sample Guiding Principles: One Company's Approach

- Protecting employee privacy is a primary element of the program.
- Intellectual property protection is key to our company's growth–protects innovation and is a market differentiator.
- Insider threat steering team governs the program.
- Start small with accessible and controllable data–gain confidence in data before adding new elements.
- Identification, management, and mitigation of anomalous behavior and activities is the goal–looks for behavior, not people.
- Ensure employee communication on insider threat program purpose.
- Insider threat program does not replace management responsibilities to address employee challenges or issues.

Protect vs. Punish

Insider threat management frequently involves approaches that constrain users, monitor behavior, and detect and punish misbehavior. These can create negative incentives that attempt to force employees to act in the organization's interests. When relied on excessively, restrictive approaches can result in negative unintended consequences that exacerbate the threat.[31]

Research suggests that positive incentives can complement traditional practices by encouraging employees to act in the interests of the organization either extrinsically (e.g., through rewards and recognition) or intrinsically by fostering a sense of commitment to the organization, the work, and co-workers. Instead of solely focusing on making sure employees do not misbehave, positive incentives create a work environment where employees are internally driven to contribute to the organization in positive ways.

Positive incentives can deter insider misbehavior in a constructive way from the outset of the employee-organization relationship with fewer negative consequences than traditional insider threat practices alone. Employees who are excited and engaged in their work, who perceive organizational support, and who feel close to those with whom they work are more positively aligned with the organization's interests.[32]

[31]Moore, A., Perl, S.J., Cowley, J., Collins, M.L., Cassidy, T.M., et al. The Critical Role of Positive Incentives for Reducing Insider Threats. (pp. v-vii). CMU/SEI-2016-TF-014 | Software Engineering Institute | Carnegie Melon University. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484929.pdf
[32]Ibid.

As such, successful insider threat mitigation programs employ a balance of positive and negative incentives, promote employee satisfaction and performance, avoid overly aggressive reactions following notification of a threat, and are not designed to catch people doing things wrong.

When messaging employees or organizational members, emphasize the organization's concern for its members' well-being, that individuals should report insider threats not only for the benefit of other employees or members of the company or organization, but for the insider as well. Emphasize the need to prevent insider threat actions before they occur and educate the workforce or membership about the potential consequences of insider threats.

A key element is to clearly communicate the collective harm an insider can pose, particularly in a business setting. One individual who steals or sabotages proprietary information or trade secrets may in fact damage the corporate brand and lead to the loss of a market edge. This, in turn, affects all trusted insiders and may even lead to the loss of their jobs, affecting their families and potentially their communities, especially if the company or organization collapses.

In government, loss of sensitive information related to national security can cause catastrophic outcomes, including loss of life. Emphasizing these consequences can foster a culture of individuals who are willing to voice concerns when they notice irregular, concerning, or illegal behavior.

☐ Develop Policy

An insider threat mitigation program will need formal policies and procedures, grounded in legal authorities. Organizations will need to ensure that they establish policies and procedures that are appropriate for their culture, mission, and locality, as well as conforming with state and federal regulations and statutes.

At a minimum, it is essential that the insider threat mitigation program policy address the following:

- How does the organization define its violence prevention and insider threat responsibilities?
- What responsibilities in these areas does the organization currently have?
- What responsibilities will the insider threat mitigation program own within the organization?
- What approaches, if any, are currently being used for the safety and security of the organization?
- What kind of security services and programs are currently in use to fulfill the organization's responsibilities?
- What is the level of support from legal counsel?
- What happens when concerning situations are received by the organization?
- What should occur when an individual who might be interested in harming an organization or person comes to the organization's attention?
- Who will carry out the violence prevention and insider threat capabilities?
- What kind of staffing is needed?
- How will the subject matter expertise developed by the program administrators be kept and shared over time?
- What type of training is needed, and how will the program staff train the rest of the organization?

Do Not Re-Invent the Wheel

Insider threat mitigation programs should leverage other programs already in use in the organization. Existing programs provide insight into useful approaches, transferable best practices, and techniques that can be tailored to the needs of the insider threat program.

Most organizations already have a range of security and threat management programs, such as harassment or violence prevention or IT security, which can support a broader insider threat program with concepts, tools, and practices. Look to other organizations in a similar sector and apply relevant elements to the local mission. Save time and money by using existing technology, people, and communication practices. Creating an insider threat mitigation program does not have to be a burden on an organization. Consider a scalable, phased approach to control costs and minimize operational impact.

Most importantly in this phase, remain flexible and adaptable. The threat landscape continually evolves, technology shifts rapidly, organizations change in response to various pressures, and companies adapt to market forces.

Avoid Zero-Tolerance Policies

Organizations should be cautious about instituting zero-tolerance approaches toward insider threat mitigation policies. Even when organizations institute policies for behavior such as harassment or violence, zero-tolerance policies can have unintended and undesirable effects. Zero-tolerance policies are generally used as automatic triggers of discipline or intervention for the offender regardless of severity and mitigating factors, and with less investigation and due process. A zero-tolerance policy may have the unintended effect of reducing and inhibiting reports of misconduct because coworkers or associate members fear that a report could cost the person of concern their position or job.

Liaise with Law Enforcement

When developing governance and policy for an insider threat mitigation program, it is helpful to liaise with local law enforcement authorities to ensure that their potential role in the process is clearly understood. An existing relationship and communication channel between an organization and local law enforcement authorities may make the entire mitigation and management process more effective when an incident occurs. The need to establish these relationships and communication channels applies to organizations of all sizes and maturity levels. The **dialogue with local police should result in an understanding of the responses to many of the following questions** to enhance threat management capabilities:

- What is the standard response to reports of observable warning signs or prohibited behaviors?
- How will the department or agency respond to a report of an unauthorized person on the property or in the building with a weapon?
- Is there a policy of investigating threats before any injury occurs?
- If the organization does not have forensic cyber threat analysis for their members' computers, does local law enforcement have a resource?
- Will the department or agency take part as an ad hoc member of an interdisciplinary threat management team?
- What are the local mental health commitment laws and requirements?
- What are the local weapons possession or acquisition procedures?
- What are the local stalking and harassment laws and requirements?
- Will the department or agency participate in high-risk personnel actions such as expulsions, suspensions, or terminations?
- What is the department or agency policy on responding to conduct that creates fear, such as threatening, bullying, and intimidation, but that may not be characterized as criminal?
- What is the procedure following a report of a crime in progress at our facility?
- How long does the department or agency estimate it will take law enforcement responders to reach the scene after an emergency call?

In building a channel of communication with a law enforcement agency, it is a best practice for organizations to appoint one person, preferably a member of the threat management team, as its permanent liaison with the police. It is even better if the police department also provides a single point of contact. Many police agencies have assigned threat assessment personnel, so, if such a position exists, an organization's policy and plans should include when and how to appropriately engage the person overseeing threat assessment efforts.

A cooperative relationship with local police can also benefit an organization by providing a channel to resources that can only be accessed through law enforcement agencies. For example, if an organization is concerned about a potentially dangerous employee and a cooperative relationship with law enforcement has been established, then the local police could contact the FBI's National Center for the Analysis of Violent Crime (NCAVC)[33] to conduct a violence risk assessment. The NCAVC can recommend possible intervention strategies if the employee is assessed as presenting a serious risk of violence.[34]

[33]The National Center for Analysis of Violent Crime (NCAVC) is a major branch of the FBI's Crisis Incident Response Group. This department provides behavioral-based investigative support to the FBI, national security agencies, and other federal, state, local, and international law enforcement agencies involved in the investigation of unusual or repetitive violent crimes, threats, terrorism, cyber-crimes, public corruption, and other matters. https://www.fbi.gov/services/cirg

[34]American Society for Industrial Security International & the Society for Human Resource Management. (2011, September 02). American National Standard; Workplace Violence Prevention and Intervention. (p. 38). ASIS/SHRM WVPI.1-2011. ASIS International. ISBN 978-1-934904-15-2

☐ Address Legal Obligations

Navigating the legal landscape is a sensitive area for both an organization, its membership, and their associates. It is imperative that every organization realize that both the organization and its people are vulnerable to insider threat incidents. A sound insider threat mitigation program will determine the appropriate level of trust to give individuals while, at the same time, not infringing on the privacy, civil rights, or civil liberties of the personnel within the organization.

The list below includes a host of complex legal foundations, duties, and constraints an insider threat mitigation program will need to consider.

- Employment law
- Regulatory law
- Criminal law and procedure
- Civil law
- Ethics
- Liability and management
- Pre-hire background checks
- Lawful termination
- Privacy/confidentiality laws and regulations
- Disability laws and regulations
- Occupational Safety and Health Act
- Education (Clery Act, Title 9, etc.)
- Freedom of Information Act and open records
- Stalking and criminal threats
- Due process protections and investigative procedures
- Criminal and civil protective orders
- Emergency protective or restraining orders
- Civil commitment
- Wrongful termination and retaliation
- Privilege and confidentiality
- Informed consent
- Duty to warn and duty to protect
- Liability, negligence, foreseeability, emotional distress
- Health Insurance Portability and Accountability Act
- Trademarks, patents, piracy, counterfeiting

In addition, it is vital that insider threat programs both act in accordance with policy and document actions. Maintaining consistent records protects the integrity of the organization, the program, and the trusted insiders. It also provides insiders with clear expectations about what information and activities can be expected to remain private while employed by or taking part in activities within the organization.

☐ Identify “Crown Jewels”

A central question for every organization is: what does my organization value, and what should it protect? Critical assets are possessions that the institution values. Typically, these critical assets are essential to the operation or business of an organization, and compromise, damage, or loss would have an adverse impact on its mission.

Critical assets can be both physical and intellectual and include facilities, systems, equipment, personnel, technology, proprietary software, customer or vendor data, schematics, internal manufacturing processes, and personnel privacy, to name a few.

The cornerstone to any effective insider threat program is having a process in place to identify, track, and monitor an organization's critical assets. It is the responsibility of the governance group to create the process and define the assets. **Consider a database that includes, at a minimum, a listing of the type of asset, its risk assessment ranking, its location, primary use, and those who have access.** A reliable critical asset tracking method is essential to keeping the program aligned with the organization's needs, mission, and business functions, while at the same time creating metrics for the evaluation of data and behaviors to be investigated by the insider threat team.

Organizations should refer to standards that can help with this process. These include those provided by the National Institute of Standards and Technology (NIST), a unit of the U.S. Commerce Department that provides a risk-management framework for information systems, and risk assessment and management standards codified by the International Organization for Standards.[35] These standards can provide the overall approach to identifying risk and the reason for its occurrence, identify consequences if the risk occurs, and provide a risk-treatment and monitoring methodology.

II. Organize and Equip ☑

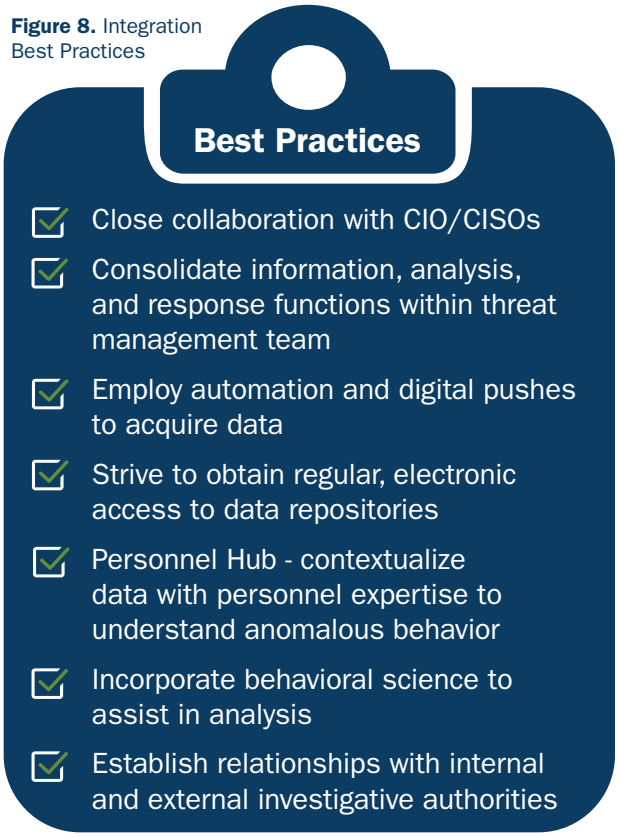
☐ Integrate Information, Analysis, and Response

Information, technology, people, reporting paths, and skilled analysts or investigators are the fundamental elements for an operational insider threat mitigation program. While each element independently can show a behavioral anomaly, it is the fusing of the elements that reveals the abnormal behavior indicative of insider threat activity.

The governance group should establish and maintain a hub to collect, integrate, review, analyze, and assess the elements to effectively administer the insider threat program. The hub should employ automated and digital pushes to acquire data and strive to obtain regular, electronic access to data repositories. There are multiple organizational assets that can be integrated:

- Personnel security files and HR records
- Facility access records
- Travel records
- Foreign contact reports
- Financial disclosure filings
- Network access and print logs
- IT enterprise audits
- Public records and financial data
- UAM logs
- Surveillance video

Figure 8. Integration Best Practices



[35]Ross, R.S. & Joint Task Force. (2018, December). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST Special Publication 800-37, Rev. 2, 183. National Institute of Standards and Technology | U.S. Department of Commerce | Washington, D.C. | https://doi.org/10.6028/NIST.SP.800-37r2 | Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

The governance group will need to create policies and procedures for the integration of assets (including directing stakeholders to provide access to information). The policies should also establish guidelines for insider threat information reporting, creating procedures for accessing sensitive or protected information, building and maintaining insider threat analytic and response capabilities, and establishing actions for responding to threats.

Confidential reporting mechanisms and procedures should be created to enable reporting of suspicious activity or concerning behaviors while protecting the privacy of the reporter and reported. Emphasizing these elements helps to create a culture of reporting by alleviating fear of retaliation while also guaranteeing that legitimate reporters are not inhibited or inappropriately monitored. Confidentiality should be built into the threat management processes to avoid giving the person of concern a new grievance, help protect the privacy of individuals involved, and help protect the sources and methods used by the insider threat team.[36]

The governance group should build relationships with external investigative authorities, behavioral science experts, and mental health agencies or experts for assistance in analyzing behaviors, investigations, and interventions. Access to integrated assets allows the threat management team to detect, collect, analyze, investigate, and respond to anomalous behavior or unauthorized activity, potentially preventing an insider attack. Figure 8 lists several integration best practices.

☐ Develop an Incident Response Plan

An Insider Threat Incident Response Plan addresses unintentional and intentional incidents, and events triggered by insiders, and is similar to an Emergency Response Plan. Creating an Incident Response Plan ensures that an organization's response to an insider incident or potential threat is standardized, repeatable, and consistently applied.

The plan should have a scope, established roles and responsibilities, methodology, guidelines for incident response processes, reporting procedures, and an escalation and reporting chain. Supplements may be needed for specific internal guidelines and procedures that describe the use of the organization's security tools and channels of communication. All response procedures should be in accordance with legal, ethical, privacy, and civil liberties laws or policies. So, legal counsel should assist in the creation.

An effective Incident Response Plan should cover the entire incident life cycle, including specifics of how an incident was detected and identified, reported, assessed, contained, managed, documented, and reported to external authorities or law enforcement where appropriate. It is important to remember that specific response processes will differ depending on the type of incident or threat (e.g., fraud versus theft of intellectual property versus sabotage versus targeted violence) as well as whether the incident or potential threat was unintentional or intentional.

See Chapters 4–6 for detailed discussions on detecting and identifying, assessing, and managing an insider threat. Additional guidance on the process to develop an Incident Response Plan can be found in the Federal Emergency Management Agency's (FEMA) Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101.[37] Organizations can use the CPG 101 processes and best practices as a detailed guide for the planning process.

[36]Behavioral Analysis Unit (n.d.) Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 78). U.S. Department of Justice | Federal Bureau of Investigation. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view
[37]Federal Emergency Management Agency. (2010, November). Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101. Version 2.0. Retrieved from https://www.fema.gov/media-library-data/1573581112287-035972e4d26817854c833457863c34cc/201911Listening_CPG_101_V2_22NOV2010.pdf

When developing an insider threat Incident Response Plan, there are unique considerations that should be taken into account for incidents that may involve domestic violence or mental illness.

Domestic Violence

An insider threat mitigation program should include the potential for domestic abuse within its policies on violence and cover both the prevention of abuse and the protection of victims. For example, a violence policy should make it an offense to threaten or harass someone (within the same organization or elsewhere) while on the job or with the use of the organization's equipment, such as phones, cell phones, faxes, email, social media accounts, or computers. It is important to realize that these devices have a clear insider threat nexus.[38]

Mental Illness in Insider Threats

It is important to recognize that the vast majority of mentally ill people are law-abiding citizens. Mental illness is among the most common health conditions in the U.S. with more than 50 percent of people diagnosed with a mental illness or disorder at some point in their lifetimes.[39] Illnesses or disorders can range from depression to substance abuse to post-traumatic stress disorder to schizophrenia.

While many assume that the mentally ill may act violently toward others, the data shows that a person with mental illness is more likely to be a victim of violent crime than the perpetrator. Key factors to consider:[40]

- Most of us know of or have experience with a family member, friend, neighbor, or coworker who may be dealing with a mental illness, yet they are a fully functional contributing member of society.
- Multiple interacting factors, such as personal stress, crisis, or loss, increase the risk of criminal and/or violent behaviors.
- Substance abuse is the most important key contributor to criminal and/or violent behavior.
- Individuals with a diagnosed or undiagnosed mental illness who have acted violently in the past are more likely to become violent again.

☐ Establish Reporting Pathways

Reporting is integral to the prevention of an insider threat. Threats that are not known cannot be mitigated. The governance group should develop confidential reporting pathways that are easy to find, understand, and use along with organizational policies that structure and implement reporting pathways that encourage reporting. While undertaking this work, the governance group should focus on helping individuals and emphasizing the benefits of reporting.

[38]American Society for Industrial Security. (2020, May 7). Standard: Workplace Violence and Active Assailant-Prevention, Intervention, and Response. (p. 32). ASIS WVPI AA-2020. ASIS International, ISBN 978-1-951997-03-8

[39]Centers for Disease Control and Prevention. (2018). Data and Publications. Retrieved from https://www.cdc.gov/mentalhealth/data_publications/index.htm

[40]Ghiasi, N., Azhar, Y., & Singh, J. (2020, April 6). Psychiatric Illness And Criminality. "StatPearls" [Internet]. StatPearls Publishing. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK537064/

Reporting can be a daunting task for many individuals as they may fear consequences from their involvement, or they may fear getting it wrong and harming someone unnecessarily. Other **reporting barriers** can include the **potential for ridicule**, **fear of not being taken seriously**, **not trusting the confidentiality**, or the **desire to remain uninvolved in others' affairs**.

As such, an organization needs to create a system that encourages reporting by developing a culture of shared responsibility and making sure people know that the program is confidential and designed to help them and the potential insider. Let individuals know that:

- **Reporting can be anonymous or made to external agencies**. These can include internal tip lines, tip lines hosted by a third party, locked suggestion boxes, or social media platforms.
- **Reports can be made to the organization's Insider Threat Program or external law enforcement** if an individual believes they have witnessed an illegal activity.

Reporting can also be difficult because of the environment in which a threat or incident occurs. Many organizations are no longer concentrated in a single facility, but have expanded to include numerous types of environments such as offices or professional spaces, homes, retail settings, athletic structures, or field sites. Utility companies, charities, educational institutions, healthcare, and governments are just a few of the organizations that own multiple sites or require individuals to work outside of the traditional office settings. Specific measures should be implemented to allow those not in direct contact with their organization to easily report a potential threat or incident.

Reporting challenges can be mitigated through training and awareness, obtaining buy-in and support from leadership, clearly articulating policies and procedures, emphasizing helping (not hurting) peers, and ensuring the protection of privacy.

Employees and members should be trained to recognize abnormal or concerning behaviors. Whether it is a clear threat, an expression of intent to do harm, some type of leakage of violent thought (communication to a third party), an inappropriate statement, working or accessing the facility at unusual hours, or trying to access restricted areas, employees observing the behavior should report to ensure appropriate exploration, monitoring, or investigation.

☐ Employ Technology and Tools to Identify Concerning Behaviors

In addition to using people to report behaviors to a threat management team, technological mechanisms can be installed, providing an additional avenue for identifying concerning behaviors and reporting them to the organization. UAM, User Behavior Analytics (UBA) software, and access control systems can provide context on user behavior. These systems can monitor assets, track movements, and send alerts and reports to an insider threat team.

In general, UAM software monitors the full range of a user's cyber behavior. It can log keystrokes, capture screenshots, make video recordings of sessions, inspect network packets, monitor kernels, track web browsing and searching, record the uploading and downloading of files, and monitor system logs for a comprehensive picture of activity across the network.

UBAs are similar to UAMs except they use machine learning to look at endpoints, networks, hosts, and cloud environments that users are accessing to find outliers. In addition, access control systems employ technology to track, control, and monitor facility access and the physical movements of people.

Tools that can improve an organization's capability to protect its networks, systems, facilities, and members from insider threats include:

Database monitoring – tracks database transactions and blocks unauthorized transactions from being performed

Whitelisting – blocks any unauthorized program from being placed on a network without permission

Privileged Access Management technologies – prevent insiders from accessing certain systems, applications, or facilities without the proper permissions. These systems use passcodes, session management, and access management

Access control systems – track, control, and watch access and movement within and around facilities. Examples include: proximity cards, biometric systems, fingerprint recognition, facial recognition, keypads, and security cameras. These systems can be web-based so that they can fully integrate into an organization's IT architecture

Network flow analysis – monitors data packets to see if the communications leaving a host network are between malware and another command-and-control server. This is important because insider threats can use malicious data packets to siphon intellectual property from an organization's network

Security Information and Event Management Systems – collect, analyze, and report on log and event data in real time to provide threat monitoring, event correlation, and incident response

Data loss prevention – allows organizations to secure communications across email, endpoints, the web, networks, and the cloud before it leaves the host network so information is not leaked. Some tools can also block, monitor, or alert when a USB or external device is connected to a computer. Additionally, other data loss prevention tools can initiate emails or pop-up messages to employees and supervisors when employees attempt to send out attachments

An organization should notify its employees that it is monitoring networks and systems activity by having associates sign UAM and UBA acknowledgment and internet user policy agreements and regularly reminding individuals through network banners that the systems are active. Organizations should employ multiple technological tools, especially as the organization grows and matures. An organization should ensure it can configure the tools to look for and alert to specific behaviors related to what it values. Remember, technology only enhances the ability of an organization to detect and identify, assess, and manage insider threats. Insider threat cases require a skilled analyst or investigator to interpret and make sense of data.

The Ponemon Institute's 2020 Global Report on Insider Threats includes a valuable listing of the most frequently used tools and activities to reduce the cyber threat from a trusted insider (see figure 9).

Figure 9. Tools and Activities Employed[41]

Security Tools and Activities that Reduce Insider Threat	Frequency of Companies	Percentage of Companies
User training & awareness	112	55%
Data loss prevention (DLP)	110	54%
User behavior analytics (UBA)	102	50%
Employee monitoring & surveillance	96	47%
Security incident & event management (SIEM)	91	45%
Incident response management (IRM)	89	44%
Strict third-party vetting procedures	87	43%
Threat intelligence sharing	85	42%
Privileged access management (PAM)	80	39%
Network traffic intelligence	77	38%

[41]Ponemon Institute LLC. (2020). 2020 Cost of Insider Threats Global Report. (p. 23). Retrieved from https://www.observeit.com/cost-of-insider-threats/

☐ Establish a Threat Assessment Methodology and Risk Rubric

The data and information collected as part of the insider threat mitigation program will drive a threat assessment process. Threat assessment is a unique discipline that requires extensive knowledge in the detection and identification, assessment, and management of threats.

