



INSIDER THREAT MITIGATION GUIDE

SEPTEMBER 2026

Table of Contents

- About This Guide4
- 1 | Introduction5
 - The Financial Cost of Insider Threats 6
 - The Human Cost of Insider Threats 7
 - Insider Threat Mitigation Program 8
- 2 | Defining Insider Threats10
 - Definition of an Insider..... 11
 - Definition of an Insider Threat..... 11
 - Types of Insider Threats..... 12
 - Other Threats..... 13
 - Expressions of an Insider Threat..... 14
 - Progression of an Insider Threat Toward a Malicious Incident 17
 - Concluding Thoughts 21
 - Key Points21
- 3 | Building an Insider Threat Mitigation Program22
 - Characteristics of an Effective Insider Threat Mitigation Program 23
 - Core Principles 25
 - Keys for Success 28
 - Establishing an Insider Threat Mitigation Program..... 30
 - Plan 31
 - Organize and Equip..... 39
 - Train and Execute 50
 - Evaluate and Improve 53
 - Concluding Thoughts 56
 - Key Points56
- 4 | Detecting and Identifying Insider Threats57
 - Threat Detection and Identification 58
 - Threat Detectors..... 61
 - Threat Indicators 62
 - Concluding Thoughts 70
 - Key Points70

5 Assessing Insider Threats	71
Assessment Process	72
Violence Indicators in Threat Assessments.....	77
Awareness of Scrutiny.....	82
Use of a Behavioral Health Professional	82
Case Considerations for the Involvement of Law Enforcement	83
Concluding Thoughts	85
Key Points	85
6 Managing Insider Threats	86
Intervention Strategies	89
Domestic Violence Concerns.....	91
Mental Health as a Factor	93
Use of Law Enforcement in Threat Management.....	95
Involuntary Employee Separations.....	96
Monitoring and Closing a Case.....	98
Avoiding Common Pitfalls	99
Concluding Thoughts	100
Key Points	103
7 Conclusion.....	104
Appendix A Tools and Resources	106
Appendix B Terms and Acronyms.....	109



About This Guide

The recommended approaches and best practices described in the *Cybersecurity and Infrastructure Security Agency (CISA) Insider Threat Mitigation Guide* (hereafter referred to as the “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-government 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 does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products,

processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

CISA's publication of informational materials about this topic are intended for public awareness, and are not intended to restrict, diminish, or demean any person's right to hold, express, or publish any opinion or belief. This product describes activities and behaviors that may be suspicious or indicative of criminal activity. These activities may be constitutionally protected and should be reported only when there are articulable facts to support a rational conclusion that the activity or behavior is suspicious. Do not report based solely on protected activities or on the basis of race, ethnicity, religion, sex, sexual orientation, other individual characteristic, or a combination of only such factors.

1 | Introduction

Insider threats pose risks to critical infrastructure owners and operators of all types and sizes, from small public entities to Fortune 100 corporations, as well as to state, local, and federal government 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 can commit harmful acts across all infrastructure sectors. These disruptions can cause significant damage.

To combat harmful acts, critical infrastructure organizations should consider developing and implementing a proactive and prevention-focused insider threat mitigation program. This approach can help organizations 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 save lives.

This *Insider Threat Mitigation Guide* is designed to assist critical infrastructure owners and operators, related 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 threats and the many expressions those threats can take, and offers an integrated approach necessary to mitigate risk. **The *Guide* shares best practices and key points from across infrastructure communities to assist organizations in overcoming common challenges and 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, and, as such, 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.

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

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 to use in 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 coworkers

The Financial Cost of Insider Threats

Although difficult to quantify, insider threats present a complex and rapidly evolving set of challenges that organizations cannot afford to ignore. Annual losses are hard to quantify due to significant underreporting of insider threat incidents.¹ Still, the estimated annualized cost of insider threat incidents rose from approximately **\$16.2 to \$17.4 million**. Losses may result from physical

damage to infrastructure, disruption of productivity, intellectual property theft, leakage of sensitive data, or damage to an organization's reputation. Each of these may contribute to a loss of competitive advantage.

Figure 1 provides a high-level overview of the financial cost of insider threats.