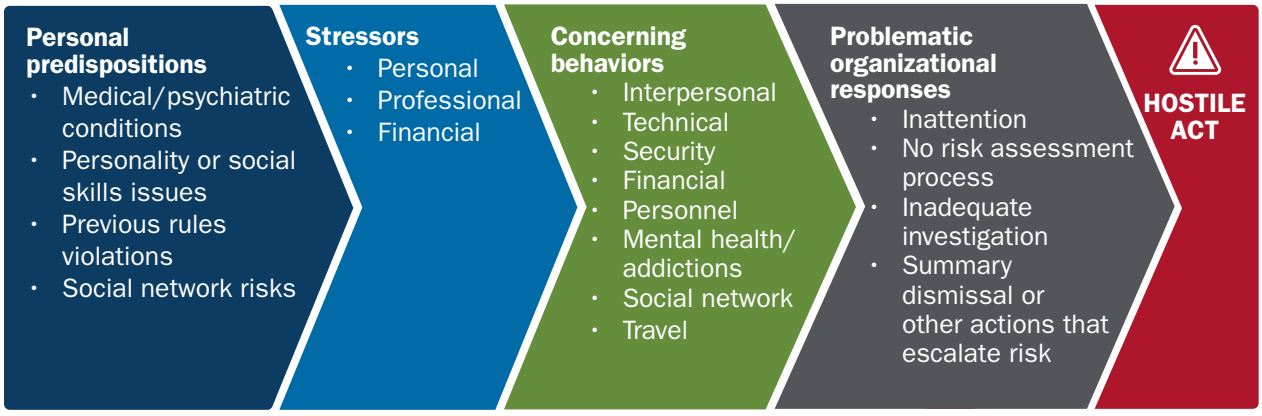
History and empirical research have shown that those who have committed malicious acts followed a predictable pathway. As a best practice, organizations should begin their threat assessment by using a general risk tool to determine if a person of concern is on a path to committing an insider threat incident. Next, they should use additional tools, such as risk rubrics and data analytics, to confirm their findings or to determine how quickly an insider threat is progressing.

Effective insider threat mitigation programs are frequently built around one or more evaluation frameworks, risk rubrics, or data analytic tools. Some risk rubrics are created based on empirical research on the threat expression in question (violence, cyberattacks, theft of intellectual property, etc.), while others are more generalized and solely used to determine if an individual is a potential threat based on concerning behaviors. It is essential that organizations identify these types of enabling tools and technologies early in the development process of their insider threat mitigation programs since these tools and technologies will frequently form the core of the planning, training, and implementation processes to follow.

It is important to avoid an overreliance on risk rubrics or data analytic tools. Organizations must have a threat management team to analyze a person of concern's predispositions, behavior indicators, and stressors to determine whether they are on a path to action and, if so, how fast are they moving and if intervention is possible.

The Factors Along the Critical Path to Insider Risk (figure 10)[42] is one such model that organizations should consider. It is an evaluation framework used to assess if a person of concern poses a general risk to an organization. Created by Dr. Erik Shaw and Laura Sellers, it demonstrates that the pathway from disgruntled individual to a hostile act is the accumulation of predispositions and stressors, possibly triggered by a maladaptive organizational response to that individual's concerning behaviors.

Figure 10. Factors Along the Critical Path to Insider Risk



[42]Adapted from Shaw, E. & Sellers, L. (2015, June). Application of the Critical-Path Method to Evaluate Insider Risks. Internal Security and Counterintelligence. Studies in Intelligence 59(2) pp. 1-8. Retrieved from https://static1.squarespace.com/static/596a623ba5790afcec9c024e/t/59c9e849cd39c3877ffc5098/1506404436555/Shaw-Critical+Path-June-2015.pdf

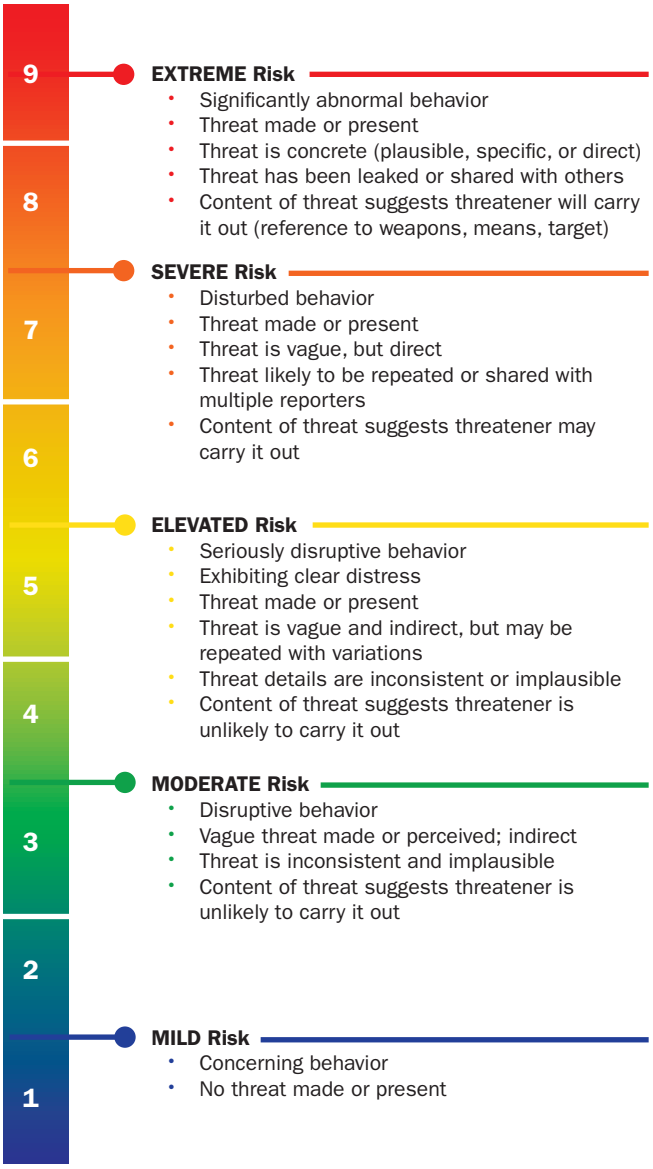
Risk Rubrics

Risk rubrics are evaluation tools, such as categories or scales, that use a rating or categorizing system to indicate whether an individual poses a low/medium/or high risk of committing violence, theft, sabotage, etc. Risk rubrics can either be generic or threat-specific and customized based on an organization's threat criteria and acceptable level of risk.

Risk rubrics work in conjunction with intervention strategies as each risk level should be assigned potential management solutions based on the concerning behaviors observed or reported at each level.

Threat management teams should use a risk rubric to initially assess and then re-assess a person of concern's specific level of risk to determine if the individual is progressing toward a malicious act and, if so, at what rate. It is important to note that these models are best used after a person of concern has been identified and is demonstrating behavior consistent with progressing toward a malicious act. Establishing baseline behaviors will make deviations or anomalies stand out from normal activities. Figure 11[43] is an example of a notional scale risk rubric for determining a general risk to an organization.

Figure 11. Notional Risk Rubric



Additionally, a wide array of data analytics methods, tools, and techniques exist to assess potential insider threats, including computer-based learning, rule-based algorithms, correlation algorithms, pattern recognition, statistical inference, and cognitive behavioral computing, to name a few. These approaches require data sets, metrics, identity and behavior attributes, member privilege and access rights, organizational risk control profiles, and historical examples of malicious insider incidents for each threat expression to be able to analyze and predict potential insider threats. While data analytics shorten the detection time of an insider threat, these systems still require an experienced investigator to review the data for accuracy and contextual understanding.

[43]Adapted from National Behavioral Intervention Team Association. (2019). The NaBITA Risk Rubric; The NaBITA 2019 Whitepaper. Retreived from https://cdn.nabita.org/website-media/nabita.org/wp-content/uploads/2019/04/17142743/NaBITA-2019-Whitepaper-Final1.pdf

☐ Establish a Multi-Disciplinary Threat Management Team

A multi-disciplinary threat management team is perhaps the single most important feature of an effective insider threat mitigation program. This entity will provide the analysis and management strategies an organization will consider to mitigate insider threats. A team with a well-rounded composition of diverse members provides a versatile group of practitioners who bring a variety of perspectives, capabilities, and backgrounds to address concerns.[44] The truth of a situation can be best ascertained and understood with this comprehensive approach to assessing the facts and data.

When forming the team, ensure a multi-disciplinary approach by including different entities from within the organization. Consider the following:

- **Leverage organic and existing functions**
- **Involve external resources**–on a case-by-case basis
- **Gather information from trusted sources**
- **Retain an insider threat analyst**–for entities of substantial size, complexity, or risk

Threat management depends on the synthesis and analysis of many diverse information sources; therefore, the team should be comprised of trusted staff that possess a fundamental knowledge across a wide range of functional disciplines and representatives from departments within the organization. They should be experienced individuals, often with investigative backgrounds, who can understand the thought processes of potential threats. Team members should value integrity, be creative, have a curious mindset, and have a relentless desire to protect the organization. Membership can include:

Organic and Existing Functions

- Chief Security Officer (CSO), Security, Program Protection
- CIO, CISO, IT Functions
- Operations & Administration
- General Counsel and Chief Privacy Officer
- HR, Equal Employment Opportunity
- Data Owners

External Resources

- Law Enforcement or Investigative Offices
- Risk-Screening Professionals
- Counselors, Medical, or Mental Health Professionals

Trusted Sources

- Supervisors and Coworkers
- Other Responsible Adults

Dedicated Insider Threat Capabilities

- Counterintelligence

Each of these disciplines plays a key role in the insider threat program as each has access to information or a perspective that others in the organization typically do not. Together, the team will be able to contextualize anomalous behavior and determine the most appropriate response actions. Figure 12 provides an example of a notional insider threat management team.

[44]Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 71). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Because the team will be interacting with protected and private information and serious allegations with significant consequences, consider vetting the individuals extensively before they join the team. Organizations should require team members to complete continuous specialized training for mental health guidelines; the laws and regulations regarding collection, integration, retention, and safeguarding of data; civil liberties protections and privacy laws; and how to conduct interviews, refer to investigations, and request referrals or prosecution. Organizations should arrange for regular, and even unannounced, audits from an external team to ensure that individual information and privacy is protected.

Figure 12. Notional Insider Threat Management Team

Team Labels, Formation, and Operation

The perceptions of the employees or members within an organization are an important consideration when establishing the team. The label selected will inform the perceptions and participation of the members. A name that reinforces the helping nature of the program is advisable. For example, consider names such as the Incident Management Team, Case Management Team, or Crisis Action Response Team.

The team should have a designated leader and a regular schedule to consider new developments and manage cases. It is a good practice to provide several team members with the authority to convene the team when a situation or fact pattern demonstrates the risk of an event, compromise, or act of violence is imminent.

It is important for the team to identify its assessment limitations as it is being established, not when taking on cases.

- At a minimum, threat management teams should be able to assess a general threat risk to an organization.
- If a more thorough or specific threat assessment is needed beyond the capabilities of the management team, then the team should have a referral process for the use of outside resources. For example, the possible threat of espionage or terrorism might require a deeper background check on the person of concern or the involvement of cyber analysts.
- If an organization is lacking a needed discipline, a memorandum of agreement should be established with an external entity for specialized support.

Teams should act quickly upon initial reports of a person of concern, violent incident, or technological indicator of insider threat behavior to gather information. Typically, the information will be scattered and fragmented, coming from automated systems or from the reporting

of employees or associates. The information will be pieces of a puzzle and will need to be assembled to determine if an individual poses a threat and is progressing toward a malicious insider incident.

Assessments should consider the following:

- Risk factors, concerning behaviors, stressors, precipitating events, the environment, and predispositions
- Insider threats follow a logical and detectable progression from ideation to action
- A person may leak or communicate ideas and plans for action to a third party

Why threat management teams work:[45]

- No one individual is positioned to see every single risk factor, warning behavior, or mitigator, nor is one single person positioned to manage a threat.
- When a threat management team receives a new case for review, individuals may recognize an important detail due to their particular skill set, whereas other team members may not initially realize its importance.
- A team member may ask a question during the consultative process that prompts others to think in a different way. This in turn could lead to a more accurate assessment and a more creative, and ultimately successful, threat management strategy.
- Consensus, derived from individual assessments of team members acting in concert, is the most powerful method to assess and mitigate future concerns.
- Open discussion and professional debates or disagreements are embraced.
- Diverse perspectives can generate new investigative leads and can prompt additional areas for inquiry, thus allowing for a more complete, holistic, and accurate threat assessment and management.

Use of a Behavioral Scientist on a Threat Management Team

As noted in detail later in this *Guide*, the use of a behavioral scientist in the assessment of potential insider threats is a best practice for insider threat teams. They are uniquely qualified to determine the potential contribution(s) of psychological or personality disorder issues, previous violations, social network influences, and stressors on a person of concern. While they are an excellent resource, it is critical that they have specialized training in insider risk assessment methods, including violence risk assessment. Too often in organizations, a person of concern is referred to a therapist untrained in violent risk, such as an EAP therapist. In addition, the therapist often is provided only limited information on the concerning behaviors, resulting in a missed or an under-assessed threat. As with other specialized skill sets, support from a Behavioral Scientist may be obtained on an as-needed basis to support threat management team activities. To understand the roles and contributions of a behavioral scientist in insider threat assessment, see the descriptions included in Chapter 5, *Assessing Insider Threats*.

[45]Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 71). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Training for Threat Management Teams

Threat assessment professionals require specialized training. Whether using organic assets or an outside expert, organizations must ensure the threat assessor is trained on a range of specialized topics and is aware of all relevant laws and regulations.[46] Training for a threat management team should include detailed and comprehensive training covering the behavioral or psychological aspects of insider threats, violence (workplace and intimate partner), violence risk screening, investigative techniques, incident resolution, and management or intervention strategies as well as the broad range of insider threat indicators discussed in Chapter 4 of this *Guide*.

At a minimum, the threat management team should receive training in basic threat assessment, safety, suicide prevention, legal considerations, and domestic violence. Training regarding the basics is available, often at no cost, from community groups or specific agencies that provide support services.

This training, along with critical thinking for analysts, privacy and civil liberties, personal security, de-escalating and preventing targeted violence, and active shooter awareness, can equip threat management team members with the knowledge, skills, and abilities required. The best way to achieve training objectives is for the threat management team to receive this training from outside specialists or subject matter experts with experience in insider threats.

On-the-job training should include table-top exercises covering an array of simulated threats to allow the team to talk through the process of recognizing behaviors, assessing a person of concern, suggesting intervention strategies, and understanding their roles and responsibilities during a case.

☐ Documentation and Recordkeeping

The documents generated in support of an insider threat mitigation program need to be collected, retained, and disposed of in accordance with the policies set forth by the organization. These policies should address the retention, disposition, and access to the records as well as security and auditing.

A program should use a system of centralized recordkeeping, making sure that reports, logs, interventions, etc., are recorded and tracked. Insider threat program personnel should be trained on laws and regulations regarding the protection of insider threat records. Both hardcopy and digital records should be kept secured, and all information contained in the records should be handled with the highest degree of confidentiality and shared on a strict need-to-know basis. Insider threat program personnel should also be required to sign non-disclosure agreements before being given access to program records.

It is a best practice to document every report that a threat management team or organization receives to improve the likelihood of successful prevention. One assessment that results in *concern unwarranted* can change to a *need for intervention* at a later date based on the nature of subsequent reports that demonstrate changes in the person of concern's environment, predispositions, stressors, or behaviors.

Accurate records are also beneficial if a person of concern moves out of their immediate area, especially if the person of concern is part of an ongoing investigation for theft or sabotage. It may be necessary to pass their records to law enforcement to prevent future threats or incidents at a new location.

[46]Interagency Security Committee. (2019). Violence in the Federal Workplace: A Guide for Prevention and Response. (pp. 49-50). Retrieved from cisa.gov/publication/isc-violence-federal-workplace-guide

III. Train and Execute

☐ Sell the Program

Successful programs require committed support from all levels within an organization. Selling the program will require an organization to communicate the costs of their insider threat mitigation program in terms of cultural and operational impacts, as well as financial.

Start by framing the program in the context of the organization's values. Organizational leader and member buy-in can provide the program with the explicit authority and legitimacy it requires to be effective.

Define the program's principles and share the privacy and civil liberties protections. Insider threat programs examine personal data as part of the investigative process. It is critical that the program guarantee the protection of private information to gain program acceptance.

Emphasize the organization's return on investment by revealing what could be lost with a successful insider incident. The loss of jobs, revenue, organizational capabilities, market edge, market share, and brand reputation, among other negative consequences, are elements that can help unify an organization's people in support of a program.

☐ Encourage a Culture of Reporting

Managing the potential consequences of an insider incident is the ultimate goal of an insider threat mitigation program. To do this, an organization needs to know that a potential threat exists. A culture of reporting creates an intervention opportunity when people see something or say something, paving the way for the early detection and identification of possible insider threats.[47]

According to accounts from some of the most devastating insider threat incidents, people often knew something was wrong but did not report their suspicions. Approximately 2 million people each year report some type of workplace or organizational violence, yet, estimates are that 25 percent of violence goes unreported.[48] Colleagues and associates often feel overwhelmed or fearful of reporting.

An insider threat mitigation program should guide positive change by encouraging members of an organization to hold their organization and their peers accountable and report suspicious behavior to guide positive change in the environment. Suggestions for developing a culture of reporting include:

- Enabling anonymous reporting
- Developing an online reporting system
- Encouraging reporting by associated individuals
- Accepting reports from outside of the organization (family, friends, etc.)
- Developing an amnesty policy to eliminate any fears or misconceptions of reporting
- Encouraging participatory culture and instilling upward communication
- Considering availability and accessibility of reporting
- Protecting individuals who report from the possibility of retaliation
- Acting when threats are reported so employees know reports are taken seriously

[47]U.S. Department of Homeland Security. (n.d.). If you see something, say something® . Retrieved from https://www.dhs.gov/see-something-say-something

[48]Ricci, D. (2018). Workplace Violence Statistics 2018: A Growing Problem. AlertFind. Retrieved from https://alertfind.com/workplace-violence-statistics/

Putting monitoring programs in place may cause employees to feel uncomfortable. There are a number of best practices that organizations can put in place to ensure that employees view monitoring programs as good-faith security efforts, and not negative surveillance, including:

- Maintain transparent and open documentation concerning the monitoring.
- As part of insider threat program procedures, ask that employees or organizational members sign non-disclosure agreements when making a report.
- For employees that are unionized, organizations should secure union support for their insider threat program to bolster employee confidence the program is security-focused versus punitive.
- Ensure reporting is valued and treated with discretion. Organizations that have a confidentiality program members can use to report suspicious behavior show an increase in suspicious incident reporting.[49]

☐ Implement a Formal Training & Awareness Program

Training and awareness are key processes in an effective insider threat program. All organizational personnel, to include members, contractors, and consultants, should receive training to prevent a malicious insider threat. A highly aware and properly trained membership is key to early detection and prevention of an insider threat, as they can act as sensors who can report anomalous or unauthorized activity or concerning behaviors.

What Should Be Trained?

An organization should teach its members to recognize insider threat indicators, the concerning behaviors that could lead to an incident in the organization, and how to report. Organizations should include the following topics in their training program:[50]

- **Insider Threat Awareness Training** that defines the distinct types of insider threats and describes the motivations and possible behaviors associated with each type. This training should supply specific examples of insider threat activities that might be encountered.
- **Insider Threat Reporting Training** that instructs the organization's policy on how to confidentially report suspected or concerning activity.
- **Physical and Information Security Training** that defines how to protect oneself, one's personal information, and information entrusted by the organization.
- **Employee or Member Security Policy Awareness Training** that effectively communicates an organization's acceptable use policies and the intent to pursue and prosecute crimes against employees or members who violate those policies.
- **Classification Policy Training** that covers the proper handling of sensitive and/or classified documentation and items.
- **Agreements Training** that covers the requirement for all employees, members, contractors, and other trusted insiders to sign **acceptable use policy, non-compete, non-disclosure, and non-solicitation agreements** as well as the content of these agreements.

[49] Intelligence and National Security Alliance. (2013, September). A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector. (p. 2). Cyber Council: Insider Threat Task Force. Retrieved from https://www.nist.gov/system/files/documents/2017/06/08/20131213_charles_alsup_insa_part4.pdf

[50] Kowalski, E., Conway, T., Keverline, S., Williams, M., National Threat Assessment Center, & et al. (2008, January). Insider Threat Study: Illicit Cyber Activity in the Government Sector. (p. 26). Software Engineering Institute | Carnegie Mellon. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52247.pdf

The governance group should receive additional specialized training on:

- The laws and regulations regarding collecting, integration, retention, and safeguarding of sensitive data
- Civil liberties protections and privacy laws
- The Insider Threat Response Plan
- How to refer to investigations, and request prosecution
- Threat awareness training based on functional roles

How Often?

Insider threat awareness and mitigation training should be continuous. It should begin as soon as access has been granted to a facility and networks as part of an onboarding program or assigned with a due date. Refresher training typically takes place annually; however, refresher training of critical information can be scheduled as often as the organization deems necessary. The training can be in person or online via an Automated Learning Management System. It is a best practice to supplement training with products that reinforce organizational policies, including posters, newsletters, alert emails, and all-hands meetings. Training should be documented, recorded, and tracked.

There are a range of training resources available with tools offered from DHS agencies, such as CISA, FEMA, and United States Secret Service (USSS); the CDSE; and the NITTF. See Appendix C of this *Guide* for useful tools and resources that can be integrated into training.

IV. Evaluate and Improve

☐ Conduct Exercises

Organizations should use exercises to evaluate the training and effectiveness of their insider threat program and Incident Response Plan. Exercises will help determine whether the program's goals and objectives were met, if the insider threat's actions were predicted, and if the policies outlined in the plan led to a successful response. After action reports provide feedback and lessons learned from the exercises that inform program revisions and future training needs.

When testing an organization's capabilities, it is important to use a progressive exercise approach. Use a crawl, walk, run method to develop an exercise plan. Start slowly with small, discussion-based exercises used to test an organization's knowledge of insider threat indicators and reporting requirements and build to a full-scale insider threat event operational exercise.

Progressive exercise programs enable organizations to take part in a series of increasingly more complex scenarios, with each successive exercise building upon the previous one until mastery is achieved. FEMA's Homeland Security Exercise and Evaluation Program serves as a useful guide for the design, execution, and evaluation of progressive exercises.[51] FEMA also offers independent online training courses for exercise design and development and how to serve as an exercise evaluator.

[51]FEMA. (2020, August 05). Homeland Security Exercise and Evaluation Program. Retrieved from https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

☐ Maintain the Program

To keep the insider threat program current, the governance group should establish a formal maintenance process for reviewing and revising the policies, procedures, standards, and legal obligations. The maintenance process should be a recurring activity with tasks scheduled monthly, semiannually, and annually. A program maintenance schedule should be included in the program's operating procedures, and precise records of reviews, revisions, deletions, and additions should be captured.

To help the program mature, the governance group and threat management team members need to remain current on evolving best practices and tools while benchmarking other programs and studying lessons learned from insider threat cases. An insider threat mitigation program should continuously evolve because the threat landscape is continually transforming, technology is upgrading or becoming obsolete, organizations reconfigure or try new processes, the market fluctuates, lessons are learned, information and insights are obtained, and priorities are adjusted.

The governance group should consider reviewing and updating the program after any of the following events:

- The resolution of an insider threat case
- A change in operational resources (e.g., personnel, organizational structures, management processes, facilities, equipment, or technology)
- A formal request to update the policies, procedures, or standards
- The introduction of new or amended laws or ordinances
- A change in the risk acceptance appetite of the organization

☐ Provide Oversight and Compliance

An important concept in insider threat mitigation is ensuring that there is a means in the organization to watch the watchers. Organizations should designate officials who will conduct independent assessments of the program's compliance with insider threat mitigation program guidelines and policies, particularly due to the highly sensitive nature of the data to which the team has access. This oversight activity will enable the program to continue to learn and improve, provide accountability for those entrusted with insider threat monitoring activities, and provide credibility to leadership, the governance team, and the organization's members.

Concluding Thoughts

The program management elements offered in this *Guide* can help any organization, small or large, establish an effective insider threat mitigation program. Applying these practices and concepts and tailoring them to an organization's environment can provide a means to protect what the organization values while deterring harmful and illegal behavior.

As noted, the program should not be focused on catching people doing things wrong. Rather it should be grounded in the notions of helping people avoid mistakes, providing a safe environment, and preventing insider incidents from occurring while mitigating the potential risks before an issue escalates to theft, sabotage, espionage or, especially, violence.

Case Study

Establishing an Insider Threat Mitigation Program

During a first person interview in support of this *Insider Threat Mitigation Guide*, leadership from a large manufacturing corporation described how they established an insider threat program to manage and mitigate its loss of intellectual property, the theft of which could cost the company millions of dollars.

FIRST STEPS

Implementation of the company's program began by obtaining corporate leadership support through enumerating the potential loss to company revenue, market share, and market edge. Critical to the program's approval was the definition and subsequent allocation of resources necessary to fund and sustain the program.

The company chose its threat management team members from professionals with investigative (i.e., counterintelligence or law enforcement), legal, HR, and IT backgrounds. This ensured that its investigations were accurate, legal, and ethical. Further, corporate leadership instituted policies requiring internal and external audits of the insider threat team to ensure its integrity and adherence to the protection of private information.

DEVELOPING THE PROGRAM

The insider threat team was first tasked with determining which intellectual property was most valuable, how to identify when the property was at risk, and how best to protect the property. Next, the corporation used its internal technological tools to fuse data from HR, physical security, insider tips, outside leads, and real-world developments to create a risk database. The company developed a life cycle process that incorporated and analyzed new information entering the database. Over time, a database of successful cases was developed, allowing the corporation to generate metrics which led to predictive analytics for identifying high-risk threats.

CHALLENGES ADDRESSED

One of the most important challenges corporate leadership had to address was communicating program information to the staff. Message content, the means of delivery, tone and tenor, and frequency were some of their considerations. The company decided that messages would be disseminated quarterly that would feature stories of intellectual property theft and its devastating impacts. The resulting communications reminded the staff that an insider threat program was active, that it focused on the company's intellectual property, and that regardless of an individual's motivation or seniority, there would be consequences.

IMPACT OF THE PROGRAM

Since the inception of the program, the organization's insider threat team has been able to disrupt the potential theft of highly valuable intellectual property as well as successfully recover stolen proprietary information. Its managers stated that the program has paid for itself hundreds of times over.

Key Points

Principles and Keys for Success

- **Promote a protective and supportive culture** throughout the organization.
- **Safeguard organizational valuables** while protecting privacy, rights, and liberties.
- **Remain adaptive** as the organization evolves and its risk tolerance changes.
- **Focus on prevention** and helping people versus just catching them doing things wrong.
- **Employ a balance of positive and negative incentives**, promoting employee satisfaction and performance while avoiding overly aggressive reactions following notification of a threat.

Plan

- **Visibly involve executive or senior leaders** in emphasizing the program to drive positive support.
- **Appoint a single individual, commonly called the Senior Official**, as the responsible official for the overall management and oversight of the program.
- **Form a governance group** consisting of multiple stakeholders who possess information pertinent to the background, conduct, and activities of trusted insiders.
- **Establish guiding principles** that align to the culture and business of an organization and describe its purpose, goals, and objectives.
- **Sell the program** to leadership, members, and associates by **describing why it is being established**; a key element is to emphasize the collective harm an insider can pose, particularly in a business setting.
- **Start small, using existing capabilities and resources**; use programs such as harassment and/or violence prevention as a practical starting point for a broader insider threat program.
- **Identify, track, and monitor the organization's critical assets.**

Organize and Equip

- **Employ the fundamental elements for an effective operational program—information, technology, people, reporting paths, and skilled investigators**; when the elements are fused, an intricate pattern of abnormal behavior indicative of insider threat activity can be recognized.
- Grow a program by employing **automated tools or dedicated personnel based on the type and size of an organization and its culture**, the nature and value of its mission, and its risk tolerance toward insider threat incidents.

- **Augment technology with a skilled investigator** to interpret and make sense of data.
- **Develop an Insider Threat Incident Response Plan** inclusive of the scope, established roles and responsibilities, methodology, incident response phases, guidelines for incident response processes, reporting procedures, and an escalation chain.
- **Develop and employ risk rubrics as evaluation tools** to rate or categorize insider threats to indicate whether an individual poses a low/medium/or high risk of violence, theft, sabotage, etc.
- **Customize risk rubrics** based on an organization's threat criteria and acceptable level of risk.
- **Establish a threat management team** to assess and manage insider threats; it is the backbone of a threat management program and is integral to the program's success.
- **Staff the team with a wide range of functional disciplines and representatives**; threat management depends on the synthesis and analysis of many diverse information sources.
- **Consider alternative naming conventions for the threat management team**—one that reinforces the helping nature of the program is advisable.

Train and Execute

- **Instill a positive culture for reporting and supply confidential means of reporting.**
- **Emphasize the need to prevent insider threat actions before they occur**; educate the workforce or membership about the potential consequences of insider threats.
- **Train employees on insider threat awareness and reporting** and encourage participation to help detect and identify, assess, and manage insider threats.

Evaluate and Improve

- **Regularly exercise the insider threat mitigation program**, update its policies using a conditions-based as well as a temporal-based approach, and conduct regular audits of the program to ensure oversight and compliance.
- **Designate officials who will conduct independent assessments of the program's compliance** with insider threat mitigation program guidelines and policies.

4 Detecting and Identifying Insider Threats

Successful insider threat programs proactively use a mitigation approach of detect and identify, assess, and manage to protect their organization. The foundation of the program's success is the detection and identification of concerning observable behaviors or activities. These behaviors may indicate that a trusted individual is at risk of becoming a threat to themselves, their associates, and/or the organization.

Insider threat research has shown that potential insider threat perpetrators evolve over time, moving as if on a pathway, and potentially exhibiting multiple, overlapping, detectable and observable behaviors. This research has established a number of potential threat indicators as well as a common understanding of the progression of an insider toward a malicious incident.

Detecting and identifying potential insider threats requires both human and technological elements. The people in the organization are an invaluable resource to observe behaviors of concern, as are those who are close to an individual, such as family, friends, and coworkers. These people will often understand an individual's life events and any related stressors, and may be able to put behaviors into context.

The insights gained from human observation should be supplemented with technology and tools that can help to detect anomalous cyber activity or unauthorized physical access, which are two of the indicators that can assist in detecting and identifying insider threats. A successful program will consider each of these tools and build a culture that encourages their use.

This chapter will discuss:

- **Threat detection and identification**
- The **progression of an insider threat toward a malicious incident**
- The wide-ranging **threat detectors** and **threat indicators** that can help an organization detect and identify those who may be progressing to violence or a harmful insider act

Threat Detection and Identification

Threat detection and identification is the process by which persons who might present an insider threat risk come to the attention of an organization or insider threat team, frequently as a result of observable concerning behaviors.

As the body of knowledge for insider threat detection and identification continues to grow, researchers with the Defense Personnel and Security Research Center have identified **four core behavioral principles** to consider:[52]

1. The risk of becoming an insider is not randomly distributed across any population. **Certain individuals are more likely to pose threats**.
2. Insider threats occur in a social context. **Certain environments are more likely to facilitate insider threat behavior**.
3. **An individual's transformation from a trusted insider to a malicious actor is a process**, not an event.
4. **High-impact, low-frequency insider threat behavior correlates with and is preceded by common indicators** that can be observed, modeled, and mitigated.

Research assessing risk of targeted violence concluded that most offenders did not threaten their targets directly but displayed identifiable behaviors that reflected a potential insider threat, making detection a realistic and achievable goal.

Detection and identification will vary depending on threat expression and manifestation. For example, non-violent insider threat expressions are primarily detected through technological indicators with peers and bystanders secondarily identifying concerning behaviors or providing context, such as stressors or predispositions, to support the threat assessment. Conversely, violent threat expressions are typically detected and identified through direct reporting of concerning behaviors by peers and bystanders, with technology serving as a supplemental means of detection—in the form of hostile emails or other communications.

[52]Jaros, S. L. (2018, October). A Strategic Plan to Leverage Social & Behavioral Sciences to Counter the Insider Threat. | OPA-2018-082 | (p. 12). Defense Personnel and Security Research Center, Office of People Analytics. Washington, D.C. Retrieved from https://www.hsdl.org/?abstract&did=818886

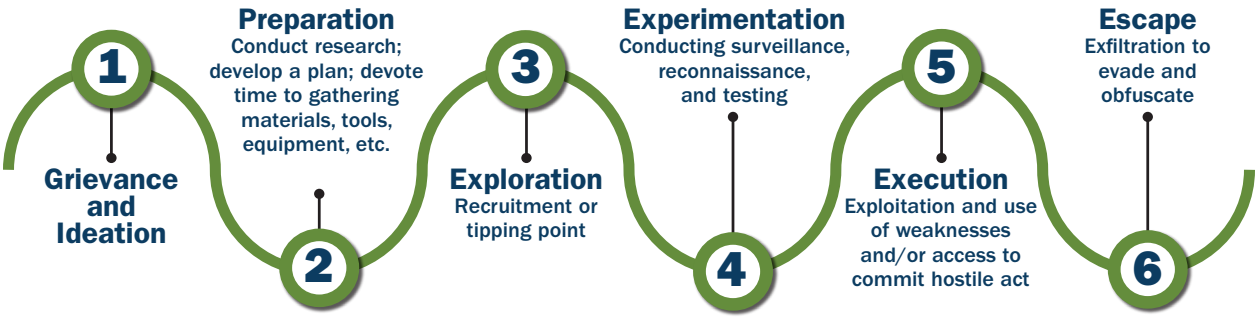
Progression of an Insider Threat Toward a Malicious Incident

While virtually every person will experience stressful events in their lives, the vast majority do so without resorting to disruptive or destructive acts. For those insiders that do turn to malicious activity, researchers have determined that the acts are rarely spontaneous; instead, they are usually the result of a deliberate decision to act.

Researchers of insider threats describe an evolution from trusted insider to insider threat as a critical pathway wherein the subject's personal predispositions and background, which make them susceptible to the temptation of a malicious act, interact with their personal stressors and the organizational environment, moving them down a pathway toward a malicious incident.[53]

Often, the perpetrator harbors resentment, displaying behaviors that may be observed and reported by peers and colleagues. The journey may be rapid or slow, and the path varies from person to person. Warning signs, stressors, and behaviors may be evident along the progression to action. A deeply held grievance or humiliation, whether real or perceived, is often the first step on a journey toward intended violence.[54]

Figure 13. Progression of an Insider Toward a Malicious Incident[55]



As illustrated by figure 13, the Progression of an Insider Toward a Malicious Incident, the coalescence of the factors presented below result in a path which can often be identified through an individual's behaviors. It is important to note that the mere exhibition of insider threat behaviors does not guarantee that an individual will commit a malicious act.

But once an individual begins moving down the pathway, they are more likely to act. Special attention should be given to individuals who may be close to resignation, disassociation, or termination. Individuals who have been unwillingly terminated or disassociated from an organization or association should be closely observed and the risk of violence assessed as their tenure comes to an end.

---

[53]Shaw, E. D. & Stock, H. V. (2001, December). Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall. White paper. (p. 7). Retrieved from https://static1.squarespace.com/static/596a623ba5790afcec9c024e/t/59c9e063a803bb62117213c0/1506402404657/Symantec+Malicious+Insider+Whitepaper+FINAL2.pdf

[54]Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 24). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

[55]Adapted from the National Cybersecurity and Communications Integration Center Analysis Team. (2014, May 2). Combatting the Insider Threat. (p. 32). Retrieved from us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf

1 Grievance and Ideation

The first step on the pathway is the initial expression of someone's distress or reason for complaint or resentment—a real or perceived wrong that takes on a highly personalized meaning for the individual. Or, it could be a stressor involving social, financial, or ideological concerns. No matter the reason, this is the starting point when an individual begins to progress from idea to action, an intentional choice to violate the organization's trust.

From a threat assessment context, these grievances can translate into behaviors related to a sense of mission, destiny, loss, or desire for revenge. Whether objectively rational or not, what matters is that the insider feels an urge to act to satisfy their feelings or sense of injustice, humiliation, anger, or other perceived deficit.

If the insider does not talk themselves out of the conceptual need, or the organization ignores the signs of their distress or does not adequately respond when it becomes aware, these grievances or stressors can grow and expand, moving them down the path toward a malicious incident.

2 Preparation

The idea or grievance will manifest in behaviors as the insider begins to conceptualize how they wish to carry out their plan to commit an insider or hostile act. Behavior reflects one's beliefs, feelings, and emotions, manifesting in observable actions. Preparation activities may involve research and the development of a plan.

The individual may also begin to acquire items needed to carry out the planned act, whether sabotage, theft, espionage, or violence. For cyberattacks, preparation may take the form of logic bombs (e.g., malicious code), stealing passwords, obtaining privileges, or other technological tools. For violent threats, preparation could include acquiring firearms, ammunition, explosives, or other weapons. Such behaviors may offer bystanders, colleagues, friends and family, or others the first opportunity to observe behaviors of concern that can help identify individuals on the pathway.

A majority of individuals do not advance beyond the Preparation phase in this pathway to action. Often the active fantasy of retaliation is sufficient to satisfy this disgruntlement. Others may talk themselves out of their conceptualized act based on interventions from their personal support networks or as a result of changes in the situation or setting that mitigate their stressors. They may be deterred by the threat of capture or accountability or find healthy outlets for their concerns.

3 Exploration

Before this stage, the person of concern may be uncommitted, wavering between action or acquiescence. However, at this stage something happens to cause the person of concern to commit to acting, a triggering point. This could be an additional stressor such as a loan coming due, a lack of attention from their target, or a dismissive response to their grievance from their organization.

During this stage, the malicious insider may begin to seek weaknesses in security, find new access points, or decide which data they want to destroy, misuse, or steal. The person of concern may also begin trying to recruit other like-minded individuals to assist in the act.

4 Experimentation

Surveillance, reconnaissance, testing, and rehearsal of the plan ushers in a dangerous phase along the pathway to action. Malicious insiders review and refine plans during this phase. An insider may attempt to begin surveillance of certain locations, attempt to infiltrate a building or technological system, appear in areas where they do not belong, or otherwise test boundaries within their organization.

Experimentation behaviors may extend over a length of time with insiders camouflaging their intent and attempting to dull others' awareness of or concern with their probing or breaching, actions that are designed to circumvent security to gain access to a target.

It is critical to note that if this type of experimentation behavior is detected by an organization, permitting an insider to continue with unacceptable behavior without correction, consequence, or even notification to authorities may embolden the insider.

5 Execution

With a hostile attack or violation formulated, planned, and rehearsed, the insider may now take advantage of their access and knowledge to execute their plan. If not disrupted, an insider incident can result in the theft of information, sabotage of equipment, or violence against colleagues or others.

6 Escape

Insider threats often develop an escape strategy prior to committing an insider incident. Depending on the type of action taken, escape may involve evading detection and distorting evidence of the act, such as shifting blame, altering records, or covering movement or malicious actions. In cases of a violent act, the insider may attempt to evade capture and arrest or commit suicide—either by their own hand or through intentional provocation of armed responders.

Some insider threats may focus on publicizing the malicious act by broadcasting stolen data, information, or intellectual property for the public's view. The actions taken during this stage may be adapted to cover a range of possible variations. After an incident, the insider may act alone or engage other complicit and non-complicit individuals to avoid or misdirect the immediate consequences of the act.

While this potentially ends the active threat from the insider, the consequences of their actions are often significant and can potentially continue for an extended period of time. This may be particularly true if the act involves the ongoing theft or misuse of proprietary data while the person of concern remains in place.

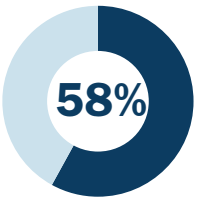
Threat Detectors

People as Sensors

Coworkers, peers, friends, neighbors, family members, or casual observers are the human component for the detection and identification of an insider threat. They are frequently positioned to have insight into and awareness of predispositions, stressors, and behaviors of insiders who may be considering malicious acts. Often, those who perpetrate violence and those who steal data or secrets leak their plans or grievances to others before acting. Some persons self-identify. They call, write, email, or approach a public official or figure or indicate an unusual or inappropriate interest in an entity. These individuals often give their names or provide other information that leads to identification. As figure 14, below, demonstrates, perpetrators frequently communicate their intentions in advance.

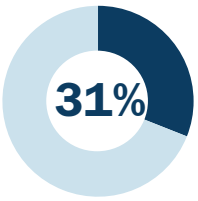
Figure 14. U.S. Secret Service and CERT National Insider Threat Center Studies

In **42 computer system sabotage incidents** throughout the critical infrastructure sectors:[56]



of perpetrators communicated negative feelings, grievances, and/or an interest in causing harm

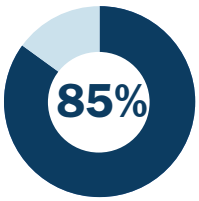
- **92%** verbally
- **12%** via email



of the time, others had information about the insiders' plans, intentions, and/or activities

- **64%** coworkers
- **21%** friends
- **14%** family members
- **14%** someone involved with the incident

In **27 violent attacks in public spaces**:[57]



of the attackers made concerning comments

- Expressing **interest in previous attackers**
- Making or suggesting **racist and misogynistic comments**
- Referencing a **desire to purchase a gun**
- Expressing **aspirations to commit future violence**

Figure 15. Considerations in Observing Behavior

Two Important Qualities to Remember When Observing Human Behavior

Listen through their frame of reference, not your own. Do not assume that somebody will ask for help or ask to be stopped, or that they will speak about their intentions in the same way you would.

Listen with your eyes. Peoples' intentions are often disclosed through nonverbal means.

[56]Keeney, M., Kowalski, E., United States Secret Service's National Threat Assessment Center, Cappelli, D., Moore, A., & et al. (2005, May). Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. (p. 16). Software Engineering Institute | Carnegie Mellon. Retrieved from https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf

[57]National Threat Assessment Center. (2019, July). Mass Attacks in Public Spaces – 2018. (p. 9). U.S. Secret Service | U.S. Department of Homeland Security. Washington, DC. Retrieved from https://www.hsdl.org/?abstract&did=826876

Insider threat mitigation programs can sensitize employees to indicators of concern and the value of their observations in detection. Employees and members should be taught the various threat indicators—such as the concerning behaviors and stressors—as well as the data on leakage to help them understand the role each person can play in detecting and identifying warning signs.

Emphasize listening at a deeper level, to include observation of body language. Context is a key element in assessing whether a person of concern is posing a threat. Figure 15 showcases two important qualities to remember when observing human behavior:

- **Listen with your eyes**. A person's behaviors and communications are often disclosed through nonverbal means. Pay attention to what people are saying with their expressions, emotions, and body language.
- **Listen through the speaker's frame of reference**. Individuals are different and will likely not discuss their intentions or needs in the same manner as others. Behaviors that some people find troubling or threatening may very well be another person's way of asking for help.

There are multiple potential options for intervening to mitigate an insider threat, but the most important action that a person can take is to convey what they know, observe, or fear may happen.[58] Individuals who hear concerning comments, threats, plans, leakage, or see social media posts should take them seriously and pursue proper reporting to supervisors, organizational leadership, senior managers, HR, or law enforcement, as appropriate.

Insider Activity Monitoring

Specialized technologies should be used in conjunction with human sensors to detect and prevent insider threats. Technological detection tools mine diverse datasets for anomalies, such as physical or computer access records, keystrokes or mouse clicks, or communication recordings. These tools can be helpful in the detection of abnormal behaviors by:

- Providing continuous monitoring that is automated and needs little direct engagement
- Notifying users when their credentials are used for login
- Mapping user privileges against their actual accesses to identify anomalous conduct
- Leveraging predictive analytics to identify potential offenders
- Identifying outlying behavior, such as an active user when others are inactive
- Seeing when sensitive data is accessed and by whom
- Flagging large downloads, file transfers, or other forms of data exfiltration
- Generating risk portfolios that allow management to prioritize protection of the most important or valuable data
- Identifying users who access or manipulate information outside the scope of their permissions, authority, portfolio, or need-to-know
- Discovering malware or compromised accounts
- Performing keyword and psycholinguistic monitoring of communications

Detection Tools

- UAM Software
- UBA Software
- Facility Access Control System
- Video Surveillance
- Web-monitoring Tools
- SIEM Tools
- DLP Tools

[58]Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 12). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Threat Indicators

Threat indicators are a person's behaviors, stressors, predispositions, and background that may indicate an increased probability that they will commit a hostile or malicious act. Important to this process is the understanding that behavior is what matters most, not the motivation, whether it is political, religious, ideological, financial, or revenge. While motivations are important in understanding what drives a perpetrator, it is the individual's behaviors and indicators that can help flag an individual for additional consideration, monitoring, or assessment.

Early detection of an insider threat remains challenging. Confirmation of any threat indicator requires a solid understanding of context and a holistic view of the person of concern. It is important to understand that a person may display behaviors representative of a particular point in their life that may not result in a direct expression of a threat. However, a person exhibiting multiple indicators should be flagged and reported for additional monitoring or investigation. Ongoing vigilance is necessary to detect and act upon threat indicators in a timely manner, as well as within the appropriate context to enable an intervention to prevent an incident.

The following paragraphs present a representative sample of possible indicators; it is not all inclusive.

Remember:

The presence of some, or even all, threat indicators does not mean an insider is an insider threat.

Nor does a lack of threat indicators guarantee an insider is not an insider threat.

Personal Indicators

Personal indicators are a combination of predispositional attributes and personal stressors reflecting on the events currently impacting the insider.

Predispositional indicators can include psychiatric or medical disorders, particularly those that influence judgment and self-control, such as alcoholism or compulsive behavior, a lack of social skills, the inability to get along with others, and a history of rule violations, criminal conduct, or convictions. Other predispositional indicators, such as narcissism, history of aggression or violence, psychopathy, or self-injury, can place individuals at higher risk for hostility, anger, violence, or suicide.

Even though personal indicators may require probing into an individual's life, peers and coworkers may have suspicions relating to the personal well-being of the insider that may be indicative of an emerging or continuing threat. Because of the sensitive nature of this type of threat indicator, it is important to be delicate and ensure compliance with all privacy, labor and employment law statutes, regulations, rules, and policies. This requirement will be discussed in further depth later in this *Guide*.

88%
of security authorities believe it is necessary to identify high-risk insiders based on their personal indicators and behaviors.[59]

Personal stressors are typically situations that cause strain or tension in an individual's personal or professional life. It should be noted that both negative and positive developments (i.e., demotion or promotion) can cause strain or tension in an individual. Though unexpected events can occur to anyone at any time, stressors can act as triggers to individuals with the potential to become an insider threat. This is especially true when the event involves an unmet expectation, such as a failure to win an expected award or promotion.

[59]Cybersecurity Insiders. (2018). Insider Threat 2018 Report. (p. 22). Retrieved from https://www.cybersecurity-insiders.com/wp-content/uploads/2016/09/Insider-Threat-Report-2018.pdf

Personal Stressor Examples[60]

- Serious physical, emotional, or mental health concerns
- Financial need
- Address change/move
- Death among family or friends
- Addiction (drugs, alcohol, gambling, etc.)
- Criticism from significant other, friends, coworkers, or employer
- Break-up or divorce
- Unmet expectations relating to role, responsibility, recognition, or compensation
- Legal problems

Additionally, employees may experience a subset of personal stressors identified as professional stressors originating from direct interactions with an employer. These may include:

- Demotion or failure to achieve anticipated advancement/promotion
- Loss of seniority or status in merger or acquisition
- Disagreements regarding intellectual property rights
- Transfers/relocation
- Disappointing performance review
- Conflict with coworkers
- End of contract
- Termination

Professional stressors have the additional effect of creating potential grievances against an employer, organization, or agency. An individual may feel disrespected and see the hostile action as a way to gain respect, or they may feel the need for revenge against an organizational policy, management, peer, or a specific decision. These stressors may become the justification in an individual's mind for hostile acts. As such, organizations should educate their members or employees of the potential indicators.

Background Indicators

Background indicators are events that happen before an individual is hired by an organization or prior to an individual gaining access. They are typically not observable by peers, supervisors, or HR, but are identified through an objective screening of an individual's historical records. These background checks are common prior to an individual joining an organization, especially where insiders will gain access to sensitive information or systems. It is important to note that individuals can and will withhold personal and background information, even if its disclosure is mandated for their association or employment with an organization.

An in-depth background check may be necessary to acquire the information needed to identify a potential insider threat. Organizations should not shy away from comprehensive background checks for fear of perception, legal issues, or union issues, especially those that include viewing a person of concern's mental health records or public social media profiles. The data collected during these checks can provide insight into which type of threat an insider may express, as well as potential countermeasures to be applied if that threat does manifest. Organizations are strongly advised to involve legal counsel when requesting background records to ensure compliance with privacy, Health Insurance Portability and Accountability Act, and federal, state, local, or other laws.

[60]Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., Osula, A., (n.d.). Insider Threat Detection Study. (pp 29-30). NATO Cooperative Cyber Defense Center of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Background Indicator Examples[61]

- Involvement with individuals or groups who oppose core beliefs or values of the organization
- Engagement in activities that may represent a conflict of interest with the organization
- Addiction (alcohol, drugs, gambling, etc.)
- Multiple short-term employments
- History of emotional or mental health concern
- Spending exceeds income
- Criminal record
- Concerning business relationships
- Social/Professional network concerns

Behavioral Indicators

An individual's behaviors reflect patterns of normal or benign activity based on the way the insider interacts within the organization or on its network. Over time, these behaviors create a baseline of activities from which changes may be considered a threat indicator. Unlike personal and background indicators, which typically require an examination of the person of concern's life, behavioral indicators are directly observable by peers, HR personnel, supervisors, and technology.