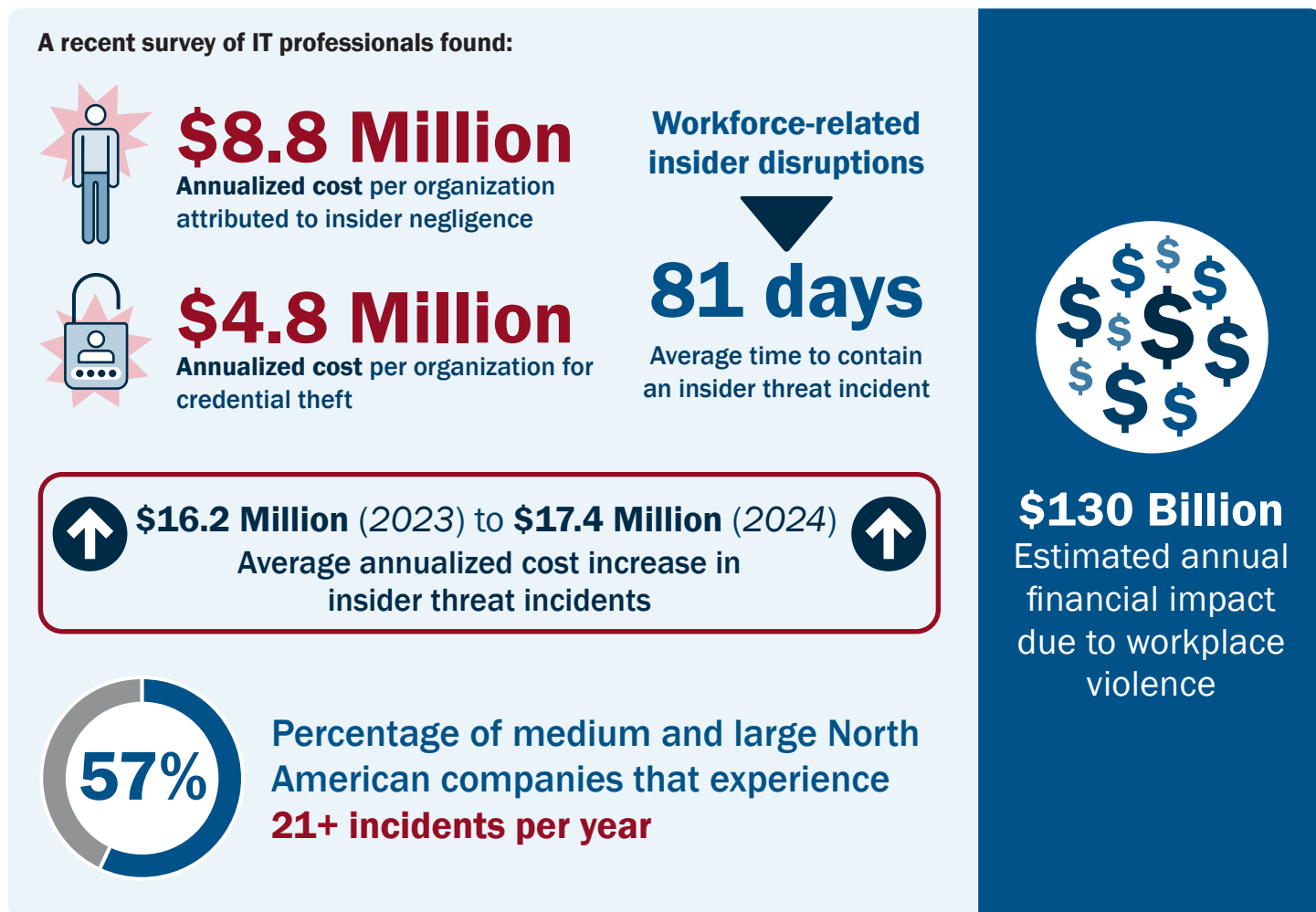


Figure 1. The Financial Costs of Insider Threats²

¹ "Protect Your Organization from the Insider Out: Government Best Practices," National Insider Threat Task Force (NITTF), 2016, accessed November 4, 2025, available at www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf, 3.

² "Cost of Insider Risks," Ponemon Institute, 2025, accessed October 9, 2025, available at ponemon.dtexsystems.com, 4, 6, 8, and 9; "Workplace Violence Statistics 2018: A Growing Problem," AlertFind, 2018, accessed October 9, 2025, available at alertfind.com/workplace-violence-statistics/; and "Reshaping the Cybersecurity Landscape," Deloitte Insights, 2020, accessed October 9, 2025, available at www.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html.

The Human Cost of Insider Threats

Some insider threats, particularly those involving acts of workplace violence, can have a direct and tragic impact on the lives and wellbeing of employees at an organization, as well as their families. In the United States, data has shown an upward and unabated trend in acts of workplace violence over recent years.³ Acts of workplace violence can occur not just between an insider and their colleagues, but also between an insider and an organization's clients, visitors, or others in the

vicinity when the attack occurs. As with any violent incident, those who are witness to an insider attack which results in physical harm or loss of life can suffer lasting trauma, even if they are not physically hurt in the attack. This potential impact, in both lives lost and lives permanently changed, is the human cost of insider threats. *Figure 2* provides an important overview of the human cost of insider threat.



Figure 2. Human Cost of Insider Threat⁴

³ "Table 2: Fatal Occupational Injuries for Selected Events or Exposures, 2018-22," U.S. Bureau of Labor Statistics (BLS), 2023, accessed October 9, 2025, available at www.bls.gov/news.release/archives/cfoi_12192023.htm.

⁴ "Fatal Occupational Injuries," BLS; "Table R4. Number of nonfatal occupational injuries and illnesses involving days away from work by industry and selected events or exposures leading to injury or illness, private industry, 2020," BLS 2021, accessed November 5, 2025, available at www.bls.gov/iif/nonfatal-injuries-and-illnesses-tables/case-and-demographic-characteristics-table-r4-2020.htm; "Assault at Work," National Safety Council (NSC), 2021, accessed October 9, 2025, available at injuryfacts.nsc.org/work/safety-topics/assault/; and "With Workplace Violence on the Rise, 1 out of 7 People Don't Feel Safe at Work," Society for Human Resource Management (SHRM), 2019, accessed November 5, 2025, accessible at www.shrm.org/about/press-room/workplace-violence-rise-1-7-people-dont-feel-safe-work.

Insider Threat Mitigation Program

An effective insider threat mitigation program spans the entire organization and is designed to support and empower employees, not to serve as an enforcement or policing mechanism. A strong insider threat program should promote behavior with training and awareness, clear policies and procedures, and management practices that encourage employees to act in the best interests 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 act through appropriate management or enforcement actions. It is important for organizations to balance focus, policy, processes, and cost, as some mitigation measures are

cost prohibitive and projected cost savings may be a significant determinant of an insider threat mitigation program's return on investment (ROI). It remains critical for organizations to invest wisely in insider threat mitigation, as both physical and cybersecurity incidents, including those generated by insiders, can result in substantial financial losses. In a recent study of small businesses that suffered cyber incidents, 42 percent reported revenue losses, while another 32 percent saw loss of customer trust and increased employee turnover. Investing in a robust insider threat mitigation program prior to a potential incident can generate significant potential savings not just in revenue, but in the safety and well-being of employees.⁵

Effective Insider Threat Mitigation Programs...



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



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



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



Leverage multidisciplinary 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.



Establish a protective and supportive culture, protect civil liberties, maintain confidentiality, and provide safe environments where individuals who might pose a threat are identified.

⁵ "2023 Business Impact Report," Identity Theft Resource Center (IRTC), 2023, accessed October 10, 2025, available at www.idtheftcenter.org/publication/itrc-2023-business-impact-report/, 9.

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 to be used 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 that has full support from senior leadership 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 an individual is the first line of defense in protecting the organization

2 | Defining Insider Threats

Insider threats exist because it is nearly impossible to predict the future negative actions, wittingly or unwittingly, of trusted insiders. Organizations rely on insiders to perform every function—from the most basic to the most sensitive.

The basic disposition of an insider threat may be similar for many organizations: a trusted individual who uses their access and knowledge to harm an organization. But the 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 a 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 relevant terms. While not inclusive of every potential insider incident, definitions provide a common vocabulary and understanding to help frame the discussion of insider threats, 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 how to identify 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 types of insider threats
- » The definition of an insider threat
- » How insider threats can occur 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. An insider may be:



A person the organization trusts and to whom the organization has provided sensitive information and access. This can include both full and part-time employees, contractors, and external third parties who still have some level of access



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



A person with regular or intermittent access to facilities and/or networks



A person who is knowledgeable about the organization's fundamentals, including pricing, costs, and its strengths and weaknesses, and/or the organization's business strategy and goals

Definition of an 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, negligent, or unintentional acts that negatively affect the confidentiality, integrity, and availability of the organization, its data, personnel, facilities, and/or associated resources.

Many organizations have adapted this 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). Some use the types of assets to which insiders have access (e.g., information technology, facilities, or data). Another approach uses the types of harm they could inflict on an organization (e.g., fraud, theft, sabotage, or violence). The approach or definition that works for one organization may not necessarily work for another.

A best practice is for an organization to **define the insider threat in a way that addresses the unique nature of its operating environment, its values, or the resources determined to be most at risk**. The threat landscape will evolve and the specific needs and priorities of the organization will change, so an organization may need to expand or refine its definition over time.

Types of Insider Threats

Insider threats originate from two primary kinds of activity: unintentional and intentional.

Unintentional

A majority of recent insider threats are unintentional and negligent in nature, caused by mistakes on the part of employees or employees ignoring established organizational security protocols. Although more common, unintentional insider threats are on average financially less costly to organizations than malicious, intentional threats. *Figure 3* provides examples of the different types of insider threats. Unintentional actions can be further broken down into negligent and accidental acts.

Negligent

Insiders can expose an organization to a threat through carelessness. Insiders of this type are generally familiar with security and/or IT policies but fail to comply with them, creating risks 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 typically passive or careless in their disregard for the rules; however, these are behaviors that can be changed, particularly with greater awareness and a sense of urgency around the topic.

Accidental

Even the best employee can be oblivious or naive and **make a mistake that causes 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, opening an attachment that contains a virus within a phishing email, or improperly disposing of sensitive documents. No organization can prevent every possible accident, but they can mitigate the harm from those that do occur.

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 a dangerous environment within the workplace. They may even think they are acting in the best interest of the public. For example, unmet expectations due to lack 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. Beyond motivations related to personal gain or financial benefit, some insiders may commit intentional harmful acts driven by ideological objectives, believing their damaging actions serve a significant, larger goal.⁶

⁶ “Insider Threat Indicators: Job Aid,” Center for Development of Security Excellence (CDSE), 2021, accessed October 10, 2025, www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf, 11.

Examples of Unintentional Incidents		Examples of Intentional Incidents	Shared Characteristics
Accidental • Misplacing or losing a portable storage device containing sensitive information • 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	Negligent • Allowing someone to “piggyback” through a secure entrance • Ignoring messages to install new updates and security patches • Leaving items, such as laptops or mobile phones, unattended and unlocked • Improperly disposing of sensitive documents	• Deliberate actions aimed at harming an organization’s facilities, equipment, or technical assets • Unauthorized disclosure of information • Planting malware on internal systems • Selling sensitive information to the highest bidder • Conducting espionage for a foreign entity or business competitor • Workplace violence	• Harms the organization • Costly • May Physically Harm People • Damage to Reputation • Damage to Infrastructure • Intellectual Property Theft • Loss of Privacy Information

Figure 3. Unintentional vs. Intentional Incidents

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, commit intellectual property theft, leave a door unlocked, 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 personnel to complete their work. This threat sub-type can also extend to multiple third-party threats. 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 an Insider Threat

Insider threats can manifest in several different ways, including violence, espionage, sabotage, theft, and cyber, and can be committed intentionally or unintentionally. *Figure 4* defines these areas.

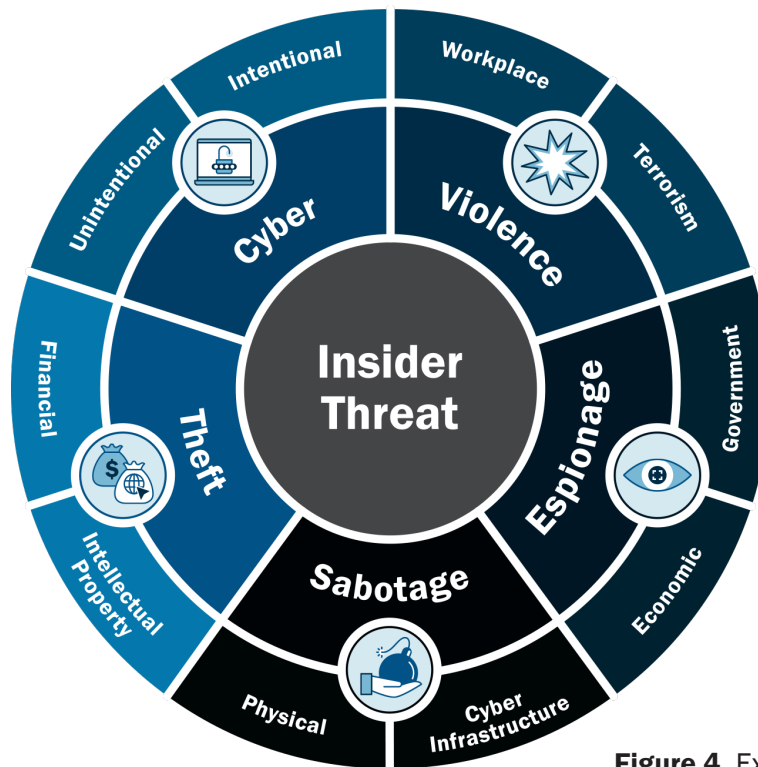


Figure 4. Expressions of Insider Threats



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 threats that precede a physical attack that damages infrastructure, or threatens or harms the health and/or safety of an individual or group, resulting in an unsafe work 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 and hostile behavior by a coworker or associate that occurs in a person's place of employment or while a person is working.

Terrorism

Terrorism is a premeditated threat or act of violence against people, property, environmental, or economic targets, to induce fear or to intimidate, coerce, or affect a government, the civilian population, or any segment thereof in furtherance of political, social, ideological, or religious objectives. In the context of insider threats, terrorism may involve insiders using their knowledge of an organization's security procedures, facility layout, and other internal information to execute or threaten to execute a terrorist attack.⁷

⁷ "DHS Lexicon," U.S. Department of Homeland Security, last modified June 8, 2022, accessed November 14, 2025, available at www.dhs.gov/publication/dhs-lexicon.



Espionage

Espionage is the practice of spying on behalf of a foreign government, organization, entity, or person to covertly or illicitly obtain confidential information for military, political, strategic, or financial advantage. Due to their trusted access and knowledge of an organization, insiders are uniquely positioned to more effectively carry out espionage.