[61]Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., Osula, A., (n.d.). Insider Threat Detection Study. (pp 31-32). NATO Cooperative Cyber Defense Center of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Behavioral Indicator Examples[62]

- Unwillingness to comply with established rules, procedures, or organizational policies
- Observable resentment with plans of retribution
- Excessive or unexplained use of data copy equipment (scanner, copy machine, cameras)
- Making unapproved contacts with competitors or business partners
- Discussions of new opportunities or of resigning from current position
- Excessive overtime work, or working odd or late hours without reason or authorization
- Bringing personal equipment into high-security areas
- Carelessness or impulsiveness
- Inappropriate statements, jokes, or bragging
- Poor social interaction or social withdrawal
- Disgruntlement toward peers due to perceived injustice
- Increasingly erratic, unsafe, or aggressive behaviors
- Repeated breaches of rules, procedures, or organizational policies
- Litigiousness
- Exploitable behavior (including excessive gambling, sexual misconduct, drug and alcohol use, or criminal activity)
- Excessive volunteering that elevates access to sensitive systems, networks, facilities, people, or data
- Financial difficulties or unexplained financial gains
- Taking multiple, short unexplained trips outside the U.S.
- Efforts to conceal foreign travel and contacts

Technical Indicators

Technical indicators are those that require direct application of IT systems and tools to detect. These indicators involve network and host activity, such as activities on a computer, terminal, or landline/mobile device, and incidents occurring within the core IT infrastructure of an organization. One of the most frequently used applications for the detection of insider threat indicators is UAM, a capability used by analysts to observe human behavior in the IT realm.

Most insider threat incidents require little technical sophistication to execute. Research in the banking and finance sector indicated that most attacks were neither complex nor required much technological skill and were committed by individuals who did not work in IT and did not have extensive backgrounds in technology. Instead, these individuals exploited vulnerabilities in systems and processes to commit theft.

These examples are intended to present a generic structure of potential insider threat indicators. The examples listed below are not a definitive list. Instead, they provide a generic structure of potential insider threat indicators and a starting point for organizations to identify threat indicators appropriate for its specific, unique characteristics and concerns.

[62]Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., Osula, A., (n.d.). Insider Threat Detection Study. (pp 30-31). NATO Cooperative Cyber Defense Center of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Technical Indicator Examples[63]

- Direct correspondence with competitors
- Email messages with abnormally large attachments or amounts of data
- Domain Name System (DNS) queries associated with Dark Web activities
- Use of activity masking tools (e.g., virtual private networks [VPN] or the Onion Router [Tor])
- Executing offensive tools
- Executing malware
- Connecting an unauthorized device to the network
- Downloading or installing prohibited software
- Unexpected activity outside of normal working hours
- Attempts to bypass or disable malware protection tools or security controls
- Unauthorized attempts to escalate permissions or privileges, especially without a need to know
- Attempting to print or copy protected or restricted documents
- Abnormally large number of software or operating system errors
- Attaching an unidentified device to a workstation (USB, external hard drive)
- Maintaining access to sensitive data after termination notice
- Different users attempting to log in from the same workstation or device
- Lack of log messages or monitoring data
- Unauthorized modification of centrally stored files
- Copying large numbers of documents to a local drive
- Authentication failures or failed login attempts
- Unauthorized configuration file changes or permission changes
- Unauthorized database content changes
- Irresponsible social media habits
- Insider attempts to access resources not associated with that insider's normal role
- User account used from multiple devices
- Multiple accounts identified for a single user
- Triggering of key words or phrases in emails, text messages, or phone calls

The Software Engineering Institute (SEI) at Carnegie Mellon University provides additional evidence to support the concept of human and technical monitoring. From their extensive research into the insider threat, SEI developed the 10 most frequently observed potential cyber indicators of an insider threat:[64]

- Lack of controls to prevent unauthorized modification of critical data
- "Disgruntled" employee
- Use of excessive access privilege
- Compromised passwords
- Email/chat with external competitors/ conspirators
- Failure to protect critical files
- Violation of need-to-know policy
- Unauthorized data download to/from home
- Unauthorized data exports
- Ability of users with system administrator privileges to sabotage systems or data

[63]Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., Osula, A., (n.d.). Insider Threat Detection Study. (pp 30-31). NATO Cooperative Cyber Defense Center of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf
[64]Costa, D. L., Albrethsen, M. J., Collins, M. L., Perl, S. J., Silowash, G. J., & et al. (2016). An Insider Threat Indicator Ontology | CMU/SEI-2016-TR-007 | (p. 70). Software Engineering Institute | Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_454627.pdf

Employees or organizational members tend to pose a higher risk of insider threat when they have been terminated or expelled or have secured a new position. In these instances, insiders tend to steal information with which they work or encounter most regularly. Some feel they are entitled to this information and that it belongs to them, rather than to the organization. In these cases that involve information and data with which an insider has frequent contact, the warning signs for theft may not be as noticeable.

Some employees may be recruited by competing corporations or nation states and may collude with fellow employees who also feel disenfranchised or aggrieved. This type of engagement may make the theft or sabotage harder to detect, particularly if the collaboration occurs with users who are supervisors or who have administrator rights in the systems containing the information.

Furthermore, insiders who are leaders, supervisors, or administrators can enable and even conceal insider threat indicators by altering the information that tracks and logs user movements, meaning it may take even longer to identify the perpetrator of theft or sabotage.

Organizational/Environmental Indicators

There is a broad perception that insider threats are primarily, or even entirely, driven by individual predispositions, stressors, and choices. What is frequently missed is the relationship between individual behaviors and the environment that influences them.

The social context of insider threats means that environmental factors can escalate or mitigate stressors that can contribute to behavioral changes and an individual's progression from trusted insider to insider threat. Organizational policies and cultural practices can play a significant role in creating or managing an insider threat. For example, the organizational issues listed below can create additional motivation for an insider to become a threat to an organization. Of most concern are those issues that become part of the person of concern's justification to commit an insider act and those that prevent the organization from responding definitively to a threat. Inappropriate organizational responses can often provide the tipping point or "last straw" to motivate an insider threat to act.

Organizational Indicator Examples

- High stress environment
- Lack of candor or transparency
- Tolerance of poor performance
- Toxic leadership
- Inconsistent enforcement of policy
- Inaction following notification of grievance, threat, or increased risk
- Overly aggressive reaction following notification of threat
- Inappropriate disciplinary action
- Bureaucratic compartmentalization of information
- Lack of understanding or awareness regarding insider threat risk
- Pattern of overwork
- Lack of appreciation for employees/members
- Heightened uncertainty–financial or contractual
- Recent merger/acquisition
- No risk assessment process
- Apparent indifference to complaints of harassment or discrimination
- Undertrained staff (particularly in cybersecurity)

Violence Indicators

The threat of an insider causing physical harm to facilities or networks, fellow organizational members or employees, or themselves is a common concern. Sabotage, workplace or organizational violence, domestic abuse, and terrorism are all examples of individuals using their access and knowledge of facilities or networks to intentionally harm people or destroy an entity's assets. Violence carries with it specific behaviors or collections of behaviors that can instill fear or generate a concern that a person might act; the list below contains some examples.

Violence Indicator Examples[65]

- Intimidation
- Stalking
- Emotional abuse
- Domestic violence
- Expressions of hatred or prejudice
- Harassment or bullying
- Excessive use of alcohol or drugs
- Unexplained absenteeism
- Change in behavior
- Statements indicating desperation or suicidal thoughts
- Resistance to change, persistent complaining about unfair treatment
- Decline in job performance
- Paranoia
- Violation of company policies
- Emotional responses to criticism, mood swings
- Threats of homicide/suicide

Domestic Abuse Indicator Examples

As part of an organization's or business' obligation to provide a safe environment, insider threat mitigation program's policies should consider a commitment to support domestic violence victims and take protective steps when such violence threatens to intrude on the workplace or organization. Examples of some common domestic abuse indicators include the following:

- Personality changes (e.g., low self-esteem in someone who was always confident)
- Constantly checking in with their partner
- Never having money on hand
- Overly worried about pleasing their partner
- Wearing clothes that do not fit the season (e.g., long sleeves in summer)
- Uncharacteristic absenteeism or lateness
- Poor concentration
- Increasing errors and inconsistent work quality
- Injuries such as bruises, black eyes, or broken bones with concealment or unconvincing explanations for occurrence
- Signs of emotional distress (e.g., unusual quietness or solitude)
- An unusual number of phone calls, text messages, or emails from a current or former partner
- Abrupt changes of address or reluctance to divulge where they are living or temporarily staying

[65]Adapted from Interagency Security Committee. (2019). Violence in the Federal Workplace: A Guide for Prevention and Response. (pp. 28-29). Retrieved from cisa.gov/publication/isc-violence-federal-workplace-guide

Terrorism/Bias Incident/Hate Crime Indicator Examples

Terrorism, as an insider threat, is the unlawful use of force and/or violence by a trusted insider against their organization or workplace in furtherance of a political, religious, or social objective. A bias incident, as an insider threat, is any hostile conduct by a trusted insider against an associate or their organization motivated by racism, religious intolerance, gender discrimination, or other prejudice; while a hate crime is the evolution of a bias incident to the point of breaking a state or federal law. An important distinction to make is that all hate crimes are bias incidents but not all bias incidents are hate crimes. Examples of some common terrorism, bias incident, and hate crime indicators include the following:

- Expressing bias or hatred toward a race, religion, disability, sexual orientation, gender, or identity
- Browsing extremist websites
- Expressing hatred or intolerance of U.S. society or culture
- Advocating violence for a political, religious, or ideological cause
- Monitoring or recording security equipment, movement, or responses
- Engaging in deception or concealment

Concluding Thoughts

As described throughout this chapter, there are a range of observable behaviors that can serve as warning signs for a person of concern who is on a pathway to an insider incident. To successfully apply the Insider Threat Mitigation framework, organizations should establish the capability to detect and identify these concerning, observable behaviors.

It is imperative that organizations educate their employees on how an individual may progress on the pathway to a malicious act and on the behaviors that malicious insiders may exhibit as they move from an idea to action. Organizations should establish a culture of reporting and train their members on how to report their concerns or observations. The combination of human observation and reporting and technology-based insider activity monitoring may enable an organization to detect and identify possible malicious or hostile incidents, setting the stage for successful insider threat mitigation.

Case Study

Recognizing the Warning Signs

A range of observable behaviors can serve as warning signs for someone who is on a pathway to an insider incident. Also known as indicators, these observable behaviors can include personal predispositions, such as a pattern of rule breaking, an inability to assume responsibility for one's own actions, or holding grudges, among others. The addition of personal, professional, financial, organizational, or community stressors increases the likelihood of a malicious insider act. Typically, no one stressor is the driver for a decision to breach the organization's trust. Unfortunately, sometimes, an insider will breach trust in a very hostile manner. Such was the case at Fort Hood, Texas in 2014.

WHAT HAPPENED

On April 2, 2014, an Army Specialist opened fire in an administrative office, targeting soldiers in his unit and then randomly shooting at soldiers in a populated area with no apparent pattern or method to his selection of victims. When confronted by military police, the assailant shot himself. Three soldiers lost their lives in the incident, and 14 others were wounded.

INDICATORS

A subsequent investigation revealed several personal predispositions. The Specialist had been dealing with depression and post-traumatic stress disorder and undergoing psychiatric treatment. Additionally, the assailant had a reported history of deception, including an unsubstantiated claim related to an alleged hostile event during a deployment and a secret Facebook account through which he communicated under a pseudonym.

Stressors leading up to the incident are believed to have begun in 2013 when the Specialist was removed from a leadership position and replaced with a more junior coworker. Three months prior to the shooting, both the assailant's mother and grandfather died, and he experienced problems in obtaining leave approval to attend his mother's funeral. One month prior to the incident, the Army transferred him to Fort Hood, and, again, he was frustrated with the military leave support for his family's move. In addition, the assailant was in debt by approximately $14,000.

On the day of the shooting, the Specialist decided to go home, retrieve his personal weapon, and return to Fort Hood to commit his act of violence, targeting first those with whom he had argued over the processing of his leave form.

LESSONS LEARNED

The U.S. Army's investigation highlighted gaps in information sharing, and the Specialist's supervisors mistakenly believed they were unable to obtain his personal health information due to federal medical privacy laws.

Key Points

- A successful program will recognize that the **insider threat evolves over time and exhibits multiple overlapping detectable and observable behaviors**.
- **Behavior is what matters most**, not the motivation, whether it is political, religious, ideological, financial gain, or revenge.
- **Confirmation of any threat indicator requires a solid understanding of context**; recognizing that people often display behaviors representative of an individual point in their life that may not result in a direct expression of a threat.
- **Exhibiting no indicators does not guarantee that a person will not pose an insider threat**.
- **Professional stressors have the additional effect of creating potential grievances** against an employer, organization, or agency.
- **Behavioral indicators reflect patterns of activity over time**, based on the way the insider interacts within the organization. These indicators are directly observable by peers, HR personnel, supervisors, managers, and technological systems.
- **Technical indicators are those that require direct application of IT systems and tools to detect**. UAM is the most frequently used application for the detection of technical insider threat indicators.
- **Violence carries with it specific behaviors or collections of behaviors** that instill fear or generate a concern that a person might act out violently.
- **People are key sensors for the detection and identification of an insider threat**. People may have an awareness of the predispositions, stressors, and behaviors of insiders who may be considering taking violent actions toward an organization.
- **Those who perpetrate violence or steal data or secrets often leak their plans or grievances**. It is well established that a person of concern will tell others of their intent or plan at a much greater rate than they will tell the target of their plan.
- As part of an organization's or business' obligation to provide a safe environment, the **insider threat policies and programs should always consider a commitment to support domestic violence victims** and to take protective steps when such violence threatens to intrude on the workplace or organization.

5 Assessing Insider Threats

Threat assessment is a complex discipline that requires an investment in training and preparation to develop proficiency. Because there is no demographic profile of an insider threat, objective assessment of threat enhancing and mitigating circumstances as well as a contextual assessment of the behaviors exhibited by a person of concern are essential to understanding the threat presented. Organizations with a fully developed threat assessment process provide a means to intervene to prevent an incident or to mitigate its impacts if it cannot be prevented.

Threat assessment is the process of compiling and analyzing information about a person of concern who may have the interest, motive, intention, and capability of causing harm to an organization or persons. A primary purpose of an assessment process is to inform decision-making regarding how to manage a person of concern, with the goal to prevent an insider incident in any of its expressions.

This chapter provides guidelines and best practices for conducting insider threat assessments that can inform the selection and application of insider threat mitigations. These guidelines and best practices cover the following areas:

- The threat **assessment process**
- Knowing and recognizing the indicators for **violence in threat assessment**
- **No useful profile in threat assessment** exists
- The difference between **making a threat vs. posing a threat**
- Understanding the common occurrence of **leakage in targeted violence** and how it can aid in the assessment process
- Addressing an insider's **awareness of scrutiny**
- Understanding when **use of a behavioral scientist** is beneficial to the assessment process as well as **case considerations indicating when the involvement of law enforcement is advisable**

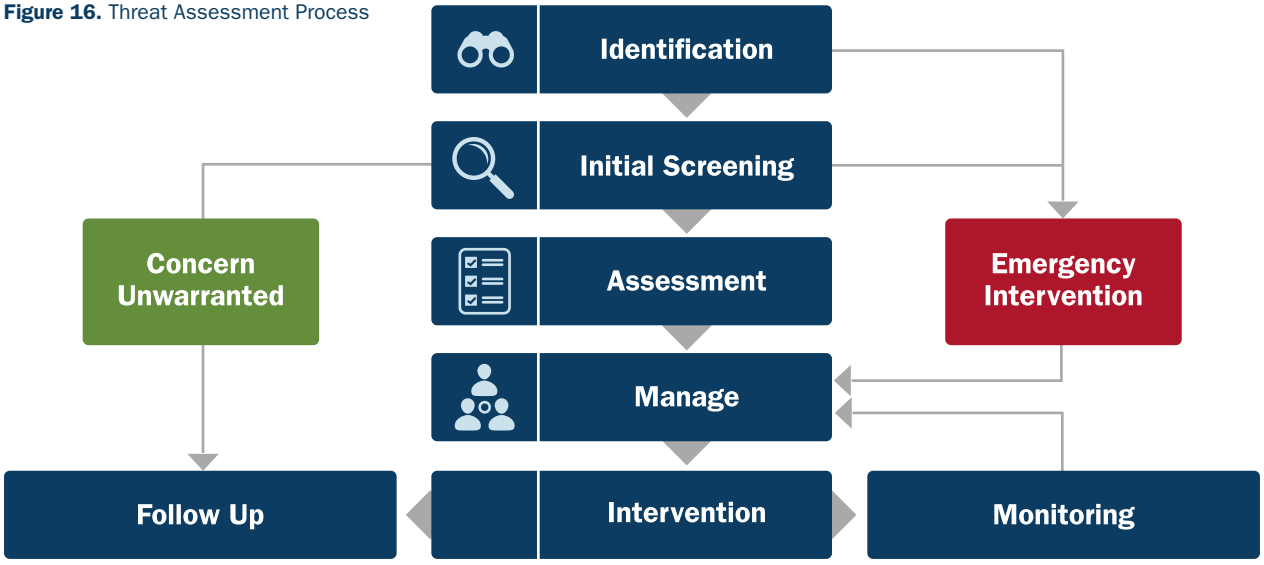
Assessment Process

The threat assessment process consists of a pre-established set of operational activities employed by a threat management team that combines an investigative process and information-gathering strategies. This process applies in both urgent/emergency situations and in non-urgent/non-emergency situations, with the former potentially requiring emergency intervention to protect life, safety, or property. In both circumstances, the approach asks those conducting the investigation to answer several key questions:

- Is there **evidence** to suggest the person of concern poses a threat?
- What **type of threat** does the person of concern pose?
- Is the person of concern **moving toward committing a malicious act**?

Any concerning communication, behavior, or report should be brought to the attention of the threat management team for evaluation consistent with the process described below.

Figure 16. Threat Assessment Process



Initial Screening

When a concerning communication, behavior, or report is brought to the attention of the threat management team, the team should activate and conduct an initial screening to determine the validity of the concern.

The goal of a preliminary screening is to ascertain in a gross or general manner the urgency presented by the situation or behavior in question. The threat management team should consider all information gathered with the intent to determine if the concern is unwarranted, if an assessment is necessary, or if emergency intervention is required (see figure 16). There are no universal criteria for determining which path to follow. The decision should be based upon the facts presented in the reporting and investigative process, as well as the culture and tolerance for risk in an organization.

Concern Unwarranted

If, based on an initial screening, the threat management team determines that a concern is unwarranted, then the incident may be addressed within routine HR, disciplinary, or employee relations protocols. The key is to remain proactive, while documenting the incident response and, as needed, following up by engaging both the individual or individuals who raised the initial concern(s) and the identified person of concern.

Assessment

Alternatively, if the threat management team determines that the person of concern potentially poses a threat and may have the interest, motive, intention, and capability of causing harm to an organization or persons, but the reported situation does not appear to present an immediate threat, then the threat management team should initiate a deeper investigation. The investigation will inform the assessment, which is a deliberate process of gathering information and re-evaluating risk based on information as it is developed. The quality of an assessment is directly related to both the relevance and depth of the investigation.

When an initial risk screening indicates that a concern for violence is not urgent, the threat management team should also begin early incident management steps, including:[66]

1. Continuing or expanding its information collection
2. Consulting with an internal or external threat assessment professional; an external professional is advisable when the team is uncertain about its ability to accurately assess risk, even in a general or gross fashion
3. Consulting with legal counsel
4. Assessing the need for additional security
5. Initiating, when necessary, coordination with local law enforcement
6. Conferring as a team to determine the next steps

Emergency Intervention

If the threat management team determines that emergency intervention is required based on the initial screening, then the threat management team should take immediate action, whether it is a call for assistance from first responders or law enforcement, or activation of an organization's Incident Response Plan.

In the event of physical violence or sabotage, the threat management team should initiate the organization's Incident Response Plan, skip the initial screening, contact the appropriate authorities, and begin the investigation immediately. For cases of targeted violence or sabotage, an emergency intervention can sometimes result in the need to evacuate a location or facility, initiate a lockdown, or shelter in place. The threat management team should have plans in place for each response and coordinate across the organization for immediate action.

[66]American Society for Industrial Security. (2020, May 7). Standard: Workplace Violence and Active Assailant-Prevention, Intervention, and Response. (p. 23). ASIS WVPI AA-2020. ASIS International, ISBN 978-1-951997-03-8

Assessment Process

After the threat management team has determined that an assessment is necessary, the threat management team begins a deep investigation into the person of concern, which involves gathering evidence, analyzing information, generating a report outlining findings, and making clear, actionable recommendations.

Gather the Evidence

The investigation begins with the threat management team seeking and collecting information and evidence to corroborate any alleged statements, behaviors (both physical and technological), or actions of the person of concern. A successful investigation of a person of concern and any insider incidents or potential incidents requires the collection and analysis of available information gathered from all potential sources, including the person of concern, coworkers or associates, family or neighbors, and IT-related or online material.

- **During organizational planning, the threat management team should give careful consideration to several factors in the inquiry and assessment process**, including whether the incident intake will be accomplished by internal trained staff or outside law enforcement, the need for immediate safety and/or security to protect people and property, ensuring criminal prosecutions are not compromised, and handling hostility in the investigative process.[67]

- **The team should collect evidence from different departments in the organization**, which can include employment, membership, security or HR records; cybersecurity or physical security logs; video surveillance footage, and any reported concerns or behaviors from coworkers, associates, friends, or the threat management team. This type of information is instrumental in identifying an insider threat or corroborating a reported threat.

- **A mature insider threat mitigation program should have a centralized hub for the collection, integration, review, analysis, assessment, reporting, and storage of information**. The hub serves as a single, catalogued, searchable repository for easy and quick access to up-to-date, pertinent information.

- **In addition to collecting evidence, a thorough assessment should include an interview with the person of concern and/or any witnesses to their behaviors, history, or stressors**. It is essential that the key facts of an assessment be corroborated, with appropriate skepticism about the credibility, accuracy, and veracity of witnesses. Corroborated, information is more useful to a threat assessment than subjective information or opinions because it provides greater confirmation about the individual's behavior and facilitates the assessment of their interest, motive, and capacity to carry out an act of targeted violence or an insider incident.

- **The threat management team should decide whether to conduct "subject" interviews within the context of an overall behavioral risk/threat assessment strategy and the case facts**. Whether to interview the person of concern is a key question that depends on the need for information, the facts leading to the initiation of the process, the threat management team's standing in relation to the subject, the resources available to the threat management team, and the threat management team's training and experience.[68]

[67]Interagency Security Committee. (2019). Violence in the Federal Workplace: A Guide for Prevention and Response. (pp. 41-53). Retrieved from cisa.gov/publication/isc-violence-federal-workplace-guide
[68]Interagency Security Committee. (2019). Violence in the Federal Workplace: A Guide for Prevention and Response. (p. 52). Retrieved from cisa.gov/publication/isc-violence-federal-workplace-guide

Threat management team members should consider asking the following questions to both the person of concern and corroborating sources (family members, coworkers, associates, neighbors, friends, and mental health professionals). The answers to these questions will guide the assessment and should provide or corroborate evidence as to whether the person of concern is progressing toward a malicious act.

Sample Questions to Ask in a Threat Assessment[69]

- Why, at this particular time, has the person of concern made comments or actions that have been perceived by others as threatening?
- What is happening in the personal life of the person of concern that might be relevant?
- What has been said to others (e.g., friends, colleagues, coworkers, etc.) regarding the matter that is troubling them?
- How does the person of concern view themselves in relation to everyone else?
- Does the person of concern feel they have been wronged in some way?
- Does the person of concern accept responsibility for their own actions?
- How does the person of concern cope with disappointment, loss, or failure?
- Does the person of concern blame others for their failures?
- How does the person of concern interact with coworkers or associates?
- Does the person of concern feel they are being treated fairly by the company or organization?
- Does the person of concern have problems with supervisors, management, or leadership?
- Does the person of concern care about job practices and responsibilities?
- Has the person of concern received unfavorable performance reviews or been reprimanded?
- Is the person of concern experiencing personal problems, such as divorce, death in the family, health problems, or other personal losses or issues?
- Is the person of concern experiencing financial problems, high personal debt, or bankruptcy?
- Is there evidence of substance abuse, mental illness, or depression?
- Has the person of concern spoken of homicide or suicide?
- Does the person of concern have a past criminal history?
- Does the person of concern have a planned course of action, and, if so, does the plan make sense, is it reasonable, and is it specific?
- Does the person of concern have the means, knowledge, and ability to carry out their plan?

Try to keep the questions specific, clear, significant, answerable, and relevant. The answers to some questions may be subjective, and, therefore, will vary depending on who is answering them.

[69]Adapted from Federal Bureau of Investigation's National Center for the Analysis of Violent Crime & Critical Incident Response Group. (n.d.). Workplace Violence: Issues in Response. Department of Justice. Quantico, Virginia. Retrieved from https://www.hsdl.org/?view&did=444583

Determine a Person of Concern's Baseline Behavior

A change in behavior for a person of concern from their typical baseline is an important consideration in assessment. An individual's baseline behaviors reflect patterns of normal or benign activity reflected in the way the insider interacts within the organization and on its network. The National Behavioral Intervention Team Association (NaBITA) strongly recommends that the threat management team or those retained as assessors develop a baseline of the person of concern's behaviors, and then collect information from multiple reliable sources to detect and identify changes in that behavior.[70]

To allow comparisons to baseline behavior, the assessor should:[72]

- **Write detailed descriptions** of the initial behavior(s) and concern(s) that supported the determination that the person of concern was a threat.
- **Monitor the trajectory of the person of concern's behavior** by using a pre-determined risk rubric to understand if their presentation is resolving, escalating, or decompensating.[71]
- **Remain alert** during a long-term assessment and during post-intervention **for any new information or behaviors that might require additional action**, either with respect to the specific situation at issue or the organization in general.
- **Implement and coordinate measures to assess and manage any risk of violence**, with the consideration of the choice of measures being dependent on the level of perceived risk.

Analyze

Once the threat management team has collected enough evidence to cover the full scope of an assessment, the team should begin to analyze the information to determine if the person of concern is progressing toward a malicious act. If the threat management team makes a positive determination, they should also make a judgment about how quickly events are progressing. Example analytical questions include:[73]

- What is the exact nature and context of the threat and/or behavior?
- Who or what is the intended target?
- Was the threat and/or behavior intentional or unintentional?
- What was the possible motivation for the threat and/or behavior?
- Has an organizational policy or regulation been violated?
- Does the person of concern have the intent, motivation, and ability to carry out the threat?
- Has a law been broken?
- What is the person of concern's history?
- What are the behavioral and technological indicators?
- Does the person of concern have any stressors/personal predispositions?

[70]Adapted from National Behavioral Intervention Team Association. (2019). The NaBITA Risk Rubric; The NaBITA 2019 Whitepaper. Retrieved from https://cdn.nabita.org/website-media/nabita.org/wp-content/uploads/2019/04/17142743/NaBITA-2019-Whitepaper-Final1.pdf
[71]Decompensating is to lose the ability to maintain normal or appropriate psychological defenses, sometimes resulting in depression, anxiety, or delusions.
[72]Adapted from Fein, R.A., & Vossekuil, B. (2000, January). Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials. NCJ 179981. National Institute of Justice. (pp. 57-58). U.S. Department of Justice. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/179981.pdf
[73]Adapted from Federal Bureau of Investigation's National Center for the Analysis of Violent Crime & Critical Incident Response Group (n.d.). Workplace Violence: Issues in Response. (pp. 25-26). Department of Justice. Quantico, Virginia. Retrieved from https://www.hsdl.org/?view&did=444583

As noted in Chapter 3, there are a variety of evaluation frameworks or models, risk rubrics, and data analytic tools that, once customized to an organization's threat criteria and risk tolerance, are used in threat assessment, depending on the threat expression in question (violence, cyber-attacks, theft of intellectual property, etc.). Threat management teams should use a risk rubric to initially assess and then re-assess a person of concern's specific level of risk to determine if the individual is progressing toward a malicious act and, if so, at what rate.

To objectively assess risk, threat management teams should apply their standardized tool to every case—regardless of how serious or how trivial the case may seem—and consistently apply a rating system to indicate whether an individual poses a low/medium/or high risk of violence, theft, sabotage, etc. Assessing the level of risk in this manner will enable the organization to identify its safety concerns and then select the appropriate intervention measures needed to address concerns.[74] A recommended best practice is to document the risk level each time a case is discussed, with the level potentially shifting over time as interventions are implemented or as the situation evolves.

Report and Recommend

After completion of evidence collection, analysis, and determination of whether a person of concern poses a threat, the threat management team should generate a formal report outlining its findings. This report should include clear, actionable recommendations to manage the threat and prevent an insider incident. This is the final step in the threat assessment process and the first step in managing the threat.

A good threat assessment report will include multiple documents with personal private information, some of which may have specific storage, maintenance, and viewing rules or laws. Accordingly, the assessment team should coordinate with legal counsel for the proper control and handling of the report.

At a minimum, the threat assessment report should include:

- The person of concern's historical documents (e.g., HR report, background check, health records, previous assessments)
- A list of warning signs; indicators/ stressors/triggers
- Open source search results (e.g., social media, blogs, internet search)
- Reports from concerned coworkers, associates, family, friends, etc.
- Interview reports
- Threat management team findings, including risk level
- Recommendations for management strategies

Management strategies can be a single intervention or a series of interventions focusing on the person of concern, potential targets, the situation, and/or the environment. Management strategies can include administrative actions, such as probation or expulsion; criminal enforcement, if it is determined that a law was broken; increased security to protect the organization; or target relocation, if the person of concern is tending toward a violent act. Chapter 6 contains additional management strategies.

[74]National Behavioral Intervention Team Association. (2019). The NaBITA Risk Rubric; The NaBITA 2019 Whitepaper. (p. 4). Retrieved from https://cdn.nabita.org/website-media/nabita.org/wp-content/uploads/2019/04/17142743/NaBITA-2019-Whitepaper-Final1.pdf

Violence in Threat Assessment

Violence is recognized as a specific category of insider threat and includes homicides, terrorism, domestic violence, sabotage, and any other type of physical assault. The threat management team should know and recognize the indicators for violence.

Workplace/Organizational Violence

The Interagency Security Committee categorizes workplace or organizational violence into four types:[75]

Criminal Intent: The person of concern has no legitimate relationship to the workplace or organization or its employees/members, and is committing a separate crime, along with the violence.

Customer or Client: The person of concern has a legitimate relationship with the workplace or organization and becomes violent while being serviced by an employee or member.

Employee, Member, or Contractor on Employee, Member, or Contractor: The person of concern is a current or former employee, contractor, or organizational member who threatens or attacks another current or former employee, member, or contractor in the workplace or organizational site.

Personal Relationship: The person of concern does not have a relationship with the agency or organization but has a personal relationship with an employee or associate, including domestic violence that affects the workplace or organizational site.

During a comprehensive threat assessment, a threat management team should take each category into consideration when deciding who to interview or from whom or where to collect evidence.

[75]Adapted from Interagency Security Committee. (2019). Violence in the Federal Workplace: A Guide for Prevention and Response. (pp. 9-10). Retrieved from cisa.gov/publication/isc-violence-federal-workplace-guide

Domestic Violence

Domestic violence does not always occur in the home. It often spills over into other environments in the victim's life (e.g., the workplace, associations, religious facilities, daycares, or retail shops). According to the Centers for Disease Control and Prevention, victims of intimate partner violence lose a total of 8 million days of paid work each year.[76] The cost of intimate partner violence exceeds $8.3 billion per year, and between 21-60 percent of domestic violence victims lose their jobs due to reasons stemming from abuse.[77]

A threat management team should be aware that domestic violence typically escalates in frequency and intensity over time. The perpetrator may first begin to harass a victim at a work or organizational site by telephone or email, then threaten to come to the workplace or organizational facility, and finally, appear and threaten or attack the victim.

Reports or threats of domestic violence must be taken seriously and assessed on the facts rather than assumptions or pre-conceived notions of how a victim looks or behaves.

Terrorism/Bias Incident/Hate Crimes

Terrorists do not always infiltrate an organization; sometimes they are already an established, trusted insider. Terrorists as insiders can use their familiarity with an organization's structure, security, building layout, and other knowledge to maximize casualties or sabotage facilities or systems for a political, ideological, or social agenda. A threat management team should learn the threat indicators and stay informed about the terrorism exposure in its region, state, city, and/or organizational site.

Bias incidents and hate crimes are widespread and typically result in assault, murder, arson, or vandalism. According to the FBI, out of the 8,437 hate crime offenses committed in 2017, 78 percent were directed at individuals, 6 percent were against businesses or financial institutions, nearly 4 percent were against government entities, 3 percent were against society/public, 2 percent were against religious organizations, and the remaining 7 percent were directed at other, unknown, or multiple victim types.[78]

Threat management teams should be well informed of the indicators of terrorism and hate crimes in order to properly assess and mitigate a violent or potentially violent insider. It is important to be aware of the risks and indicators but also to remember that threat assessment is based on behaviors, not profiles. Threat management teams should be careful of prejudices and avoid profiling in the assessment of terrorism.

[76]National Center for Injury Prevention and Control. (2003, March). Costs of Intimate Partner Violence Against Women in the United States. | Centers for Disease Control and Prevention | Atlanta, GA. Retrieved from https://www.cdc.gov/violenceprevention/pdf/ipvbook-a.pdf

[77]Rothman, E.F., Hathaway, J., Stidsen, A., de Vries, H.F. (2007, April). How employment helps female victims of intimate partner violence: a qualitative study. Journal of Occupational Health Psychology 12(2):136-43. DOI: 10.1037/1076-8998.12.2.136. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/17469996

[78]Uniform Crime Reporting Program. (2017). Hate Crime Statistics: By victim type. U.S. Department of Justice | FBI. Retrieved from https://ucr.fbi.gov/hate-crime/2017/topic-pages/incidents-and-offenses

Sample Questions to Ask in a Threat Assessment for Violence

In addition to the suggested questions to ask during a threat assessment, a threat management team should consider asking these questions to both the person of concern and corroborating sources (family members, coworkers, associates, neighbors, friends, and mental health professionals) when the threat is one of violence:[79]

- What motivated the person of concern to make the statement or take the action that caused them to come to attention?
- What, if anything, has the person of concern communicated to someone else—target, law enforcement, family, friends, colleagues, associates—or written in a social media, diary or journal concerning their intentions?
- Has the person of concern shown an inappropriate interest in any of the following?
  - Weapons (including recent acquisition of a weapon)
  - Violent or extremist ideas/groups
  - Murders, murderers, mass murderers, workplace violence, or stalking incidents
- Is there evidence that the person of concern has engaged in menacing, harassing, and/or stalking-type behaviors?
- Has the person of concern engaged in attack-related behaviors? Questioning on attack-related behaviors should include any inappropriate interest in any of the following:
  - Developing an attack idea or plan
  - Approaching, visiting, and/or following a target
  - Approaching, visiting, and/or following a target with a weapon
  - Attempting to circumvent security
  - Assaulting or attempting to assault a target
- Does the person of concern have a history of mental illness involving command hallucinations, delusional ideas, feelings of persecution, etc., with indications that the person of concern has acted on those beliefs?
- How organized is the person of concern?
- Can the person of concern plan and execute a violent action against a target?
- Is there evidence that the person of concern is experiencing desperation and/or despair? Has the person of concern experienced a recent personal loss and/or loss of status? Is the person of concern now, or has the person of concern ever been, suicidal?
- Is the person of concern's story consistent with their actions?
- Are those who know the person of concern worried that they might act based on inappropriate ideas?
- What factors in the person of concern's life and/or environment might increase or decrease the likelihood that they will attempt to attack a target (or targets)?

[79]Fein, R. A., & Vossekuil, B. (1998, July). "Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials" National Institute of Justice; Research in Action. NCJ 170612. (pp. 50-51). U.S. Department of Justice, Office of Justice Programs, Washington, DC. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/179981.pdf

Profiles – No Useful Profile in Threat Assessment

The term profiling has received much criticism from the general public and leadership at all levels in government due to concerns that law-abiding citizens have been pulled over in traffic stops, detained, and questioned merely because they fit a descriptive demographic profile such as race or ethnicity.

Profiling, as originally developed by the FBI Behavioral Science Unit, involves using information gathered from a crime scene to generate a set of hypotheses about the characteristics—physical, demographic, personality, and others—of the person most likely to have committed the crime.[80]

For the purposes of threat assessment, there is no useful profile to identify and assess the potential risk of an individual committing an insider incident. Prospective profiling to identify an individual likely to commit an insider incident or an act of violence carries considerable risk of false positives. Even though a person may, at some point in their life, display one or more of the indicators for targeted violence and fit a so-called profile, that person is no more or less likely to engage in acts of targeted violence than someone who displays the same indicators and does not fit the so-called profile.[81]

Behaviors, informed by life circumstances, are what is relevant to a threat assessment, not a person's demographic details. Focusing on behaviors and communications will help a threat management team determine if someone appears to be planning or preparing for an act.

[80]Douglas, J.E., Ressler, R.K., Burgess, A.W., & Hartman, C.R. (1986). Criminal Profiling from Crime Scene Analysis. Behavioral Sciences & the Law, 4, 401– 421. Retrieved from https://doi.org/10.1002/bsl.2370040405
[81]Sewell, K.W., & Mendelsohn, M. (2000). Profiling potentially violent youth: Statistical and conceptual problems. Children's Services: Social Policy, Research, and Practice, 3(3), 147–169. DOI: 10.1207/S15326918CS0303_2

Making a Threat vs. Posing a Threat

The central question in threat assessment is whether an individual poses a threat, not whether the individual made a threat. Making a threat is a singular behavior or expression and is often one of the first ways in which an individual comes to the attention of an organization or a threat management team. Posing a threat is the result of an analysis of the behaviors and stressors exhibited by the person who made the threat, along with the circumstances and context in which the threat was made, and a determination that the person of concern does indeed have intent toward a malicious act.

It is widely understood that insider threat incidents are rarely sudden, impulsive acts. Individuals do not normally just snap and engage in impulsive or random malicious acts. Instead, insider threat incidents are usually the result of a discernible progression as described in Chapter 4 of this *Guide*. It is important to note that:[82]

- Not everyone who makes a threat will pose a threat.
- Some individuals who pose a threat will never make a threat.
- Some individuals who make a threat ultimately pose a threat.

Determining if an individual poses a threat will sometimes require monitoring a person of concern's communications, including their organizational emails or phone conversations and publicly accessible social media pages or weblog posts. Organizations should consult with legal counsel as part of the planning process and before taking these monitoring steps since speech and the gathering and viewing of public communications are protected by the First Amendment and privacy rights.

Nevertheless, organizations should respond to all persons who make threats. Whether an actual expression of intent to carry out an insider threat, a leakage of violent thought, or merely an inappropriate statement, organizations should promptly investigate. The person making the threat could perceive a lack of response as permission to proceed with carrying out the threat.

[82]Adapted from Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 15). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Leakage in Targeted Violence

According to the targeted violence research conducted by the FBI and USSS, direct threats to a target are rare, and leakage, intentional or unintentional threats communicated to a third party, are common. Direct threats are communications of an intent to do harm delivered directly to a potential victim in person (i.e., confrontation) or through text, email, telephone, social media, etc. Direct threats to the victim are infrequent because announcing a plan to attack directly to an intended target might result in an investigation, increased vigilance, and target hardening–all of which would be counterproductive to the would-be offender's intentions.

Sometimes, however, a person of concern will communicate or leak their threat, idea, or plan for a possible attack to a friend, acquaintance, or peer. Leakage can occur with coworkers, neighbors, family members, associates, and/or classmates as well as through email, social media, artwork, journal entries, or other means. Some persons self-identify—they call, write, email, or approach a public official or figure or indicate an unusual or inappropriate interest in an entity. Such a person may threaten for various reasons: to warn of a possible attack, to ask to be stopped, to demand help or attention, to express frustration or anger, or to communicate distress. Research of past instances of targeted violence has shown that oftentimes many individuals knew about an attacker's threats, ideas, and plans before an act of targeted violence was carried out. However, individuals only reported that information ahead of time in very few cases.[83]

As a result, it is important that threat assessment inquiries involve efforts to gather information from everyone who may have had contact with the person in question so that all relevant information may be discovered.

Awareness of Scrutiny

At some point in the investigative process, a person of concern may become aware of investigative scrutiny. A threat management team should expect behavioral changes once a person of concern becomes aware of a threat assessment.

Depending on the particulars of the threat or malicious incident, those behavioral changes may be expected and acceptable to the team. Awareness of scrutiny can serve as a mitigator when the person who yearns for attention or direction finds relief in being heard, or serve to mitigate any plans for malicious intent by making them more difficult to carry out undetected.

On the other hand, this awareness can cause the person of concern to engage in impression management (an attempt to influence the perceptions of others), outright deception, acceleration of their plan, or to completely go dark and conceal behaviors that would otherwise alarm observers. Additionally, the extra attention could also generate or amplify feelings of persecution or paranoia.

Remember, establishing a baseline of behavior prior to awareness of scrutiny is crucial for detecting behavioral changes that could signify a person of concern is beginning or continuing down a pathway to a malicious incident. As with any behavior, change means something, and noticing that change and interpreting its meaning is important.

[83]Silver, J., Simons, A., & Craun, S. (2018). A Study of the Pre-Attack Behaviors of Active Shooters in the United States Between 2000 – 2013. Federal Bureau of Investigation, U.S. Department of Justice, Washington, D.C. 20535. Retrieved from https://www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view

Use of a Behavioral Scientist

The use of a behavioral scientist in the assessment of potential insider threats is a best practice for insider threat teams, especially for larger organizations. These experts are best positioned to determine the possible contribution(s) of any psychological or personality disorder issues, previous violations, social network influences, and stressors on a person of concern. They are also prepared to help determine the relevance and importance of concerning behaviors and organizational activity (or lack of activity) in response to a potential threat. Because of their training, behavioral scientists are uniquely qualified to design mitigation strategies and determine their subsequent effectiveness. Additionally, they may be able to request and review treatment and diagnostic records to constructively inform a threat management team of a concerning person's violent or malicious insider threat potential.

Of note, organizations should consult legal counsel and, when applicable, a union representative before requesting a person of concern's medical or diagnostic records, when using a behavioral scientist, and when requesting that an individual undergo an evaluation. Federal, state, and local laws, and union regulations may limit or control the scope of medical information available to the organization as well as impose restrictions on how the documentation is used and stored.

In general, clinical assessments may involve the remote evaluation of a person of concern's HR records, communications, clinical records, and other reports of behavior. Or, these assessments may involve an interview and/or psychological testing of the person, followed by a risk evaluation. This process is often referred to as a guided clinical judgment, which is where a clinician verifies clinical observations against empirical risk tools, such as violence prediction or insider risk analytical frameworks.

Depending on their training and certifications, a behavioral scientist may be able to determine the personality characteristics of unknown insider threats based on their writings in cases of anonymous threats or leaks, help determine the best intervention and/or termination strategies based on a person of concern's emotional and psychological state, or determine if a person of concern needs further mental health assistance or confinement.

Finally, a person with a confirmed mental health diagnosis, history of a condition, or who is suspected to have a condition may fall under the purview of the Americans with Disabilities Act (ADA) or similar state and/or local laws. For this reason, organizations should consult with legal counsel to ensure ADA compliance.

Case Considerations for the Involvement of Law Enforcement

The role of law enforcement will depend on the type of threat and the situation presented, but most insider threat assessments will not reach the level of complexity or criminality associated with a criminal investigation.

If a situation arises in a facility that requires law enforcement involvement, such as an act of targeted violence, an organization should call 9-1-1 to summon police or other emergency personnel to the scene. In these cases, law enforcement officers will be responsible for

protecting lives and ensuring safety, investigating the incident, detaining and/or arresting any offender(s), gathering evidence for criminal prosecution, and protecting property.

For incidents where a law has been broken, or there is an imminent threat of violence, the threat management team should ensure its incident response and assessment actions do not interfere with the ability of law enforcement to investigate or inhibit future prosecution. It is imperative that the threat management team record the specific circumstances of evidence collection to ensure that any evidence associated with an incident is handled properly and adheres to proper chain-of-custody protocols.

Finally, the threat management team should consult legal counsel when requesting the assistance of law enforcement.

Concluding Thoughts

Threat assessment is a unique discipline requiring a team of individuals to assess a person of concern and determine the scope, intensity, and possible consequences associated with a potential threat. Threat assessment is based on behaviors, not profiles, and behaviors are variable in nature. The ultimate goal of a threat assessment is to prevent an insider incident, whether intentional or unintentional.

To achieve prevention, a threat management team must determine whether a person of concern poses a threat. It is important to note that individuals may not actually pose a threat just because they make a threat or behave in a concerning manner. A threat management team will need to analyze a person of concern's predispositions, behavior indicators, and stressors to determine whether they are on a path to action and, if so, how fast are they moving and whether intervention is possible. As such, the threat management team will need to be multi-disciplinary and trained in order to take a comprehensive approach to assessing the facts and data and developing intervention strategies.

While there is no one-size-fits-all approach to threat assessment, it should be holistic, respectful, and focused on helping the person of concern, recommending intervention strategies to prevent an insider incident, and mitigating the effects if a hostile act does occur.

Case Study

Failure to Conduct a Thorough Assessment

Failing to conduct a thorough assessment on persons whose behaviors raise concerns can have tragic consequences, especially when those concerns coincide with stressful situations. Empirical research has shown that acts of targeted violence are not impulsive acts.[84] Targeted acts are planned, and they usually are accompanied by observable behaviors, often influenced by life stressors that were not brought to the attention of the target or law enforcement prior to an attack. Stressful events can include illness, divorce, debt, unfulfilled expectations, and career changes, such as terminations.

WHAT HAPPENED

The February 2019 mass shooting in Aurora, Illinois, in which an employee killed five coworkers and injured six others is an example of missed warning signs and lack of an assessment process. During a disciplinary meeting in which he was fired, a 45-year-old male employee opened fire with a .40 caliber pistol, killing three people in the meeting (the company's HR manager, the plant manager, and a 21-year-old HR intern—a student at Northern Illinois University who was on his first day of work) as well as two warehouse workers in the plant. Police killed the shooter following an exchange of gunfire, with five responding officers wounded during the incident.

INDICATORS

The case background provides numerous risk indicators along the pathway to the insider threat incident, as well as signs of the potential for violence. In 1995, the shooter was convicted in Mississippi of a felony aggravated assault and served two-and-a-half years in prison. The Aurora Police Department reported he had six arrests, including arrests for domestic violence and violating a restraining order. He also had a 2017 arrest in Illinois for disorderly conduct and criminal damage to property. These violations show personal predispositions toward violence and rule breaking.

In this case, the perpetrator applied for and was issued an Illinois Firearm Owners Identification (FOID) card in 2014, which Illinois residents need to legally purchase or possess firearms or ammunition. Later that year, he bought a gun—believed to be the one used during the shooting—from a licensed gun dealer in Aurora using that FOID card. When he subsequently applied for a concealed carry license, his felony conviction was discovered. The Illinois State Police rejected his concealed carry application, canceled his FOID card, and sent him a written notice demanding he turn in the gun he had purchased. He did not do so.

THREAT ASSESSMENT CONSIDERATIONS

Notably, the perpetrator joked to coworkers prior to his termination that he would "shoot the place up" if he were fired, an ominous warning and a concerning behavior that should have been reported. This behavior is consistent with other similar events where perpetrators communicate to at least one person their attack plans. This type of reporting is important to threat assessments because of the frequency with which individuals reveal their plans to others.

[84]Holden, G. A., Vossekuil, B., Fein, R. A. (1995, July). "Threat Assessment: An Approach to Prevent Targeted Violence" National Institute of Justice; Research in Action. NCJ 155000. (pp. 1-7). U.S. Department of Justice, Office of Justice Programs: Washington, DC. Retrieved from https://www.hsdl.org/?abstract&did=1377

Key Points

- **Threat assessment is the process of compiling and analyzing information about a person of concern** who may have the interest, motive, intention, and capability of causing harm to an organization or persons.
- A **primary purpose of an assessment process is to inform decision-making regarding how to manage a person of concern**, with the goal to prevent an insider incident in any of its expressions and not necessarily to make an arrest or enforce policy with disciplinary measures.
- An **assessment process applies in both urgent/emergency situations and in non-urgent/non-emergency situations**, with the former potentially requiring emergency intervention to protect life, safety, or property.
- Once the threat management team has determined that an assessment is necessary, the **threat management team begins a deep investigation into the person of concern**, which involves gathering the evidence, analyzing the information, and generating a report outlining findings and making clear, actionable recommendations.
- The **ultimate question to answer in a threat assessment is whether a person of concern is on a path to action**, and, if so, to determine how fast they are moving and where intervention may be possible.
- In **investigative and assessment planning**, considerations include determining the use of trained internal staff or outside law enforcement for incident intake, the need for immediate safety and/or security to protect people and property, ensuring criminal prosecutions are not compromised, and handling hostility in the investigative process.
- A **successful investigation** of a person of concern and any insider incidents or potential incidents **requires the collection and analysis of available information gathered from all potential sources**, including the person of concern, coworkers or associates, family or neighbors, and IT-related or online material.
- For incidents where a law has been broken or there is an imminent threat of violence, the **threat management team must ensure that its actions in incident response and assessment do not interfere with the ability of law enforcement to investigate or inhibit future prosecution**.
- After evidence has been collected and analyzed and the threat management team has determined whether a person of concern poses a threat, the team **generates a report outlining its findings and making clear, actionable recommendations to manage the threat and prevent an insider incident**. The report is the final step in the threat assessment process and the first step in threat management.