Economic Espionage

Economic espionage involves the covert practice of obtaining trade secrets (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) and providing these secrets to an outside party without authorization. This is 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 a political or military advantage. It can also include government(s) spying on corporate entities such as aeronautics, consulting firms, think tanks, or munition companies. This is also referred to as intelligence gathering.



Sabotage

Sabotage involves deliberate actions aimed at harming an organization's physical or cyber infrastructure, including noncompliance with maintenance or IT procedures, contamination of clean spaces, physically damaging facilities, or deleting code to prevent regular operations. Due to their physical and digital access to an organization's assets, insiders can carry out especially damaging acts of sabotage.

Physical Sabotage

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

Cyber Infrastructure Sabotage

Cyber infrastructure sabotage consists of malicious actions using organization networks to disrupt, halt, or damage an organization's operations, processes, or assets.





Theft

Theft includes multiple subcategories of stealing. The two subcategories most perpetrated by insiders involve finance and intellectual property. Financial gain is a common motive, made 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's, or organization's money or property with the intent to benefit or profit 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).⁸

Intellectual Property

Intellectual property theft is the robbery of an individual's or organization's ideas, inventions, and/or creative expressions. This includes trade secrets and proprietary products from individuals or organizations, even if the concepts or items being stolen originated from the thief.



Cyber

Malicious cyber activity can include theft, espionage, violence, and sabotage, dealing with anything related to technology, virtual reality, computers, devices, or the internet. These illicit activities are undertaken using a variety of vectors including 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 (often 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 the unsuspecting person being taken in by phishing emails, rogue software, or 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, access 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.

⁸ "Fraud and Financial Crimes," FindLaw, last modified November 4, 2023, accessed October 10, 2025, available at criminal.findlaw.com/criminal-charges/fraud-financial-crimes.html.

Progression of an Insider Threat Toward a Malicious Incident

While everyone experiences stressful events, the vast majority do not resort to disruptive or destructive acts. For those insiders that do turn to intentional malicious activity, the acts are rarely spontaneous; instead, they are usually the result of a deliberate decision to act.

Not all insider threats are violent or malicious. However, if an individual begins to exhibit escalating or dangerous behavior, their personal predispositions and background, which may make them susceptible to committing a malicious act, can interact with their personal stressors and send them on a path toward a malicious incident.

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.⁹

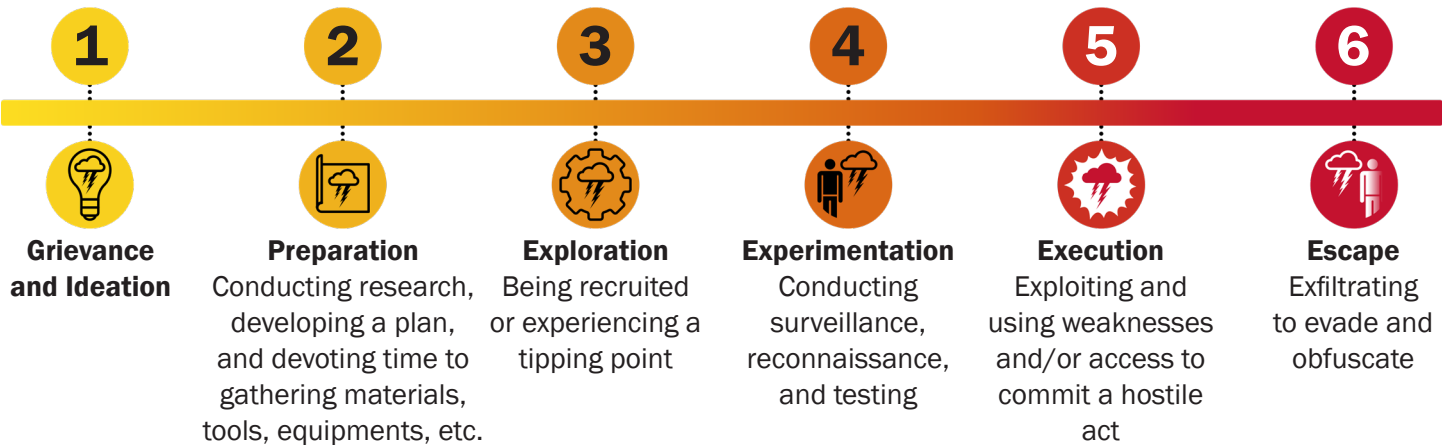


Figure 5. Progression of an Insider Toward a Malicious Incident¹⁰

As illustrated by *Figure 5*, the sequence of escalating behaviors can often be observed and monitored by colleagues and other contacts. It is important to note that the mere exhibition of insider threat behaviors does not guarantee that an individual will commit a malicious act. Likewise, an insider may not follow each step on the path exactly in the order as written. They may skip certain steps or spend varying amounts of time on each. Organizations should not wait for an insider to have progressed through multiple steps on this pathway before deciding to intervene.

However, the farther an individual moves down the pathway, the more likely they are 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 should be closely observed and the risk of violence assessed as their tenure comes to an end. Refer to CISA's Interagency Security Committee (ISC) Guide: [Managing Risk of Adverse/Involuntary Employee Separations](#) for additional information on offboarding employees.

9 "Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks," U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI), 2015, accessed October 10, 2025, www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view, 24.

10 Adapted from "Making Prevention a Reality," FBI, 24.

1 Grievance and Ideation

The first step on the pathway to becoming an insider threat 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. It could also 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 slights.

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 using malware, 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. 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. It is also important to note the distinction between those who may harmlessly vent to coworkers about their workplace complaints and those who intend to cause harm.

3 Exploration

Before this stage, the individual may be uncommitted, wavering between action or acquiescence. However, at this stage something happens to cause the individual to commit to acting—a triggering point. This could be an additional stressor such as 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 individual 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 or 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 them.

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 individual remains in place.

When an Insider Becomes an Insider Threat

The case that follows demonstrates how a trusted employee used their authorized access or knowledge to cause harm, resulting in an insider threat. It outlines several indicators of the often-observable progression from trusted insider to an 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 with 40 years of cleared defense sector experience had access to controlled engineering functions and upgrade plans for the American fighter aircraft. He worked for multiple defense companies and had raised internal alarms repeatedly over insider threat risk. He held clearances ranging from Secret to TS/SCI.