6 Managing Insider Threats

Recognizing that a person of concern poses a threat and may be on a pathway to a malicious act is an important beginning. Assessing threats and determining a person of concern's movement toward action is an essential next step. **Proactively managing insider threats**—the third element of the insider threat mitigation framework—**can change or stop the trajectory or course of events from a harmful outcome to an effective mitigation**.

When enacting insider threat management strategies, it is vital organizations remain mindful of the connectivity between protecting the organization and caring for persons of concern. Best practices in the field take both into consideration simultaneously and demonstrate that focusing on one of these aspects at the expense of the other can have hazardous effects.

Organizations manage insider threats through interventions intended to reduce the risk posed by a person of concern, always keeping in mind that the prevention of an insider threat incident and protection of the organization and its people are the ultimate goals. Threat management teams should recommend taking active (and/or passive) steps to minimize risk for an attack, such as relocating a potential victim. Or the organization could opt to monitor the person of concern more closely for changes in mitigating factors that could increase the person of concern's risk, perhaps with assistance from family and/or others close to the individual. The threat management team may also achieve the organization's prevention and protection goals by improving a person of concern's well-being, such as by addressing any perceived grievance(s).

All threat management actions should be accomplished in a respectful manner, even the arrest or hospitalization of a person of concern, and with the potential consequences considered before any action is taken. Preserving dignity is an intervention strategy, and doing so can prevent or mitigate the development of new grievances and/or rationale for an act of violence, sabotage, or other form of harm.

This chapter will provide:

- **Characteristics of insider threat management strategies**
- An overview of **intervention strategies, guidelines for managing domestic violence and mental health**, and the **use of law enforcement in threat management**
- An understanding of how to proceed with **suspensions and terminations for persons of concern** as well as **monitoring and closing a case**

Characteristics of Insider Threat Management Strategies

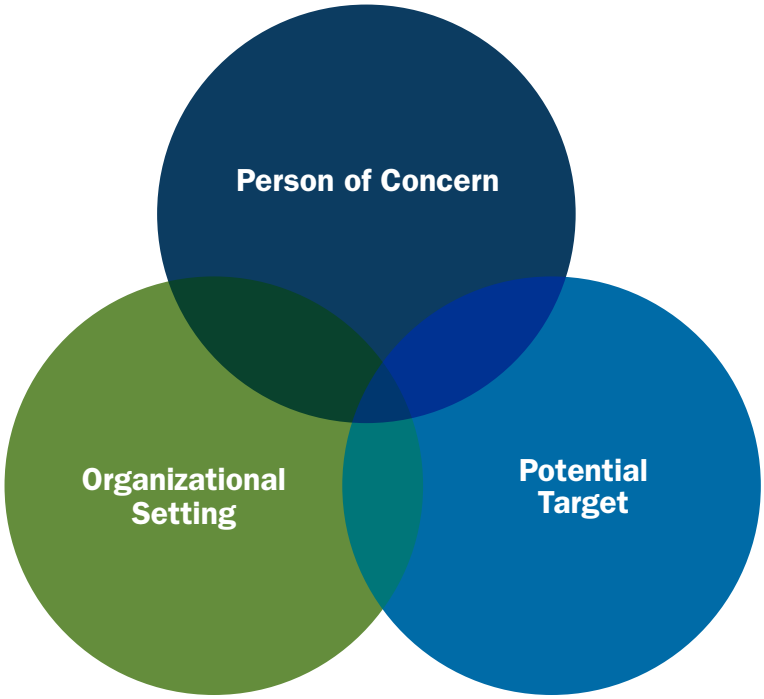
Threat management is the implementation of carefully planned, passive and/or active interventions focused on a person of concern who has been assessed as a risk or threat to an organization or target.

With the goals of prevention and protection, threat management teams should develop and recommend intervention strategies to prevent insider threat incidents and mitigate their effects if an incident occurs. As shown in figure 17, intervention strategies should incorporate actions directly involving the person of concern, any potential victims or targets, and the overall organizational environment and/or setting in which a threat could manifest.

When an assessment suggests that the person of concern has the interest, motive, and ability to attempt a disruptive or destructive act, the threat management team should recommend and coordinate approved measures to continuously monitor, manage, and mitigate the risk of harmful actions.

A vital consideration in managing the threat is understanding that, while standardization of processes from intake through assessment is a best practice, managing the threat will be tailored and unique in each instance.

Figure 17. Focus Areas for Managing the Insider Threat



Management strategies:

- **Are holistic**, considering the person of concern, potential victims or targets, and the organizational setting/or environment
- **Sometimes require multiple concurrent intervention strategies**
- **Require accurate and effective communication** with affected stakeholders
- Can be **short-term or long-term**
- Are **active**, directly engaging with a subject, **or passive**, such as monitoring a person of concern
- **Require continual reassessment**, adjustment, and follow-through
- **Allow each team member to offer a solution** based on their specific discipline and resources
- **May not work as planned**
- **Must be flexible**

Be mindful that the known or previously used intervention strategies may not provide the answer. Management strategies are only limited by the team's imagination and the law. Innovative thinking allows the threat management team to stay adaptable and provides the opportunity to mitigate risk, resolve grievances, or prevent a malicious act in ways not previously attempted.[85]

It is critically important to understand the personality and decision-making style of people when designing a management plan. For example, compromise and flexibility by management can embolden individuals with narcissistic or psychopathic personality features. People with these personality features are likely to see such approaches as weakness, or as encouraging entitlement thinking. Both of of these interpretations may encourage future violations. This can encourage future violations.

A best practice when developing intervention strategies is to avoid triggering a person of concern's breaking point by unintentionally validating their grievance or creating new ones. When designing and implementing intervention strategies, the organization should consider how their decisions, actions, and delivery could affect a person of concern's life, employment status, relationships, and dignity.

[85]Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 61). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Intervention Strategies

Considering the Person of Concern[86]

There are a range of intervention strategies that threat management teams should consider when recommending a course of action for a person of concern, to include:

Take no action—only advisable if the assessment revealed there is no imminent threat

Watch and wait—used when there is a possibility of a threat but not enough information to confirm the assessment

A return to work/duty risk assessment if necessary, performed by a behavioral scientist

Administrative actions, such as restrictions, suspension, discipline, expulsion, or termination

Legal actions, such as restraining orders or trespass warnings

Referrals for professional evaluation, such as mental health, substance abuse, or anger management

Arrest or a report of criminal activity to law enforcement

Third-party monitoring or intervention, such as by family, friends, religious organizations, social service organizations, or trusted adults

- Family, friends, and trusted adults are critical to managing a person of concern. In the majority of insider threat violent attack cases, there were no direct threats articulated to the target, but there was leakage to a third-party, and their behavior concerned others.
- Establishing and maintaining a trusted relationship to someone connected to the person of concern is a threat management best practice. Such a relationship can serve to reliably inform the threat management team of any escalation or de-escalation. Warning signs and concerning communications are often missed because of no clear, established relationship with a trusted source.

Set specific boundaries and limits to get the person of concern "in check." This approach is an especially important consideration when the organization plans to allow the person of concern continued access.

- Tailor to specific situations or behavior and monitor closely to ensure the circumstances do not reoccur.
- Ensure enforcement of standards of behavior in workplace.
- Ensure concerns are reported to the threat management team for assessment.

Address the grievance. This intervention strategy can potentially alter a person of concern's trajectory toward violence or another malicious insider incident. A study by the CERT Division of the Software Engineering Institute at Carnegie Mellon University in conjunction with the USSS National Threat Assessment Center found that in 23 insider incidents of computer system sabotage, 85 percent of the insiders held a grievance prior to the incident, and in 92 percent of these cases, the insider's grievance was work-related (including grievances against current and/or former employers, supervisors, and coworkers).[87] Addressing the grievance may not always be easy—particularly in the case of persons resistant to compromise—or palatable to stakeholders, in the case of toxic or destructive individuals. Many options are available, to include:

- Allow them to be heard
- Waive fees or debt
- Extend deadlines
- Find a way to preserve their dignity
- Allow a transfer, career change, or work from home
- Reduce stress or tension

[86]Adapted from Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (pp. 54-62). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

[87]Keeney, M., Kowalski, E., United States Secret Service's National Threat Assessment Center, Cappelli, D., Moore, A. (2005, May). "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors." (p. 14). Software Engineering Institute Carnegie Mellon. Retrieved from https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf

Considering the Victim or Target[88]

Victims and/or potential targets may also require management intervention, especially if the person of concern is allowed to maintain access to a work or organization site. In these cases, the organization should set up a support system for the protection of the victim or potential target. Organizations should also encourage potential or actual victims or targets to fully cooperate with investigations, interventions, and law enforcement, as necessary. Intervention strategies include:

- Increase vigilance
- Be alert to virtual stalking or research on public and private networks
- Change work or participation hours
- Relocate workspace
- Manage social media privacy
- Vary routes, routines, and activities
- Employ parking lot escorts
- Cease communication with the person of concern, if necessary
- Conduct personal safety planning

Considering the Organizational Setting and/or Environment[89]

Increased vigilance and target hardening are advisable when the concern for violence increases. This approach is important when a threat management team assesses that options directly related to the person of concern are limited. Examples include:

- Increased awareness of the local environment, work, or organizational site
- Notifications and warnings/information sharing
- Identity and entry verification
- Training on security procedures
- Law enforcement alerts/Be-on-the-Lookouts (BOLOs)
- Security process reviews
- Reduction of access points
- Increased visible security measures
- Flagging addresses in the 9-1-1 system

Organizational culture is another key factor in insider threat management. An environment that allows bullying, harassing, or menacing behavior is not conducive to the prevention of malicious insider acts, instilling feelings of safety and respect, or dispelling a grievance. Healthy cultures that effectively mitigate insider threat risks often share the following traits:

- Everyone is treated with fairness and respect.
- The organization communicates effectively.
- Leaders set and enforce boundaries.
- Members of the organization are held accountable for their behavior.
- The organization fosters a nurturing environment.
- Bullying and threatening are not tolerated.
- People are encouraged to report unacceptable behavior without fear of repercussion.

[88]Adapted from Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 64). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

[89]Adapted from Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 63). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Managing Domestic Violence

Domestic violence abusers and victims may also require organizational intervention, especially if the harassment or abuse follows an individual into the organization. According to the U.S. Bureau of Labor Statistics, 40 percent of women who died because of workplace violence in 2016 did so at the hands of domestic partners or relatives.[90] Both abusers and victims can be found throughout organizations.

Considering the Abuser

Special considerations are necessary for managing an abuser. Ask these questions:

- Did the abuser harm or threaten a family member within the same organization?
- Did the abuser use organizational resources to harm or threaten a family member?
- Did a victim make a report to a threat management team, managerial staff, or leadership?
- Does the organization have policies in place for preventing domestic violence?

If the answer to any of the above questions is "yes," then a threat management team can proceed with recommending targeted violence or harassment intervention strategies. In all cases, the organization should request the assistance of legal counsel to advise on appropriate courses of action.

Considering the Victim

It is not an invasion of privacy if a threat management team recommends action when made aware of a potential domestic abuse situation that could possibly involve the workplace or organizational site. Employers and organizational leadership have a responsibility to prevent violence in the workplace or organization site, regardless of the victim's expressed or unexpressed preferences regarding their involvement.

It is also important to manage these situations with sensitivity; organizations should treat victims with care and concern. And organizations should make it clear to victims that their privacy will be preserved, including only disclosing information about their circumstance to those who have a need-to-know due to their involvement with protecting the person or organization from violence. When an individual is identified as being in danger from an abusive partner, a threat management team can recommend a variety of steps, to include:

- Distribute the suspected abuser's photograph to security personnel, receptionists, and coworkers.
- Deny the suspected abuser's entry into the work or organizational site, especially if a restraining or protective order exists.
- Designate a parking space closer to the entrance; provide security escort to vehicle or public transportation.
- Change the victim's working hours to peak times.
- Remove the victim's name from telephone directories and screen incoming phone calls.
- Relocate the victim to another business or organizational location, if possible.
- Refer the victim to outside agencies for care and counseling.

The threat management team should document every report of domestic violence or threatened abuse from an abuser to a victim in the workplace or organizational site, no matter how minor. The documentation can be used later for other intervention strategies or for reports to law enforcement.

[90]U.S. Bureau of Labor Statistics. (2017). Fatal Occupational Injuries in 2016 (Charts). slide 10. Retrieved from https://www.bls.gov/iif/oshwc/cfoi/cfch0015.pdf

Managing Mental Health

Mental health concerns associated with insider threats are complex and present an area where organizations must exercise special care and diligence. In all cases, intervention strategies need to account for both the protection of the organization and the well-being of the person of concern. Nowhere is this concept more crucial than in areas where mental health may be a factor. It is a best practice to secure the advice of a qualified threat assessment professional in the early stages of incident management for those persons of concern who may be dealing with a known or suspected mental disorder.

Considering the Person of Concern

There are a range of strategies that organizations should consider with the advice of a behavioral scientist or other qualified mental health professional and legal counsel, to include:

- Referring the person of concern for professional help, such as mental health or personal counseling
- Employing third-party assistance, monitoring, and/or intervention, such as by family, friends, or social service organizations (if, after careful consideration, deemed useful and not in violation of the employee's right to privacy)
- Encouraging the person of concern to seek medical attention
- Placing the person of concern on medical leave
- Committing a person of concern to a psychiatric facility
- Engaging law enforcement for situations involving imminent threat

Although rare, hospitalization of the person of concern may be necessary to protect the safety of the person of concern or others. Involuntary commitments must meet the individual state standard for commitment, and, typically, a showing must be made that the person of concern demonstrates signs of mental illness, poses an imminent risk of harm to self or others, and is incapable of self-care. Decision-makers should avoid the temptation to accept a voluntary commitment from a person with a mental illness when they already meet the standards for involuntary commitment. If the person of concern voluntarily commits themselves, they may be able to check out of a facility at a time of their own choosing, regardless of whether they are really ready to be released.

For situations involving a person of concern who poses an imminent threat to oneself or others, it is a best practice to engage law enforcement to seek medical or mental health interventions rather than attempting an organizational intervention.

If (or when) a person of concern is assessed by a behavioral scientist or other qualified mental health professional as not presenting an insider threat risk, consider conditioning return to work or organizational activities based on a fitness-for-duty examination provided by a qualified health professional. Since a fitness-for-duty examination may be subject to certain laws depending on the type of condition and/or the job or activity in which the person of concern participates, organizations should seek legal counsel when requesting a fitness-for-duty examination.

Organizations should seek the advice of a behavioral scientist or other mental health professional and legal counsel regarding all applicable laws, duties, and protections for both the person of concern and the organization.

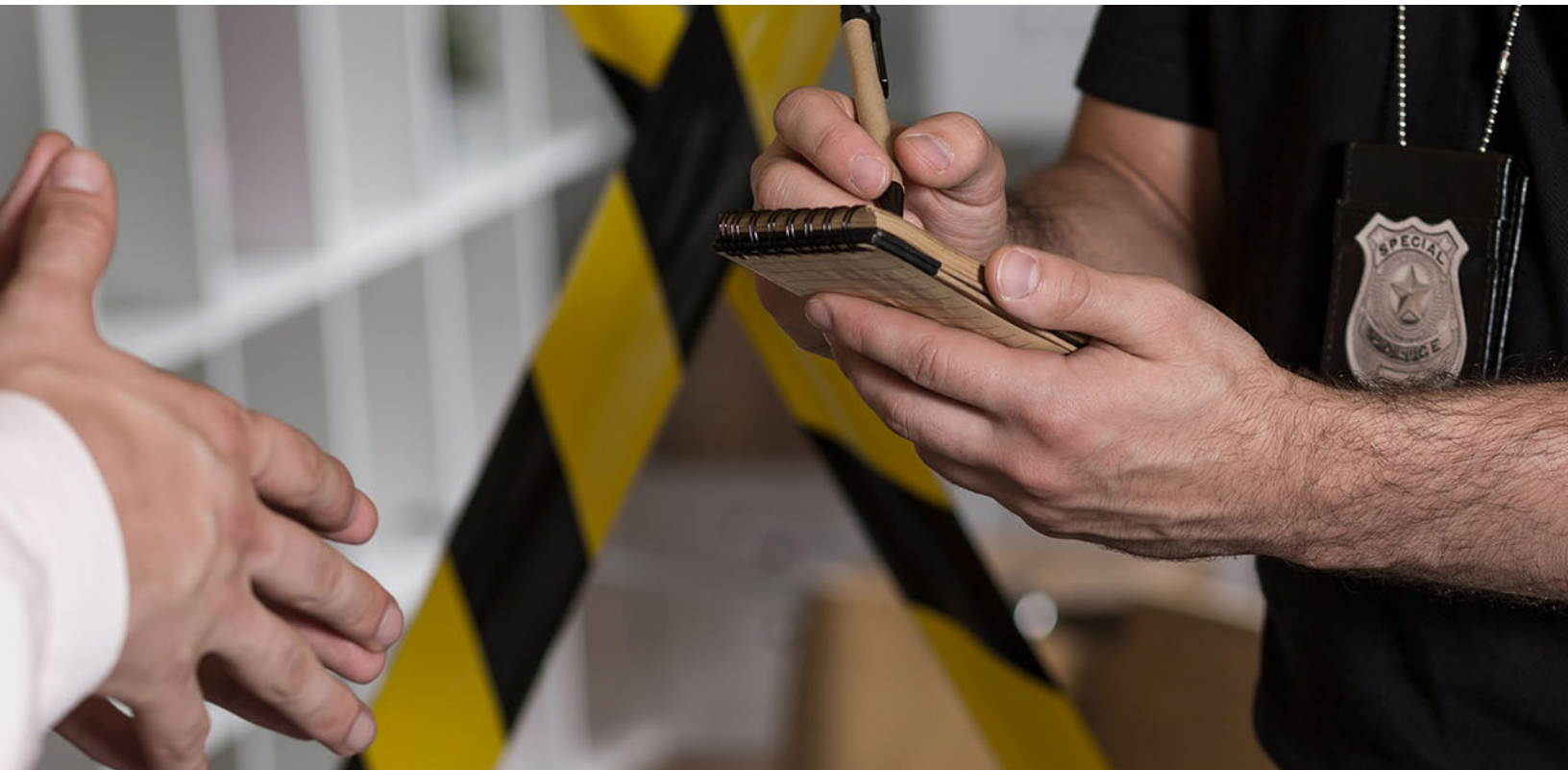
Use of Law Enforcement in Threat Management

While actual criminal violations should always be reported to local law enforcement, the organization should carefully consider the potential risks and benefits of requesting law enforcement assistance in a situation that does not rise to the level of a criminal act. In advance of any incident, the organization should establish a cooperative relationship with local law enforcement and determine the circumstances under which the threat management team may request assistance.

As a guide, consider requesting the assistance of local law enforcement when:

- Actual criminal violations exist
- A threat of violence is imminent or taking place
- An involuntary mental health commitment is necessary
- A potentially violent person is being suspended or terminated
- An incident of domestic violence threatens the safety of the organization
- Periodic or episodic wellness checks are needed to ensure the safety of a potential victim or the person of concern

Establishing a cooperative relationship with local law enforcement may also open avenues to additional resources to which a threat management team would not otherwise have access. Further, such a relationship with local law enforcement can assist the organization in planning for emergency response, ensure the police have correct information about an organization in its dispatch system, aid in gaining additional support during periods of increased risk, and better prepare the organization for emergencies.



Suspensions and Terminations for Persons of Concern[91]

When terminating an employee or expelling a member, organizations should be thoughtful and respectful, and they should develop an approach designed to achieve a safe end state. Organizations should conduct every termination and suspension in the context of threat management, especially if the reason for the termination involves behaviors tending toward violence. Consider the following actions:

Have a plan to retrieve the person's personal belongings and to stop their physical and logistical access.

Designate the space, place, and time of the meeting; it should be somewhere safe and private.

Have security present or standing by. Consider law enforcement, if applicable and available.

Describe the purpose of the meeting. Present observations and concerns about behaviors and impacts on the organization.

Address behaviors as a performance issue and describe problems in behavior-specific terms.

Do not use language that refers to attitudes, beliefs, or motives. Focus on the behaviors and the impacts.

Offer a face-saving outcome for the employee, including a termination package that allows the employee to move forward in life with dignity and self-respect intact. Organizations should consider such a package in the interest of safety, even if not typically offered by the organization, during terminations for cause.

Extend health benefits, including Employee Assistance, to the terminated employee to ensure adequate mental health treatment continues. In cases where the terminated employee possess unique capabilities (e.g., hacking, IT administration, etc.) or retains sensitive organizational information, consider making severance benefits and/or compensation contingent on appropriate behavior over an extended period of time.

Formulate a response to provide coworkers or organizational members in the event of future queries about the former employee or member.

Consider implementing ongoing security measures following the termination to look for any efforts by the employee or member to continue contact with the organization and/or its members.

Identify existing social systems that could provide insight into the former employee's or member's behavior, including social media, EAP support, the police, family, and/or friends.

Consider monitoring open source social media of the person of concern post suspension or termination, if appropriate and authorized. Often, such persons will reveal concerning behaviors, such as a recent weapons acquisition or stalking behaviors, on those sources.

Seek the advice of legal counsel to ensure an understanding of legal obligations and any constraints, particularly regarding termination, flexible separation arrangements, or securing restraining or protective orders.

[91]Adapted from American Society for Industrial Secruity. (2020, May 7). Standard: Workplace Violence and Active Assailant-Prevention, Intervention, and Response. (pp. 25-26). ASIS WVPI AA-2020. ASIS International, ISBN 978-1-951997-03-8

Monitoring and Closing a Case

If a person of concern is terminated, expelled, or banned, their removal from the environment does not mean that person is no longer a threat. Grievances may persist, and former employees may use their prior insider knowledge to regain access illegitimately. Organizations should consider implementing an elevated protection posture or additional mitigation measures. Organizations should begin threat monitoring immediately after terminating a person of concern.

Threat monitoring is a management strategy that allows an organization to continue to have contact with a person of concern to assess changes in behavior. There is no time limit or requirement for monitoring; it depends on the organization's acceptable level of risk.

In these circumstances, the threat management team should continue to gather information and assess risk. Best practices include compiling a list of persons or entities for the threat management team to contact periodically to gather information about the person of concern's behavior and ensuring the threat management team remains alert for any new information, behaviors, or circumstances that could raise concerns or risks to the organization. This information gathering can involve organizational issues that precipitated a prior grievance or an event external to the organization that could trigger a potentially harmful act from the former insider. Once an assessor has determined a person of concern's behaviors have changed enough to no longer warrant a threat to the organization or its people, the threat management team can consider discontinuing monitoring and closing the case.

To close a case, a threat management team should be able to:

- Articulate why the threat management team initially determined that a person of concern posed a threat.
- Document changes in the person of concern's thinking and behavior that negate the original concerns.
- Describe why the person of concern is unlikely to pose a future insider threat to the organization.

At the close of a case, organizations should file all documentation for the case and the person of concern and keep it in accordance with organizational policy.

Finally, at the conclusion of a case, the organization should review the incident and any precipitating events as well as the organization's response in order to determine if any changes are needed in workplace policy, conditions, or incident management to avoid similar events or to improve insider threat management.

Avoid Common Pitfalls[92]

Threat management can be short-term or long-term, with an open case ranging in duration from days to years. And case duration can be difficult to predict accurately; as cases that initially seem short-term may ultimately turn out to be long-term and cases that appear to be resolved may end up requiring reassessment as new facts and circumstances emerge.

In addition to case-duration ambiguity, fatigue can also become an issue. After a period of time, a threat management team may begin to feel exhausted, or worse, desensitized. Organizations should consider rotating the demands of a long-term case among the team members to promote fair workloads, as well as monitoring scheduling to allow for downtime or vacations. Also, organizations should ensure to weigh the priorities and demands of each case, especially as new cases develop while the team is still working existing cases.

Organizations should be prepared to transfer cases, when necessary. If a person of concern moves to another facility or organizational location the organization should transfer the case and all relevant information in a responsible manner, including thorough transfer briefings and follow-up to the new environment and threat management team. Accurate records and effective communication will help pass both responsibility for the case and for the person of concern and will serve to protect both organizations.

Concluding Thoughts

The issue of insider threat management is much more nuanced and prevalent than the highly publicized, but rare, instances of disturbed employees engaging in violent activities. Only a very few organizations will ever experience episodes of that kind; a far greater number will face other forms of insider threat, such as sabotage, theft of intellectual property, and cyberattacks. The organization's leadership is ultimately responsible to protect the organization and its members by taking measures to mitigate insider threats.

Users of this *Guide* should remember there is no "one-size-fits-all" approach to threat management. Intervention strategies may not always apply strictly to the person of concern, nor will each strategy work as intended. Effective approaches implement multiple, complementary solutions that affect the person of concern, the potential victim, and the organizational environment. They should be holistic, respectful, and prevention-focused, and they should use case-specific creative solutions. Intervention strategies should be a careful balance between protecting the organization and caring for persons of concern.[93]

An important consideration is avoiding a circumstance where the management strategies selected become a person of concern's breaking point by validating their grievance or creating new ones. When implementing intervention strategies, the organization should consider how their decisions, actions, and delivery could affect a person of concern's life, employment status, relationships, and dignity.

Organizations with effective threat management programs plan well, share information, and understand when urgency is needed. They act with care and respect to preserve dignity, especially when setting rules, limitations, and boundaries for the person of concern, and they provide clear guidance and oversight for those implementing solutions. They continually re-evaluate active cases, re-engage when necessary, and understand that patience and persistence may be needed throughout the process.

---

[92]Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 52). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

[93]Intelligence and National Security Alliance Cyber Council: Insider Threat Task Force. (2013, September). A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector. (pp. 10-11). Retrieved from https://www.nist.gov/system/files/documents/2017/06/08/20131213_charles_alsup_insa_part4.pdf

Case Study

A Successful Threat Management Strategy

To optimize the opportunity for success, threat management strategies should strike a careful balance between protecting the organization and caring for a person of concern. Even with careful attention, strategies can still fail, and some can even exacerbate the situation. A successful threat management strategy can reduce the risk posed by a person of concern, prevent an insider incident, and protect the organization and its people. If initial strategies fail, organizations should continue to seek the right option that will prevent an insider incident and mitigate risk to the organization, even if the person of concern has been removed from the organization. In this example, an employer followed a defined threat management process after identifying a person of concern and assessing those concerns as a potential threat to the organization. As the threat evolved, the organization adjusted its approach, escalating its interventions, while complying with applicable laws, rules, and regulations. When the capabilities of the organization were exceeded, the organization engaged an outside authority to help them continue to assess and manage the threat.

THE INSIDER

A 37-year old Automation Technician and Safety and Control Officer at a petroleum processing plant in the southern U.S. who was responsible for the maintenance and repair of all pneumatic, electronic, computer process controls and plant online cryogenic systems.

INDICATORS

An investigation and subsequent assessment revealed the technician had:

- A tendency toward violence
- Verbally abused and intimidated his coworkers and his supervisor
- Repeatedly sexually harassed and stalked a female coworker
- Physically confronted his supervisor
- Verbally and physically abused his terminally-ill spouse

INITIAL INTERVENTION STRATEGY

Based on their initial assessment, the organization placed the technician on progressive discipline, wrote a Warning of Unsatisfactory Job Performance, and suspended him with pay for four days. In addition, the organization instructed him to develop a plan during his suspension to improve his performance and change the behaviors laid out in his performance report. Unfortunately, this initial strategy had no apparent effect, as his performance failed to improve, and further issues developed following his return to work.

SECOND INTERVENTION STRATEGY

The technician became more belligerent, defied orders, and refused to make safety improvements to the plant, increasing the risk of accident to the organization and its people. The organization decided to issue a Final Written Warning of Unsatisfactory Job Performance and suspend him without pay for one week. In addition, they instructed him to refrain from any contact with plant personnel or work activities and cautioned him that any further problems would result in immediate dismissal.

Despite these two management interventions, the individual's concerning behaviors escalated. While suspended, he became more threatening and more hazardous to the safety of the organization and his coworkers. During this time, while at a party with coworkers, he reportedly used an assault rifle to shoot an effigy of his supervisor.

Case Study

A Successful Threat Management Strategy (cont.)

SECOND INTERVENTION STRATEGY (CONT.)

When employees covering his job asked for the password to the automated safety control system for the plant, he refused to provide it. Worse still, he tried twice to remotely manipulate the safety systems to create a crisis, which he assumed his supervisor would not be able to fix without his assistance. Fortunately, he was unsuccessful in these sabotage attempts.

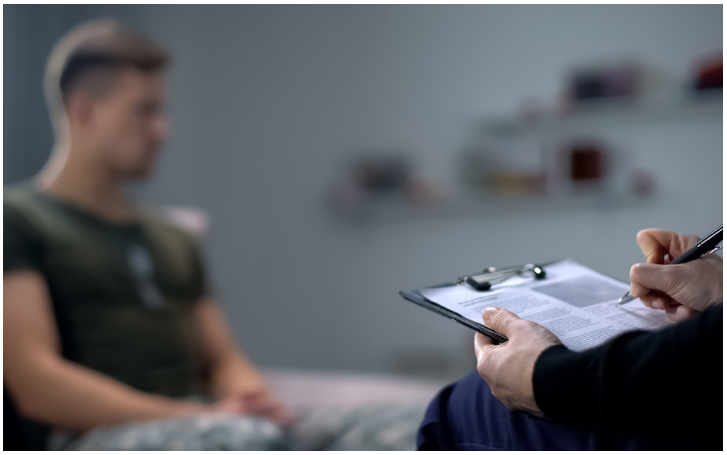
The technician's threatening behavior, his refusal to supply the password to the safety control systems, and his efforts to sabotage the plant's safety control mechanisms caused his organization to become wary of terminating him for fear of a violent reprisal.

While the technician was on suspension, the company's security, HR, and operations elements conducted a collaborative investigation of his behavior and its impact on team members and plant productivity. This review included consultation with an external security/mental health professional qualified in insider threat risk; an effort to help the threat management team assess and manage the evolving, and apparently, intractable threat.

THIRD INTERVENTION STRATEGY

After careful assessment of the evolving situation, the organization developed a third management strategy. This new approach attempted to address the individual's concerns and grievances and sought to help him manage his anger and concerning behaviors. The strategy involved obtaining medical assistance for the technician and his sick wife (who had terminal cancer and was actively suicidal), placing him on paid leave, continuing efforts to rehabilitate him through the Employee Assistance Program, sustaining ongoing therapy and evaluation, and third-party monitoring.

After some time, the organization determined that terminating the technician's employment was necessary, but, by then, they had addressed the individual's issues and were confident that the termination could take place without the risk of violence. Also, notably, the organization did not close the insider threat case on this person of concern. Instead, the threat management team continued to monitor, and the organization continued to provide assistance until a clinical psychologist decided that the former technician no longer posed a threat to the organization.



IMPACT OF THE SUCCESSFUL STRATEGY

The organization credits its sustained effort to employ an effective intervention strategy with preventing an act of sabotage or violence that an abrupt termination might have provoked.

Key Points

- **Proactively managing insider threats can change or stop the trajectory or course of events from a harmful outcome to an effective mitigation**.
- When acting, **remain mindful of the connectivity between protecting safety and caring for persons of concern**.
- **Manage insider threats through interventions intended to reduce the risk posed by a person of concern**, always keeping in mind that the prevention of an insider threat incident and protection of the organization and its people are the ultimate goals.
- **Implement recommendations for action—even arrest or hospitalization—in a respectful manner,** considering the potential consequences of planned interventions before taking action.
- **Preserving the dignity of a person of concern is a management solution** and acting with respect to preserve dignity can prevent or mitigate the development of new grievances and/or rationale for an act of violence, sabotage, or other form of harm.
- **Case management is unique for each instance**, with every insider threat case requiring a tailored and multi-disciplinary approach.
- When implementing solutions, threat management teams should **consider actions directly involving the person of concern**, as well as **measures focused on the potential victims or targets**, and the **overall organizational situation and setting**.
- The management approach should **consider addressing the source of the individual's disgruntlement** by addressing their real or perceived grievances. Addressing a grievance can alter a person of concern's trajectory toward violence or an insider threat incident.
- **Sustain management solutions**; do not end them prematurely just because an insider threat is stopped, removed, or denied access via other means. Connecting with the person of concern will aid and encourage intervention and will enable the threat management team to continue monitoring.
- **Caution should be used in each situation of concern** to make sure the response of authorities is appropriate to the problem. The most familiar response may or may not be the best response or the best course of action.

- While actual criminal violations should always be reported to local law enforcement, the threat management team should **carefully consider the potential risks and benefits of requesting law enforcement assistance** in a situation that does not rise to the level of a criminal act.
- A **cooperative relationship with local police can benefit an organization** by providing a channel to resources that can only be accessed through law enforcement agencies.
- When terminating an employee or expelling a member, be thoughtful, be respectful, and **develop an approach designed to achieve a safe termination**.
- **Conduct each termination or suspension in the context of threat management**, especially if the personnel action involves behaviors of concern.
- **Removal of a person of concern from the environment** (e.g., by termination, expulsion, or banishment) **does not mean the person is no longer a threat**.
- **Grievances may persist** after an employee's termination, expulsion, or banishment, and former employees may use their prior insider knowledge to regain access illegitimately. **Consider implementing an elevated protection posture or additional mitigation measures**.
- **Threat monitoring is a management strategy** that allows an organization to continue to have contact with a person of concern to assess changes in behavior.
- If a threat management team must continue to gather information and assess risk, **a best practice includes compiling a list of persons or entities for the threat management team to contact about the person of concern's behavior**.
- **Once an assessor has determined a person of concern's behaviors have changed enough** to no longer pose a threat to the organization or its people, the **threat management team can decide to discontinue monitoring and close the case**.
- **Case duration can be difficult to predict accurately. Some cases that may initially seem to be short-term may ultimately turn out to be long-term.** Cases that appear to be resolved may end up requiring reassessment as new facts and circumstances appear.
- **If a person of concern moves to another jurisdiction, transfer the case and all relevant information in a responsible manner**, including thorough transfer briefings and follow-up to the new environment and threat management team.
- If initial strategies fail, **continue to seek the right option that will prevent an insider incident and mitigate risk to the organization**, even if the person of concern has been removed from the organization.

7 Conclusion

The consequences of an insider incident can ripple through an organization and community with devastating outcomes and long-term negative impacts. As noted throughout this *Guide*, the goal is to help individuals, organizations, and communities to understand these threats, work toward preventing them, and provide practices that organizations of any size can consider to establish or enhance an insider threat mitigation program.

A widely cited adage applies well to the pervasiveness of the insider threat: Two types of organizations exist—those whose members have already stolen intellectual property, and those who simply do not know it yet. In response, this *Guide* offers the most enlightened recommendations and proven best practices as an aid for organizations to use to organize to prevent and mitigate the insider threat.

The costs of intellectual property theft, sabotage, or espionage are felt in innumerable ways, including the loss of customers, damage to reputation and brand, decline in revenue, loss of market share, and degraded competitive advantage. For targeted violence incidents, the costs associated with a perceived sense of safety can undermine any organization and will likely create a new long-term reality for the institution, people, and stakeholders. On a global scale, the average cost of an insider-related data breach in 2019 was $11.5 million. Malicious insider incidents cost approximately $4.1 million a year for each affected organization.[94] Financial institutions, in particular, have long been lucrative targets for insiders. Insider attacks on electronic systems can result in financial and intellectual property theft, damaged or destroyed assets, and firmwide disruption to internal systems and customer operations.

The securities industry is especially concerned with an insider's ability to capitalize on their familiarity with industry systems to launch attacks without attracting notice, and the growing risk from unintentional insider incidents, especially as authorized access to

[94]Ponemon Institute LLC. (2020). 2020 Cost of Insider Threats Global Report. Retrieved from https://www.observeit.com/2020costofinsiderthreat/

sensitive information continues to expand. At its core, industry advocates surmise, the insider threat is as much a human as a technical problem, an important consideration when thinking about the threat and defining the threat for a specific organization, sector, or function.[95]

The fundamentals are clear—an effective insider threat program provides tools to help trusted insiders before an innocent act of negligence, a grievance, or a personal stressor becomes a disruptive incident or, worse, a destructive act. Successful programs build a culture of reporting and prevention. They establish or reinforce the organization's values and provide a positive statement of its investment in the well-being of its people, as well as its overall resilience and operational effectiveness.

Prevention of insider threat incidents is achievable when organizations focus on:

- Tailoring their insider threat program to the organization's unique mission, culture, and threat landscape, particularly focusing on the assets it values most
- Applying the framework of detect and identify, assess, and manage for the prevention, protection, and mitigation of insider threats
- Training people to recognize concerning behaviors and how to report
- Instilling a positive culture for reporting and making sure people know the program is designed to help them as well as the organization
- Establishing a threat management team that uses the multi-disciplinary capabilities needed to assess the facts and concerning behaviors related to a potential insider threat
- Developing assessment and intervention capabilities and management actions that are respectful and consider the dignity, rights, and privacy of an employee
- Providing a safe, non-threatening environment where individuals who might pose a threat are identified and helped before their actions can cause harm

Preparedness is a shared, organization-wide obligation. As individuals, each of us has a role to recognize insider threats and report persons exhibiting concerning behaviors. Organizations should be prepared to receive reports of potential threats and anomalous behaviors, assess those threats, and implement management solutions focused on the person of concern, the potential target, and the organizational situation or setting. Working together helps keep the organization safe from harm and more resilient when disruptions strike.

Finally, this *Guide* presents recommended approaches and best practices as options for consideration when developing an insider threat program; they are not applicable in all circumstances or definitive, nor are they required by any law or regulation. Federal, state, local, tribal, and territorial governments, non-governmental and social organizations, and the private sector may, at their sole discretion, implement any or all of these options they consider applicable. This *Guide* is not intended to and does not create any legal rights or claims. CISA will not take any action against an entity or company that chooses not to implement these options for consideration.

[95]SIFMA. (2018, February). Insider Threat Best Practices Guide, 2nd Edition. (p.5). Retrieved from https://www.sifma.org/wp-content/uploads/2018/02/insider-threat-best-practices-guide.pdf

Appendix A. Summary of Key Points

Chapter 2: Defining Insider Threats

- **The insider threat is similar for many organizations in terms of the nature of the threat**—a trusted insider who takes advantage of his or her access to do harm to the organization's mission, products, resources, personnel, facilities, information, equipment, network, or systems.
- **The character and conduct of the threat will manifest in various ways** depending on the nature of the organization, the type of work or sector, the products and services performed, and the assets that should be protected from loss, compromise, damage, or theft.
- **Each insider threat will have or have had some level of a trust relationship with their victim** and act in a way that is outside the expectations of that trust relationship.
- **Organizations should tailor their approach to the insider threat** to address the unique nature of their operating environment and what they value.
- **Insider threats are intentional and unintentional**. A significant portion of insider threats involve negligent or accidental behaviors.
- **Not all intentional insider threats are malicious**. An insider threat can occur when an individual commits a dangerous act for any number of reasons outside of an intent to harm an organization.

Chapter 3: Building an Insider Threat Mitigation Program

Principles and Keys for Success

- **Promote a protective and supportive culture** throughout the organization.
- **Safeguard organizational valuables** while protecting privacy, rights, and liberties.
- **Remain adaptive** as the organization evolves and its risk tolerance changes.
- **Focus on prevention** and helping people versus just catching them doing things wrong.
- **Employ a balance of positive and negative incentives**, promoting employee satisfaction and performance while avoiding overly aggressive reactions following notification of a threat.

Plan

- **Visibly involve executive or senior leaders** in emphasizing the program to drive positive support.
- **Appoint a single individual, commonly called the Senior Official**, as the responsible official for the overall management and oversight of the program.
- **Form a governance group** consisting of multiple stakeholders who possess information pertinent to the background, conduct, and activities of trusted insiders.
- **Establish guiding principles** that align to the culture and business of an organization and describe its purpose, goals, and objectives.
- **Sell the program** to leadership, members, and associates by **describing why it is being established**; a key element is to emphasize the collective harm an insider can pose, particularly in a business setting.
- **Start small, using existing capabilities and resources**; use programs such as harassment and/or violence prevention as a practical starting point for a broader insider threat program.
- **Identify, track, and monitor the organization's critical assets.**

Organize and Equip

- **Employ the fundamental elements for an effective operational program—information, technology, people, reporting paths, and skilled investigators**; when the elements are fused, an intricate pattern of abnormal behavior indicative of insider threat activity can be recognized.
- Grow a program by employing **automated tools or dedicated personnel based on the type and size of an organization and its culture**, the nature and value of its mission, and its risk tolerance toward insider threat incidents.
- **Augment technology with a skilled investigator** to interpret and make sense of data.

- **Develop an Insider Threat Incident Response Plan** inclusive of the scope, established roles and responsibilities, methodology, incident response phases, guidelines for incident response processes, reporting procedures, and an escalation chain.
- **Develop and employ risk rubrics as evaluation tools** to rate or categorize insider threats to indicate whether an individual poses a low/medium/or high risk of violence, theft, sabotage, etc.
- **Customize risk rubrics** based on an organization's threat criteria and acceptable level of risk.
- **Establish a threat management team** to assess and manage insider threats; it is the backbone of a threat management program and is integral to the program's success.
- **Staff the team with a wide range of functional disciplines and representatives**; threat management depends on the synthesis and analysis of many diverse information sources.
- **Consider alternative naming conventions for the threat management team**—one that reinforces the helping nature of the program is advisable.

Train and Execute

- **Instill a positive culture for reporting and supply confidential means of reporting.**
- **Emphasize the need to prevent insider threat actions before they occur**; educate the workforce or membership about the potential consequences of insider threats.
- **Train employees on insider threat awareness and reporting** and encourage participation to help detect and identify, assess, and manage insider threats.

Evaluate and Improve

- **Regularly exercise the insider threat mitigation program**, update its policies using a conditions-based as well as a temporal-based approach, and conduct regular audits of the program to ensure oversight and compliance.
- **Designate officials who will conduct independent assessments of the program's compliance** with insider threat mitigation program guidelines and policies.

Chapter 4: Detecting and Identifying Insider Threats

- A successful program will recognize that the **insider threat evolves over time and exhibits multiple overlapping detectable and observable behaviors**.
- **Behavior is what matters most**, not the motivation, whether it is political, religious, ideological, financial gain, or revenge.
- **Confirmation of any threat indicator requires a solid understanding of context**; recognizing that people often display behaviors representative of an individual point in their life that may not result in a direct expression of a threat.

- **Exhibiting no indicators does not guarantee that a person will not pose an insider threat**.
- **Professional stressors have the additional effect of creating potential grievances** against an employer, organization, or agency.
- **Behavioral indicators reflect patterns of activity over time**, based on the way the insider interacts within the organization. These indicators are directly observable by peers, HR personnel, supervisors, managers, and technological systems.
- **Technical indicators are those that require direct application of IT systems and tools to detect**. UAM is the most frequently used application for the detection of technical insider threat indicators.
- **Violence carries with it specific behaviors or collections of behaviors** that instill fear or generate a concern that a person might act out violently.
- **People are key sensors for the detection and identification of an insider threat**. People may have an awareness of the predispositions, stressors, and behaviors of insiders who may be considering taking violent actions toward an organization.
- **Those who perpetrate violence or steal data or secrets often leak their plans or grievances**. It is well established that a person of concern will tell others of their intent or plan at a much greater rate than they will tell the target of their plan.
- As part of an organization's or business' obligation to provide a safe environment, the **insider threat policies and programs should always consider a commitment to support domestic violence victims** and to take protective steps when such violence threatens to intrude on the workplace or organization.

Chapter 5: Assessing Insider Threats

- **Threat assessment is the process of compiling and analyzing information about a person of concern** who may have the interest, motive, intention, and capability of causing harm to an organization or persons.
- A **primary purpose of an assessment process is to inform decision-making regarding how to manage a person of concern**, with the goal to prevent an insider incident in any of its expressions and not necessarily to make an arrest or enforce policy with disciplinary measures.
- An **assessment process applies in both urgent/emergency situations and in non-urgent/non-emergency situations**, with the former potentially requiring emergency intervention to protect life, safety, or property.
- Once the threat management team has determined that an assessment is necessary, the **threat management team begins a deep investigation into the person of concern**, which involves gathering the evidence, analyzing the information, and generating a report outlining findings and making clear, actionable recommendations.

- The **ultimate question to answer in a threat assessment is whether a person of concern is on a path to action**, and, if so, to determine how fast they are moving and where intervention may be possible.
- In **investigative and assessment planning**, considerations include determining the use of trained internal staff or outside law enforcement for incident intake, the need for immediate safety and/or security to protect people and property, ensuring criminal prosecutions are not compromised, and handling hostility in the investigative process.
- A **successful investigation** of a person of concern and any insider incidents or potential incidents **requires the collection and analysis of available information gathered from all potential sources**, including the person of concern, coworkers or associates, family or neighbors, and IT-related or online material.
- For incidents where a law has been broken or there is an imminent threat of violence, the **threat management team must ensure that its actions in incident response and assessment do not interfere with the ability of law enforcement to investigate or inhibit future prosecution**.
- After evidence has been collected and analyzed and the threat management team has determined whether a person of concern poses a threat, the team **generates a report outlining its findings and making clear, actionable recommendations to manage the threat and prevent an insider incident**. The report is the final step in the threat assessment process and the first step in threat management.

Chapter 6: Managing Insider Threats

- **Proactively managing insider threats can change or stop the trajectory or course of events from a harmful outcome to an effective mitigation**.
- When acting, **remain mindful of the connectivity between protecting safety and caring for persons of concern**.
- **Manage insider threats through interventions intended to reduce the risk posed by a person of concern**, always keeping in mind that the prevention of an insider threat incident and protection of the organization and its people are the ultimate goals.
- **Implement recommendations for action—even arrest or hospitalization—in a respectful manner,** considering the potential consequences of planned interventions before taking action.
- **Preserving the dignity of a person of concern is a management solution** and acting with respect to preserve dignity can prevent or mitigate the development of new grievances and/or rationale for an act of violence, sabotage, or other form of harm.
- **Case management is unique for each instance**, with every insider threat case requiring a tailored and multi-disciplinary approach.

- When implementing solutions, threat management teams should **consider actions directly involving the person of concern**, as well as **measures focused on the potential victims or targets**, and the **overall organizational situation and setting**.
- The management approach should **consider addressing the source of the individual's disgruntlement** by addressing their real or perceived grievances. Addressing a grievance can alter a person of concern's trajectory toward violence or an insider threat incident.
- **Sustain management solutions**; do not end them prematurely just because an insider threat is stopped, removed, or denied access via other means. Connecting with the person of concern will aid and encourage intervention and will enable the threat management team to continue monitoring.
- **Caution should be used in each situation of concern** to make sure the response of authorities is appropriate to the problem. The most familiar response may or may not be the best response or the best course of action.
- While actual criminal violations should always be reported to local law enforcement, the threat management team should **carefully consider the potential risks and benefits of requesting law enforcement assistance** in a situation that does not rise to the level of a criminal act.
- A **cooperative relationship with local police can benefit an organization** by providing a channel to resources that can only be accessed through law enforcement agencies.
- When terminating an employee or expelling a member, be thoughtful, be respectful, and **develop an approach designed to achieve a safe termination**.
- **Conduct each termination or suspension in the context of threat management**, especially if the personnel action involves behaviors of concern.
- **Removal of a person of concern from the environment** (e.g., by termination, expulsion, or banishment) **does not mean the person is no longer a threat**.
- **Grievances may persist** after an employee's termination, expulsion, or banishment, and former employees may use their prior insider knowledge to regain access illegitimately. **Consider implementing an elevated protection posture or additional mitigation measures**.
- **Threat monitoring is a management strategy** that allows an organization to continue to have contact with a person of concern to assess changes in behavior.
- If a threat management team must continue to gather information and assess risk, **a best practice includes compiling a list of persons or entities for the threat management team to contact about the person of concern's behavior**.
- **Once an assessor has determined a person of concern's behaviors have changed enough** to no longer pose a threat to the organization or its people, the **threat management team can decide to discontinue monitoring and close the case**.

- **Case duration can be difficult to predict accurately. Some cases that may initially seem to be short-term may ultimately turn out to be long-term.** Cases that appear to be resolved may end up requiring reassessment as new facts and circumstances appear.
- **If a person of concern moves to another jurisdiction, transfer the case and all relevant information in a responsible manner**, including thorough transfer briefings and follow-up to the new environment and threat management team.
- If initial strategies fail, **continue to seek the right option that will prevent an Insider Incident and mitigate risk to the organization**, even if the person of concern has been removed from the organization.