Indicators

Stressors

- *Possible financial:* The engineer spoke with an undercover agent about financial compensation.
- *Disillusionment with the United States:* The engineer wanted sanctuary in foreign nation.

Personal Predispositions

- *Idealization with foreign nations:* The engineer repeatedly expressed interest in a foreign citizenship.

Concerning Behaviors

- In 2017, the engineer “revealed information regarding U.S. military fighter jets...to a woman he thought might be a spy.”
- In 2018, the engineer brought a USB drive into a classified workspace and inquired about holding a foreign and American security clearance simultaneously.

The Malicious Act Of Espionage

The engineer made concerning statements over a three-year period about switching sides and working for a foreign government. He worked on “matters relating to U.S. Air Force aerospace technology” and committed numerous security violations during his four-decade career. He was identified as an insider threat by one employer but left before any corrective measures could be taken. After attempting to bring an unauthorized device into a classified space at his next job, he was

fired. Based on that conduct, the Federal Bureau of Investigation (FBI) initiated an undercover operation to determine whether the engineer would provide classified information to foreign agents. The engineer met with an undercover FBI employee posing as a foreign agent and exchanged hundreds of emails over eight months “discussing his knowledge of classified information” and “national defense information classified as SECRET.”

How It Was Disrupted

The facility security officer (FSO) at his company, following the 2017 social media postings, assessed the engineer to be an insider threat in a report to the Defense Counterintelligence and Security Agency (DCSA). However, the engineer left that company and the FSO was unable to follow up with him. At his next job in 2018 the company’s information security officer

(ISO) questioned him after he attempted to bring a USB into a classified workspace. He was eventually fired from his role. Following an FBI sting operation, he was arrested and charged with attempting to communicate national defense information to aid a foreign government, a crime with a penalty of up to life 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 trusted relationship.

This chapter helps to demonstrate the breadth of the challenge organizations face and the varying types and expressions of an insider threat. It includes those

with a specific intent to do harm. It also helps to illuminate the challenges presented by those who may be unwitting or unintentional insiders who, through acts of negligence or through manipulation, cause harm to the organization.

The examples provided 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 investment choices.

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 their 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 trusted relationship with their victim and act in a way that is outside the expectations of that trusted relationship.
- » Organizations should tailor their approach to the insider threats to address the unique nature of their operating environment and priorities.
- » Insider threats can be either intentional or 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 without the intent to harm an organization.

3 | Building an Insider Threat Mitigation Program

The people within an organization are simultaneously the strongest elements of its security program and its greatest vulnerability. Organizations cannot function without having trusted access to assets, data, and intellectual property, which inherently creates risks to the organization. The disruptive impacts of insider-related incidents jeopardize safety, undermine value, and degrade operations.

Organizations have increasingly recognized the importance of insider threat mitigation programs in response to these threats. A recent survey shows that concern over malicious insider attacks among cybersecurity professionals rose from 60 percent in 2019 to 74 percent in 2024. Despite this, only 29 percent of those polled feel adequately equipped to protect against insider threats, highlighting a need for further investment and efforts in this area.¹¹

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
- » Aid 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

11 “2024 Insider Threat Report: Trends, Challenges, and Solutions,” Securonix, 2024, accessed October 10, 2025, available at www.securonix.com/resources/2024-insider-threat-report/, 2.

Characteristics of an Effective Insider Threat Mitigation Program

Successful insider threat mitigation programs limit or monitor access across organizational functions. Consequently, they limit the damage an insider can do, whether the act is intentional or unintentional.

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.

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 already have people and teams with program objectives that address functions related to an insider threat mitigation program. Existing workplace harassment and violence policies and cybersecurity programs can serve as productive starting points. Leveraging those resources can help reduce costs and the level of effort required.

An Effective Insider Threat Mitigation Program...

- » **Identifies and focuses on the critical assets, data, and services** that the organization defines as valuable
- » **Assesses threats** to determine the individual level of risk
- » **Manages the entire range of insider threats**, including implementing strategies focused on the individual, 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 the threat

The Case for an Insider Threat Mitigation Program

What Happened

During the night shift, 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 deactivated 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. While it is important to note that stress and mental health issues alone are not indicative of a subject being an insider threat, when these concerns are raised by an individual they should be taken seriously and handled with care. In this case, the employee had previously engaged the human resources (HR) department on several occasions about his health

concerns and requested removal from the night shift. Again, mental health and stress issues by themselves are not indicative of insider threat behavior, but can play a role when a person’s baseline behavior changes or when their concerns or requests for help are dismissed. 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 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 that 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 empathetic to

individual circumstances. To enable 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 6* exemplifies, successful programs focus on helping members of an organization to deter and prevent an insider incident rather than only seeking to punish or discipline an individual following a negligent or intentional act.



Figure 6. A Protective Culture Supports a Successful Insider Threat Mitigation Program

3. Building an Insider Threat Mitigation Program

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

- » The behaviors expected from members to keep themselves and organizational assets safe and secure
- » Definitions of how these behaviors differ depending on the role or responsibilities of an individual, group, or contractor in the organization
- » The behaviors expected from partners or suppliers when handling or accessing organizational information or equipment to protect them from compromise¹²

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 Assets 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. Organizations must strike a balance between the need to protect assets and the need for transparency on monitoring policies and privacy expectations.

Insider threat programs raise 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 others. Involving legal counsel and potentially external law enforcement partners, is highly encouraged when an organization is conducting its preliminary investigation and determination into a potential insider threat. Organizations need to balance the responsibility of following up on concerning indicators of potential insider threats without jumping to conclusions, or determining an individual to be a threat before a proper investigation can be conducted.

Individuals who are determined to be a legitimate insider threat also have rights which they are guaranteed under the law. Involving legal counsel, and potentially external law enforcement partners, is highly encouraged when an organization is conducting its preliminary investigation and determination into a potential insider threat.

In some cases, an improper organizational response may provide a triggering event, transforming a potential insider threat into an actual one.¹³

“Public trust will hinge on the justified assurance that government, academic, and industry use of Privacy-Preserving Data Sharing and Analytics (PPDSA) solutions will respect privacy, civil liberties, and civil rights. The future PPDSA ecosystem must be transparent and inclusive and reflect privacy principles and preferences (e.g., individual participation and consent management). Achieving these outcomes will require developing systems informed by ethical, social, behavioral, and economic factors as well as human-centered design principles.”