Appendix B. Tools and Resources

The Department of Homeland Security provides the Insider Threat and Violence Prevention tools and resources without endorsing any specific company or entity. The tools and resources identified are a starting point for an organization's insider threat program and do not encompass all resources that may be available. Resources requiring a paid subscription are identified with an asterisk (*). The use of any paid resources is at the discretion of the organization.

Program Management

The DoD published the "DoD Insider Threat Program Best Practice 5.1 Processes: Getting Started" highlighting several DoD insider threat programs and their best practices in implementing their programs. https://www.cdse.edu/toolkits/insider/awareness.html

The Interagency Security Committee produced the "Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide" to provide guidance, best practices, and recommendations for incorporating an insider threat management program, specifically addressing an active shooter, into an already existent emergency response program. cisa.gov/publication/isc-planning-and-response-active-shooter-guide

The U.S. Department of Labor developed a Workplace Violence Program that includes policy, roles and responsibilities, prevention, warning signs, and the different levels of violence and response. https://www.dol.gov/agencies/oasam/centers-offices/human-resources-center/policies/workplace-violence-program

The Software Engineering Institute developed "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls" to discuss what could go wrong with an Insider Threat Program. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=446367

The Transportation Security Administration (TSA) published the "Insider Threat Roadmap - 2020," to provide a holistic approach, including guiding principles and strategic priorities, for the establishment of a collaborative program that comprehensively and continuously identifies and mitigates the insider risk to the TSA and the Transportation Systems Sector community. https://www.tsa.gov/news/press/releases/2020/05/14/tsa-releases-roadmap-mitigating-insider-threats-transportation

The North Atlantic Treaty Organization's (NATO) Cooperative Cyber Defense Centre of Excellence developed an "Insider Threat Detection Study" that provides a comprehensive overview of insider threats and provides an interdisciplinary approach analysis that discusses insider threats from technical, legal, and behavioral perspectives. https://ccdcoe.org/library/publications/insider-threat-detection-study/

The Software Engineering Institute published the "Common Sense Guide to Mitigating Insider Threats, Sixth Edition" technical report to provide recommendations based on continued analysis and research on the impacts of insider threats across industries. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644

The DHS published "Insider Threat Programs for the Critical Manufacturing Sector Implementation Guide" to provide guidance and information for critical manufacturing organizations to establish insider threat programs. cisa.gov/publication/insider-threats-programs-critical-manufacturing-sector-implementation-guide

The NITTF's "Insider Threat Guide - 2017" provides best practices that accompany the National Insider Threat Minimum Standards. https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf/ncsc-nittf-resource-library/nittf-produced-guides-templates

The National Behavioral Intervention Team Association Advisory Board published "Standards for Behavioral Intervention Teams" with guidance to develop the most efficient approaches for addressing and preventing crisis events on campuses. https://www.nabita.org/free-resources-list/#standards

The Interagency Security Committee published "Violence in the Federal Workplace: A Guide for Prevention and Response," providing workplace violence prevention and response guidance. cisa.gov/publication/isc-violence-federal-workplace-guide

Securities Industry and Financial Markets Association (SIFMA) published "Insider Threat Best Practices Guide, 2nd Edition" for the establishment and implementation of an Insider Threat Mitigation Program for Cyber organizations. https://www.sifma.org/resources/general/best-practices-for-insider-threats/

The FBI developed "Workplace Violence Issues in Response" aimed at prevention, intervention, threat assessment and management, crisis management and critical incident response. https://www.fbi.gov/file-repository/stats-services-publications-workplace-violence-workplace-violence/view

The Intelligence and National Security Alliance (INSA) published a "Preliminary Examination of Insider Threat Programs in the U.S. Private Sector" spanning insider threats in the public sector. https://www.insaonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/

The NITTF developed an "Insider Threat Program Maturity Framework" that aligns with the existing Minimum Standards. https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

Shawn Thompson and Gabriel Friedlander's "Insider Threat Program: Your 90 Day Plan" is a guide for initiating, developing, and implementing an insider threat program. https://www.itmg.co/e-book-insider-threat-program-your-90-day-plan/

The Occupational Safety and Health Administration (OSHA) developed a "Workplace Violence Fact Sheet" to explain what workplace violence is, who is vulnerable, reporting, protections, and how to get more information. https://www.osha.gov/workplace-violence/prevention-programs

SmartWerksUSA offers "6 Ways to Keep Employees from Stealing from You." The tips begin with the hiring process and proceed through policy development and reporting. https://smartwerksusa.com/articles/when-employees-steal/

INCORP provides information regarding Employee Theft in two parts – the first part offers statistics regarding the magnitude of the problem, and the second part gives tips for prevention.
Part 1: https://www.incorp.com/help-center/business-articles/employee-theft-and-fraud-part1
Part 2: https://www.incorp.com/help-center/business-articles/employee-theft-and-fraud-part2

The FBI launched a Nationwide Awareness Campaign, including a video, "The Company Man: Protecting America's Secrets." The video discusses economic espionage, the cost, and how it puts the Nation at risk. https://www.fbi.gov/news/stories/economic-espionage/economic-espionage

Symantec published a white paper, "Implementing an Effective Insider Threat Program," that focuses on cyber breaches. https://www.broadcom.com/site-search?q=Implementing%20an%20Effective%20Insider%20Threat%20Program

Datto provides an eBook, "The Essential Cybersecurity Toolkit for SMBs." The eBook includes information regarding social engineering scams, how to spot a cyber scam, and a cybersecurity checklist. https://www.datto.com/resources/protect-your-customers-from-cyber-attacks-today

The TSA published slides from the Insider Threat Awareness International Civil Aviation Organization Global Aviation Security Symposium in 2018 that discussed key elements of insider risk and how to mitigate the unique security risks associated with those with privileged access. https://www.icao.int/Meetings/AVSEC2018/Pages/Presentations.aspx

The Software Engineering Institute bulletin, "Navigating the Insider Threat Tool Landscape: Low-Cost Technical Solutions to Jump-Start an Insider Threat Program" includes news, publications, events, and podcasts. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=521696

The National Insider Threat Special Interest Group "Insider Threat Program Training Starts with Security 101" commentary provided by Jim Henderson explains the importance of protecting assets from the malicious insider. https://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

The Software Engineering Institute "Insider Threats: Your Questions. Our Answers" provides a webinar and slides where experts provide an overview of the ongoing research and answers questions about how insider threats continue to evolve. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=634886

The Office of People Analytics published "A Strategic Plan to Leverage the Social & Behavioral Sciences to Counter the Insider Threat" to provide lessons for researchers who want to contribute to insider threat detection, prevention, and mitigation efforts. https://www.hsdl.org/?abstract&did=818886

Veriato sponsored the "2019 Insider Threat Program Maturity Model Report" to help professionals assess their ability to monitor, detect, and respond to insider threats including budgeting for an effective program. https://www.veriato.com/resources/whitepapers

The CDSE "Insider Threat Toolkit" provides resources for awareness and training, policy/legal, reporting, establishing a program, cyber insider threat, vigilance, kinetic violence, and research. https://www.cdse.edu/toolkits/insider/index.php

The Oregon Association of Hospitals and Health Systems developed a Workplace Safety Initiative that includes a downloadable "Workplace Violence Prevention Toolkit." https://www.oahhs.org/safety

The Security Executive Council "Workplace Violence Continuum" graphic provides a downloadable overview of a comprehensive workplace violence mitigation program. https://www.securityexecutivecouncil.com/spotlight/?sid=26503

The CDSE "Cybersecurity Toolkit" provides resources to help with a vigilance campaign. https://www.cdse.edu/toolkits/insider/cyber.html

ObserveIT's "Insider Threat Law: Balancing Privacy and Protection" video explores the legal parameters of implementing an insider threat program. https://www.youtube.com/watch?v=e8XyKKjUeSg

The CDSE "Insider Threat Job Aids" provides resources for risk indicators, reporting procedures, law examples, and policies. https://www.cdse.edu/resources/insider-threat.html

Detecting and Identifying Insider Threats

The FBI published "Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks," which looks at how law enforcement officers and others may identify, assess, and manage the risk of future planned violence. https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Oregon OSHA offers an online course "Violence Prevention Program" to learn about methods to recognize, evaluate, and respond to risk factors related to workplace violence. https://osha.oregon.gov/edu/courses/Pages/violence-prevention-program-online-course.aspx

The Software Engineer Institute podcast "Workplace Violence and Insider Threat" discusses workplace violence, insider threat, and technology to detect an employee's intent. Audio and transcript are available for download. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=525011

Wolters Kluwer provides an office management & HR toolkit "Detecting and Combating Employee Theft" advocating for anti-theft policies and procedures on handling theft in a company. https://www.bizfilings.com/toolkit/research-topics/office-hr/detecting-and-combating-employee-theft

Dulin, Ward, & DeWald, Inc. posted "Steps to Help Avert Sabotage by Former Employees" that includes steps companies can take to keep from serious harm inflicted by former employees. https://dwdcpa.com/blog/steps-to-help-avert-sabotage-by-former-employees

The National Insider Threat Special Interest Group published "Considerations for Outsourcing Work to Third Party Contractors" that includes best practices for ensuring third-party entities are safeguarding your organizations information and assets. https://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

The CDSE provides security training videos available on a variety of subjects, ranging from behavioral indicators of an active shooter to cybersecurity. https://www.cdse.edu/resources/videos/insider-threat.html

* The American Society for Industrial Security (ASIS) "Standard: Workplace Violence and Active Assailant - Prevention, Intervention, and Response" provides an overview of policies, processes, and protocols that organizations can adopt to help identify and prevent threatening behavior and violence affecting the workplace and to better address and resolve unprevented threats and violence. https://store.asisonline.org/workplace-violence-prevention-and-intervention-standard-softcover.html

The Software Engineering Institute developed "An Insider Threat Indicator Ontology," a technical report to encourage using ontology to fill the gap in the insider threat community. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=454613

The INSA published "The Use of Publicly Available Electronic Information for Insider Threat Monitoring" to provide insight into perceptions, plans, intentions, associations, and actions. https://www.insaonline.org/new-insa-report-examines-use-of-publicly-available-electronic-information-for-security-determinations-insider-threat/

The Office of People Analytics developed "Enhancing Supervisor Reporting of Behaviors of Concern" to examine reporting obstacles and methods for increasing supervisor reporting of personnel issues, security concerns, and insider threats. https://www.dhra.mil/PERSEREC/Selected-Reports/

The Software Engineering Institute published an "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors" where the authors seek to close the gaps in literature that make it difficult for organizations to fully understand the insider threat. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=51934

CISA maintains an "Insider Threat Tip Card" for the mitigation and detection of an insider cyber threat. cisa.gov/publication/stop-think-connect-toolkit

The CDSE provides a job aid, "Insider Threat Indicators in User Activity Monitoring," that provides an overview for the guidance and use of User Activity Monitoring. https://www.cdse.edu/toolkits/insider/cyber.html

DHS National Cybersecurity and Communications Integration Center published "Combating the Insider Threat" to provide general characteristics and behavioral indicators of malicious threats and a list of behavior prediction theories and security detection technologies to assist in detecting an insider threat. cisa.gov/insider-threat-cyber

Assessing Insider Threats

The FBI's National Center for the Analysis of Violent Crime (NCAVC) and the Critical Incident Response Group published "Workplace Violence: Issues in Response." This guide provides sample questions to ask in assessing whether an individual poses a threat to an organization. https://www.hsdl.org/?view&did=444583

The National Institute of Justice's "Protective Intelligence and Threat Assessment Investigations" guides law enforcement and others on questions to ask in the assessment for violence. https://www.ncjrs.gov/app/publications/abstract.aspx?id=179981

The American Society for Healthcare Risk Management provides the "Workplace Violence Toolkit" checklist that includes proactive prevention and reactive responses. https://www.ashrm.org/resources/workplace_violence

The CDSE Kinetic Violence Tool kit provides policies, training and awareness, and best practices for kinetic violence. https://www.cdse.edu/toolkits/insider/kinetic.html

Ekran System's "How to Prevent Industrial Espionage: Definition & Best Practices" includes industrial espionage, targets, which industries are at the highest risk, and why we do not hear about all cases. https://www.ekransystem.com/en/blog/prevent-industrial-espionage

The National Insider Threat Special Interest Group "Fraud Prevention Checklist" helps organizations to test the effectiveness of their fraud prevention measures. https://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

The Defense Personnel Security Research Center developed an "Insider Risk Evaluation and Audit Tool" to help gauge an organization's vulnerability to insider threats that includes audit questions. https://www.dhra.mil/PERSEREC/Products/#InsiderRisk

The CERT "Insider Threat Center Vulnerability Assessment" brochure helps organizations determine how prepared they are for insider threats. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51648

The DHS published the "National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat" highlighting risks to critical infrastructure from insider threats. https://publicintelligence.net/dhs-nre-insider-threats/

The USSS developed and published "Enhancing School Safety Using a Threat Assessment Model – An Operational Guide for Preventing Targeted School Violence." The product provides fundamental direction on how to prevent incidents of targeted school violence. cisa.gov/publication/enhancing-school-safety-using-threat-assessment-model-operational-guide-preventing

NaBITA developed five violence risk assessment tools, each with a specific purpose, to assist school personnel in determining what level of risk an individual may pose. https://www.nabita.org/resources/assessment-tools/

The Insider Risk Group provides an assessment approach of "The Critical Pathway to Insider Risk" model by Dr. Eric Shaw as a means of evaluating the risk an individual poses based on behavioral indicators. https://www.insiderriskgroup.com/approach

The CDSE's Insider Threat Job Aid "Critical Thinking Techniques for Insider Threat Analysts" defines the habits of critical thinkers for the accurate interpretation of evidence. https://www.cdse.edu/catalog/insider-threat.html

Managing Insider Threats

The FBI published "Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks" which provides suggestions for how organizations may prevent violence through management strategies. https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

* ASIS "Standard: Workplace Violence and Active Assailant - Prevention, Intervention, and Response" suggests intervention strategies, guidance for the monitoring, and practices for the safe termination of an employee. https://store.asisonline.org/workplace-violence-prevention-and-intervention-standard-softcover.html

The National Institute of Justice's "Protective Intelligence and Threat Assessment Investigations" publication provides guidance on monitoring, controlling, and redirecting a subject and when it is appropriate to close a case. https://www.ncjrs.gov/app/publications/abstract.aspx?id=179981

The INSA "A Preliminary Examination of Insider Threat programs in the U.S. Private Sector" report provides recommendations for the response and management of insider threat incidents currently in use by national and global organizations. https://www.insaonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/

Appendix C. Terms and Acronyms

Terms

Assess	To evaluate or estimate the nature, ability, or quality of.
Assessment Process	To utilize a set of operational activities that combine investigative processes and information-gathering strategies with operationally relevant questions to determine if a person of concern poses a threat.
Behaviors	The way in which one acts or conducts oneself.
Civil Liberties	Individual rights protected by law from unjust governmental or other interference.
Collusive Threat	A subset of malicious insider threat where one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting an insider or several insiders to enable fraud, intellectual property theft, espionage, or a combination of the three.
Confidential	The state of keeping or being kept secret or private.
Criminal Espionage	The covert practice of a U.S. citizen betraying U.S. government secrets to foreign nations.
Critical Asset	Physical or intellectual items whose existence is essential to the operation of an organization which, if compromised, damaged, or lost can have an adverse effect on the confidentiality, integrity, or availability of the organization or cause a severe negative impact on its ability to support essential missions and functions.
Cyber	Relating to or characteristic of the culture of computers, information technology, and virtual reality.
Cyberattack	Any attempt to expose, alter, disable, destroy, steal, or gain unauthorized access to or make unauthorized use of a computer, network, or system.
Cyber Threat	A range of expressions, including theft, espionage, violence, and sabotage, related to technology, virtual reality, computers, devices, or the internet. These expressions are undertaken using a variety of vectors to include viruses, data breaches, Denial of Service attacks, malware, and unpatched software and are considered either unintentional or intentional.

Cyber Threat (Intentional)	Typically malicious actions performed by hostile insiders using technical means intended to disrupt or cease an organization's regular business operations, identify IT weaknesses, gain protected information, or otherwise further an attack plan via access to IT systems. This action can involve changing data or inserting malware or other pieces of offensive software to disrupt systems and networks.
Cyber Threat (Unintentional)	Consist of non-malicious (oftentimes accidental or inadvertent) exposure of an organization's IT infrastructure, systems, and data that causes unintended harm to an organization. Often the insider may not know they are participating in the disruption (i.e., an unwitting insider).
Detect	To discover or identify.
Deter	Prevent the occurrence of a hazard.
Due Process	Formal procedures for the fair treatment of a person of concern carried out in accordance with established rules and principles of an organization and the law.
Economic Espionage	The covert practice of obtaining trade secrets from a foreign nation (e.g., all forms and types of financial, business, scientific, technical, economic, or engineering information; methods, techniques, processes, procedures, programs, or codes for manufacturing). Also referred to as commercial or industrial espionage.
Espionage	The practice of spying on a foreign government, organization, entity, or person to covertly or illicitly obtain confidential information for military, political, strategic, or financial advantage.
Expressions of Insider Threat	The various ways in which insider threats manifest. Includes: violence, espionage, sabotage, theft, and cyber expressions.
Financial Crime	A sub-category or theft involving the unauthorized taking or illicit use of a person's, business', or organization's money or property with the intent to benefit from it.
Fraud	Wrongful or criminal deception intended to result in financial or personal gain.
Government Espionage	The covert practice of intelligence gathering activities by one government against another to obtain political or military advantage. It can also include governments spying on corporate entities, such as aeronautics companies, consulting firms, think tanks, or munition companies. Also referred to as intelligence gathering.
Hub	A single, cataloged, searchable repository for the collection, integration, review, analysis, assessment, reporting, and storage of information.
Ideation	The formation of ideas or concepts.
Identify	To recognize concerning behaviors or establish as being a particular person or entity.
Incident Response Plan	A set of instructions for the response to suspected unintentional or intentional insider threat actions or concerning behaviors.

Infrastructure	The basic physical, virtual, and organizational structures (e.g., facilities, networks, power supplies) needed for the operation of a society or enterprise.
Insider	Any person who has (or had) authorized access to or knowledge of an organization's resources, to include personnel, facilities, information, equipment, networks, and systems.
Insider Incident	The occurrence of an insider threat action.
Insider Threat	The potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, facilities, and associated resources. See organizational definitions below:
	CERT National Insider Threat Center – The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.
	Department of Homeland Security (DHS) – The threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems. This threat can manifest as damage to the Department through the following insider behaviors: espionage; terrorism; unauthorized disclosure of information; corruption, to include participation in transnational organized crime; sabotage; workplace violence; and intentional or unintentional loss or degradation of departmental resources or capabilities.
	Department of Defense (DoD)/Center for the Development of Security Excellence (CDSE) – DoD Directive 5205.16: The threat that an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.
	Ernst & Young Global Limited (EY) – An insider threat is when a current or former employee, contractor, or business partner, who has or had authorized access to an organization's network systems, data or premises, uses that access to compromise the confidentiality, integrity, or availability of the organization's network systems, data, or premises, whether or not out of malicious intent. Insider threats can include fraud, theft of intellectual property (IP) or trade secrets, unauthorized trading, espionage, and IT infrastructure sabotage.
	National Insider Threat Task Force (NITTF) – The risk an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practice.

Insider Threat (cont.)	**RAND Corporation** – The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization or national security.
	The Computer Language Company Inc. – The potential risk that employees and officers of a company can cause more harm to the IT infrastructure or to the company in general than external threats such as viruses and cracker attacks. Also known as an "authorized user threat," disgruntled employees have easy access to confidential data, especially if their feelings are not made public.
Insider Threat Mitigation Guide	A guide to lessen the severity, seriousness, or consequences of the hazards from an insider threat.
Intellectual Property	A category of property that includes intangible creations of the human intellect, such as copyrights, patents, trademarks, and trade secrets.
Intellectual Property Theft	A sub-category of theft involving the theft or robbery of individuals or organizations of their ideas, inventions, and/or creative expressions, including trade secrets and proprietary products from individuals or organizations, even if the concepts or items being stolen originated from the thief.
Intentional Insider	A current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who misuses their access with malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.
Intervention	Action taken to prevent an incident or mitigate its impact.
Leakage	Accidental communication of sensitive information to a third party.
Manage	To direct inventions focused on the person of concern, the target, and the situation or setting.
Malicious	Intending or intended to do harm.
Mitigate	To make less severe, serious, or painful.
Multi-disciplinary Governance Group	A team of stakeholders or personnel from components or offices in an organization whose discipline places them in a position to receive and retain information pertinent to the background, conduct, and activities of trusted insiders; make decisions regarding the threat management programs procedures, policies, and standards; and make decisions for intervention strategies.
Physical Sabotage	Consists of deliberate actions aimed at harming an organization's physical infrastructure (e.g., facilities, equipment).
Person of Concern	Potential insider threat perpetrator who is under consideration by an insider threat management team.
Personal Private Information	Any data that could potentially be used to identify a person. Examples include a full name, Social Security number, driver's license number, bank account number, passport number, and email address.
Predisposition	A liability or tendency to suffer from a particular condition, hold a particular attitude, or act in a particular way.

Privacy Laws	Laws that protect the disclosure or misuse of information pertaining to a private individual.
Private Sector	The part of the national economy that is not under direct government control.
Respond	The action taken as a response to a person or activity.
Risk	Someone or something that presents a hazard that could cause the chance for loss or injury.
Sabotage	Deliberate actions aimed at harming an organization's physical or virtual infrastructure, including noncompliance with maintenance or IT procedures, contamination of clean spaces, physically damaging facilities, or deleting code to prevent regular operations.
Stakeholder	A person with an interest or concern in something.
Stressor	Contributing factors, such as family, financial, employment, or workplace difficulties, that can exacerbate predispositions and increase the risk of a potential insider threat taking hostile action.
Terrorism (Insider Threat)	The unlawful use of, or threat to use, force and violence by employees, members, or others closely associated with organizations, against those organizations to promote a political or social objective.
Theft	The act of stealing.
Third-Party Threat	A threat associated with contractors or vendors who are not formal members of an organization, but who have been granted some level of access to facilities, systems, networks, or people to complete their work.
Threat Assessment Process	The process of gathering and assessing information about individuals who may have the interest, motive, intention, and capability of causing harm to an organization or persons.
Threat Management	The process of enacting threat management strategies intended to reduce the risk posed by a person of concern to prevent insider threat incidents and protect the organization and its people.
Threat Management Team	A central convening body to identify possible insider threats by collecting warning signs, reports, insider threat indicators, and automated monitoring information to fuse into a picture of an individual's behavior for threat assessment and management actions.
Trusted Insider	An individual, employee, organizational member, contractor, or consultant who has been vetted by an organization.
Unintentional Insider Threat (Accidental)	A current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, accidentally and without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

Unintentional Insider Threat (Negligent)	A current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through negligence and without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.
Violence (Insider Threat)	Consists of any act of violence, threat of violence, or other threatening behavior that creates an intimidating, hostile, or abusive environment.
Virtual Sabotage	Consists of malicious actions using technical means to disrupt or cease an organization's normal business operations.
Whistleblower	A person who exposes secretive information or activity that is deemed illegal, unethical, or not correct within a private or public organization.
Workplace Violence	Any act or threat of physical violence, harassment, sexual harassment, intimidation, bullying, offensive jokes, or other threatening behavior by a coworker or associate that occurs at the work or organizational site.

Acronyms

ADA	Americans with Disability Act
ASIS	American Society for Industrial Security
BOLO	Be-on-the-Lookout
CDSE	Center for Development of Security Excellence
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPG	Comprehensive Preparedness Guide
CSO	Chief Security Officer
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DNS	Domain Name System
DOD	Department of Defense
EAP	Employee Assistance Programs
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FOID	Firearm Owners Identification
HR	Human Resources
INSA	Intelligence and National Security Alliance
IT	Information Technology
IRM	Incident Response Management
LEO	Law Enforcement Officer
NaBITA	National Behavioral Intervention Team Association
NCAVC	National Center for the Analysis of Violent Crime
NIST	National Institute of Standards and Technology
NITTF	National Insider Threat Task Force
OSHA	Occupational Safety and Health Administration
PAM	Privileged Access Management
ROI	Return on Investment
SEI	Software Engineering Institute
SIEM	Security Incident and Event Management
TOR	The Onion Router (software name)
TSA	Transportation Security Administration
UAM	User Activity Monitoring
UBA	User Behavior Analytics
USB	Universal Serial Bus
USSS	United States Secret Service
VPN	Virtual Private Network