*2023 National Strategy to Advance Privacy-Preserving Data Sharing and Analytics*¹⁴

12 “Identifying Security Behaviors,” United Kingdom National Protective Security Authority (NPSA), last modified February 23, 2023, accessed October 10, 2025, available at www.cpni.gov.uk/identifying-security-behaviours.

13 E. Shaw and L. Sellers, “Application of the Critical-Path-Method to Evaluate Insider Risks. Internal Security and Counterintelligence,” *Studies in Intelligence* 59, no. 2 (2015): 1-8, here 5, available at www.cia.gov/resources/csi/studies-in-intelligence/volume-59-no-2/application-of-the-critical-path-method-to-evaluate-insider-risks/.

14 “National Strategy to Advance Privacy-Preserving Data Sharing and Analytics,” National Science and Technology Council (NSTC), 2023, accessed October 10, 2025, available at www.privacysecurityacademy.com/wp-content/uploads/2023/11/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf, 9.

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.¹⁵ 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:



Continuously improving from best practices and lessons learned from the broader insider threat management community.



Actively maintaining a dynamic threat risk registry with regular risk assessments and risk ratings informing a more current and accurate risk picture. This 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 insider threat reference and advisory material, allowing the collective experience of others to inform program improvements (often publicly available).¹⁶

¹⁵ “Insider Threat Program Maturity Framework,” NITTF, 2018, accessed October 10, 2025, available at www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf, iii and 12.

¹⁶ “NCSC Awareness Materials,” Office of the Director of National Intelligence, 2026, accessed July 6, 2026, available at <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials>.

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 safety and security, 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. 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 organizational policies and protections, or other negligent activities.



Establish the Proven Operational Approach of Detect and Identify, Assess and Manage

Best practices for insider threat mitigation use an operational approach that aligns with existing security programs to enable detection and identification of a potential threat, assessment of that threat, and then employs both active and passive techniques to manage the threat. All three practices are necessary to proactively mitigate the insider threat. This approach is best executed by a multidisciplinary team from across an organization, with organizational leaders, human resources, information technology, legal counsel, security, and other personnel supporting the effort to detect and identify, assess, and manage threats. Those solutions will also employ a range of proactive and protective measures focused on reducing the risk from the individual, protecting potential victims or assets, or improving the overall protective posture of the organization. Smaller organizations or those with nascent insider threat programs can leverage existing functions to support this activity.



Identify the Organization's Assets and Prioritize Risks

Understanding what an organization values and what could damage or disrupt those assets is essential for an effective insider threat mitigation program. A proven approach begins with determining the organization's resources, where those 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 to allow for the proper alignment and management of potential risks.

3. Building an Insider Threat Mitigation Program

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 the following 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 multidisciplinary, and because they intersect with numerous business functions, they require executive level sponsorship and commitment.

In some cases, 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.

There are some recognized best practices, concepts, tools, and processes for establishing such a program. The National Insider Threat Task Force (NITTF) created a list of guidelines for federal agencies and departments to develop insider threat management programs.¹⁷ This guidance provides a sound starting point for all public and private sector organizations to consider when developing a new program, implementing a more fully functioning program, or measuring the maturity of an existing program.

The National Insider Threat Task Force (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:

Plan 	Organize & Equip 	Train & Execute 	Evaluate & Improve 
a) Secure executive engagement b) Determine where to house the program c) Determine program ownership d) Establish a multi-disciplinary governance group e) Establish guiding principles f) Artificial intelligence considerations g) Address legal obligations h) Identify high-value assets	a) Integrate information, analysis, and response b) Develop an incident response plan c) Establish reporting pathways d) Employ technology and tools to identify concerning behaviors e) Establish a risk rubric and threat assessment methodology f) Establish a multidisciplinary threat management team	a) Market the program b) Encourage a culture of safety, awareness, and support c) Implement a formal training and awareness program	a) Conduct exercises b) Provide oversight and compliance, including internal audits¹⁸

17 "Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum and Change to Standards," National Insider Threat Task Force (NITTF), 2017, accessed October 10, 2025, available at www.dni.gov/index.php/ncsc-how-we-work/ncsc-nitff.

18 "Insider Threat Guide: A Compendium," NITTF.4

Plan



a) Secure Executive Engagement

Insider threat programs are more likely to succeed when they receive support from senior leadership and executives. 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.

b) Determine the Best Fit

Evaluate your organization to determine where the program should be housed. 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. 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.

c) 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 organization's 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 Mitigation Program. The Senior Official must have the ability to bring together multiple organizational activities. They will be a visible symbol for the program and will serve as a program advocate.

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. They will also be responsible for building an Insider Threat Incident Response Plan, which describes the processes for making insider threat case assessments and interventions.

Senior Official Best Practices

- ➔ Singular accountability for management and oversight
- ➔ Primary facilitator and negotiator to integrate effort
- ➔ Primary advocate to ensure policies and procedures are complied with and promoted
- ➔ Company/organization leadership is visible and frequently advocates for Senior Official and the program
- ➔ Senior Official is natural fit, such as Chief Security Officer (CSO), Chief Information Security Officer (CISO), or similar officer

Figure 7. Senior Official Best Practices



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

Duties for the Senior Official could include:

- Establishing program policies, procedures, practices, and processes to gather, integrate, and centrally analyze information
- Publishing an Insider Threat Incident Response Plan
- Ensuring the program protects privacy, rights, 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
- Establish a training plan for insider threat awareness for employees

See Figure 7 on the previous page for additional Senior Official best practices

d) Establish a Multidisciplinary Governance Group

The governance multidisciplinary group will establish the overarching policies and frameworks in which the insider threat program will operate. It is responsible for reviewing the organization's existing policies, standards, procedures, and environment for threat program compliance. 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 Health
- Equal Opportunity
- Enterprise Risk Management
- Public Information Officers

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 groups 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. It should also 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 Insider Threat Incident Response Plan.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

e) Establish Guiding Principles

Organizations should identify principles that will guide the development of its program and ensure that they match the threats the organization faces, as well as fit within the organization's structure, function, and culture. These principles should express the function of the insider threat program in the organization, align to how the program describes its purpose, goals, and objectives, and how the threat management team will operate. *Figure 8* 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.

Sample Guiding Principles: One Company's Approach



- Protecting employee privacy
- Protecting intellectual property to support company's growth, innovation and market differentiation
- Gaining confidence in data before adding new elements – start small with accessible and controllable data
- Looking for behavior, not people - identification, management and mitigation of anomalous behavior and activities is the goal
- Ensuring employee communication on the purpose of the insider threat program
- Maintaining management responsibilities to address employee challenges or issues

Figure 8. Sample Guiding Principles

– Emphasize Protection Over Punishment

Insider threat management frequently involves approaches that constrain users, monitor behavior, and detect and punish misbehavior.¹⁹

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 coworkers. Instead of solely focusing on making sure employees do not misbehave, positive incentives support a culture of collaborative, shared accountability, in which employees are motivated to contribute to the organization in positive ways.

Positive incentives can deter insider misbehavior from the beginning 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.²⁰

As such, successful insider threat mitigation programs employ a balance of positive incentives and preventative measures, which promote employee satisfaction and performance, avoid overly aggressive reactions following notification of a threat.

When communicating with employees or organizational members, emphasize the organization's concern for its members' well-being, and that individuals should report insider threats not only for the benefit of other employees or members of the company or organization, but for the potential threat actor, as well.

19 A. P. Moore, S. J. Perl, J. Cowley, M. L. Collins, T. Cassidy, et al., *The Critical Role of Positive Incentives for Reducing Insider Threats*, CMU/SEI-2016-TF-014 (Pittsburgh, PA: Software Engineering Institute (SEI), Carnegie Mellon University (CMU), 2016), doi.org/10.1184/R1/6585104.v1, available at insights.sei.cmu.edu/library/the-critical-role-of-positive-incentives-for-reducing-insider-threats/, 1.

20 Moore et al., "The Critical Role of Positive Incentives for Reducing Insider Threats," SEI-CMU, 5.

3. Building an Insider Threat Mitigation Program



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

Emphasize the need to prevent harm to people and the organization before it occurs, and educate the workforce or membership about the potential consequences of insider threats.

A key element to protecting the workforce is to clearly communicate the cascading effects an insider can inflict, 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

Organizations need to ensure that they establish policies and procedures that are appropriate for their culture, mission, and locality, as well as conform with state and federal regulations and statutes.

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

- How does the organization define its violence prevention and insider threat responsibilities?
- What responsibilities in these areas does the organization intend to have, and what does it currently have?
- 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 steps should be taken when a potential insider threat is made known to the organization?
- Who will carry out the violence prevention and insider threat capabilities?
- 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?
- How will the organization handle media and social media reporting?

– Do Not Reinvent the Wheel

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.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

– Stay Connected to Current Events

An important part of a robust insider threat mitigation program is the ability to be flexible, dynamic, and responsive to environmental factors and current events of varied scales. Geopolitical upheaval, changing economic conditions and shifts in workplace culture and expectations can all have impacts on an organization's workforce and insider threat mitigation program. Leadership should consider how these external factors might impact their organization's insider threat program, just as they would consider the impact on other parts of their organization.

– Consider Hybrid and Remote Work

Hybrid and remote work, which involve employees performing their work duties from their homes or other worksites away from a main office, has become an increasing trend across many sectors in recent years. There are a number of factors related to insider threat mitigation that organizations may need to consider when offering remote work or hybrid work arrangements to their employees.

These considerations can include the physical security of organizational documents and equipment (including IT equipment), the security of internet connections that an employee is using outside of the office, and the extra storage of digital information that may occur (such as on shared drives and server files). There are a number of options that organizations can take which allow them to offer remote/hybrid work flexibility to their organizations, without taking on additional insider threat risk.

These include updating organizational security standards, operating procedures, and specialized training for employees to address insider threat mitigation in a remote work environment. In addition, organizations may want to consider an assessment of information technology standards and network security expectations for employees using home internet connections to conduct work.

Organizations should also strive to ensure that employees working from home or locations outside the office continue to be engaged regularly by their colleagues, managers and others, both to encourage effective collaboration and completion of work as well as to detect any potential indicators of possible insider threat risk in those employees who do not have daily face-to-face interaction with their colleagues.

Organizations that offer flexible hybrid and remote work capabilities to their workforce, while integrating insider threat mitigation strategies into those capabilities, can simultaneously achieve high levels of employee satisfaction without sacrificing organizational security or resilience to insider threats.²¹

– 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 reporting of misconduct or unusual behavior because coworkers or associate members fear that a report could cost the individual their position or job, or they may fear retribution from the potential threat actor themselves.

21 "Managing Insider Threats in a Remote Work Environment: Lessons Learned from the Pandemic," Intelligence and National Security Alliance (INSA), 2021, accessed October 10, 2025, available at www.insaonline.org/detail-pages/news/2021/09/16/new-paper-addresses-insider-threat-and-remote-work-12513.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

– 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. A pre-established 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 include the following questions to enhance threat management capabilities:

- What is the standard response to reports of observable warning notifications from security systems or unusual or prohibited behaviors?
- 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 or contracts with third-party vendors, can local law enforcement serve as a resource?
- Will the department or agency take part as an ad hoc member of an interdisciplinary threat management team?
- What are the local weapons possession or acquisition procedures and laws?
- What are the local stalking and harassment laws and requirements?
- 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?
- Can the organization implement training programs with local law enforcement to practice incident response plans?

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.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

f) Artificial Intelligence and Insider Threat Mitigation Considerations

As organizations increasingly grow reliant on artificial intelligence (AI) for innovation, they must also mitigate risks to their AI systems. Malicious actors, which can include insiders within the organization as well as external threat actors seeking to manipulate insiders, may seek to carry out attacks against the AI systems using both cybersecurity and adversarial artificial intelligence (AAI) techniques.²² Because insider threats can make it easier for external attackers to carry out their nefarious objectives, data security is paramount in the development and deployment of AI systems.²³ Throughout the lifecycle of data in AI systems, the data acquirer must secure it against insider threat activity to prevent unauthorized access and modification.²⁴

Insiders with privileged access to sensitive data and the ability to bypass external security controls can attack the integrity of AI systems.²⁵ For example, insiders with access to internal data stores can deliberately inject misleading data into machine learning (ML) models during the training process (i.e., data poisoning) to alter predictions, resulting in incorrect or biased outputs.²⁶ Insiders can also alter the model's parameters (i.e. model tampering) after deployment to favor fraudulent transactions or misclassify sensitive documents.²⁷

Insiders with knowledge of an organization's AI systems also pose a heightened risk to organizations because they may have insights into vulnerabilities that can be exploited using AAI techniques. Even without malicious intentions, insiders may compromise sensitive data through their actions. For example, insiders may unwittingly compromise the security of sensitive organizational information by entering it into an AI system that is not accredited

or approved to handle or store such information. External threat actors may also use AI to assist in conducting an attack against an organization through the manipulation or deception of insiders. For example, external actors can deceive insiders through social engineering attacks using AI-generated phishing messages, user profiles, and video, image, or audio deepfakes.

– Insider Threat Mitigation Best Practices and AI

Mitigating insider threats requires adaptive and resilient practices to address the dynamic and continuously changing AI landscape. It is essential to stay informed about best practices in data security by consulting the latest cybersecurity recommendations.²⁸

Organizations should train employees on AI usage, secure their existing AI tools, and classify sensitive data. Existing legal safeguards, such as user agreements to prevent misuse of information systems, should be reviewed and updated as necessary. The insider threat mitigation best practices detailed in this *Guide* should also be integrated with any organizational initiatives that include AI.

As with other security matters, it is crucial for organizations to tailor and adjust their security measures regarding AI and insider threats based on their unique organizational culture, threat landscape, and risk tolerance. By factoring in AI considerations when developing their insider threat mitigation strategies, organizations can lower the risk of an AI-related insider attack or unintentional incident.

22 V. Beal, "Adversarial Attack: What is Adversarial Attack?," *Techopedia*, last modified December 28, 2024, accessed October 10, 2025, available at www.techopedia.com/definition/adversarial-attack.

23 "AI Data Security: Best Practices for Securing Data Used to Train and Operate AI Systems," Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australia, the United Kingdom, and New Zealand, 2025, accessed October 10, 2025, available at www.cisa.gov/resources-tools/resources/ai-data-security-best-practices-securing-data-used-train-operate-ai-systems, 2.

24 "AI Data Security," CISA et al., 9.

25 "Artificial Intelligence and the Insider Threat," Center for Development of Security Excellence (CDSE), 2025, accessed October 10, 2025, www.cdse.edu/Portals/124/Documents/jobaids/insider/Artificial-Intelligence-and-the-Insider-Threat.pdf, 6.

26 "Engaging with Artificial Intelligence (AI)," Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and CISA, 2024, accessed October 10, 2025, available at www.cyber.gov.au/resources-business-and-government/governance-and-user-education/artificial-intelligence/engaging-with-artificial-intelligence.

27 "Artificial Intelligence and the Insider Threat," CDSE, 3.

28 "AI Data Security," CISA et al.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

g) Address Legal Obligations

Navigating the legal landscape is a sensitive area for 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 not infringing on the privacy, civil rights, or civil liberties of the personnel within the organization.

There are several legal considerations that apply when addressing insider threats. CISA advises that it is a best practice to involve legal counsel in navigating the complex legal foundations, duties, and constraints an insider threat mitigation team will need to consider.

In addition, it is vital that insider threat program leadership ensures that the programs operate in accordance with existing federal and state law as well as organizational policies and that all actions are thoroughly documented. 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.

h) Identify High-Value Assets

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 to 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. Department of Commerce that provides a risk management framework for information systems, and risk assessment and management standards codified by the International Organization for Standards.²⁹ These standards can provide an 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.

29 R. S. Ross, *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 (Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2018), doi.org/10.6028/NIST.SP.800-37r2, available at www.nist.gov/publications/risk-management-framework-information-systems-and-organizations-system-life-cycle.

Organize and Equip



a) Integrate Information, Analysis and Response

The synchronized actions of analyzing information received and empowering people to investigate and respond are critical activities. While each element independently can show a behavioral anomaly, it is the combination of the elements that reveals the unusual behavior indicative of the potential for 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, including:

- 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
- User Activity Monitoring (UAM) logs
- Surveillance video

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.

Best Practices

- ➔ Collaborate closely with CIO(s)/CISO(s)
- ➔ Consolidate information, analysis, and response functions within the threat management team
- ➔ Employ automation and digital pushes to acquire data
- ➔ Strive to obtain regular, electronic access to data repositories
- ➔ Utilize a Personnel Hub that contextualizes data with personnel expertise to understand anomalous behavior
- ➔ Incorporate behavioral science to assist in analysis
- ➔ Establish relationships with internal and external investigative authorities

Figure 9. Integration Best Practices



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

Reporting mechanisms and procedures should be created to enable reporting of suspicious activity or concerning behaviors while protecting the privacy of the reporter and the reported. CISA created the [Insider Threat Reporting and Investigative Forms](#) as tools for organizations to download, review, and incorporate into their insider threat mitigation programs. The Reporting Form allows individuals to submit concerns related to a potential insider threat to an appropriate point of contact. The Investigative Form is designed to help document incidents and determine appropriate next steps, such as review by a Threat Management Team, referral to law enforcement, or other follow-on actions as necessary to protect the organization and its employees. 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 individual a new grievance, help protect the privacy of individuals involved, and help protect the sources and methods used by the insider threat team.³⁰

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 9* lists several integration best practices.

b) Develop an Incident Response Plan

An Insider Threat Incident Response Plan addresses unintentional and intentional incidents and is similar to an Emergency Response Plan. Creating an Insider Threat 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. As all response procedures should be in accordance with legal, ethical, privacy, and civil liberties laws or policies, legal counsel should assist in their creation. Collaboration with law enforcement is also advisable to ensure an effective response in case of an imminent threat.

An effective Insider Threat Incident Response Plan should cover the entire incident life cycle, including specifics of how an incident was detected and identified, 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 the process to develop an Insider Incident Response Plan, which can be found on the Federal Emergency Management Agency's (FEMA) website.

³⁰ Making Prevention a Reality," FBI, 78-79.



Plan



**Organize
& Equip**



Train &
Execute



Evaluate &
Improve

c) Establish Reporting Pathways

Reporting is integral to the prevention of an insider threat. Unknown threats 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.

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 of the system, 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 illegal activity.

Reporting can also be difficult because of the environment in which a threat or incident occurs. Many organizations are not 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 organizations, and governments are just a few of the organizations that may own multiple sites or require individuals to work outside of 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 support for peers, and ensuring the protection of privacy.

Employees and members should be trained to recognize atypical or concerning behaviors. Whether it is a clear threat, an expression of intent to do harm, some type of 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.



d) 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. User Activity Monitoring (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 and CCTV 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



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

3. Building an Insider Threat Mitigation Program



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 actively monitored and audited. 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 send alerts for 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 assess the data.

The Ponemon Institute’s 2022 *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 10*).

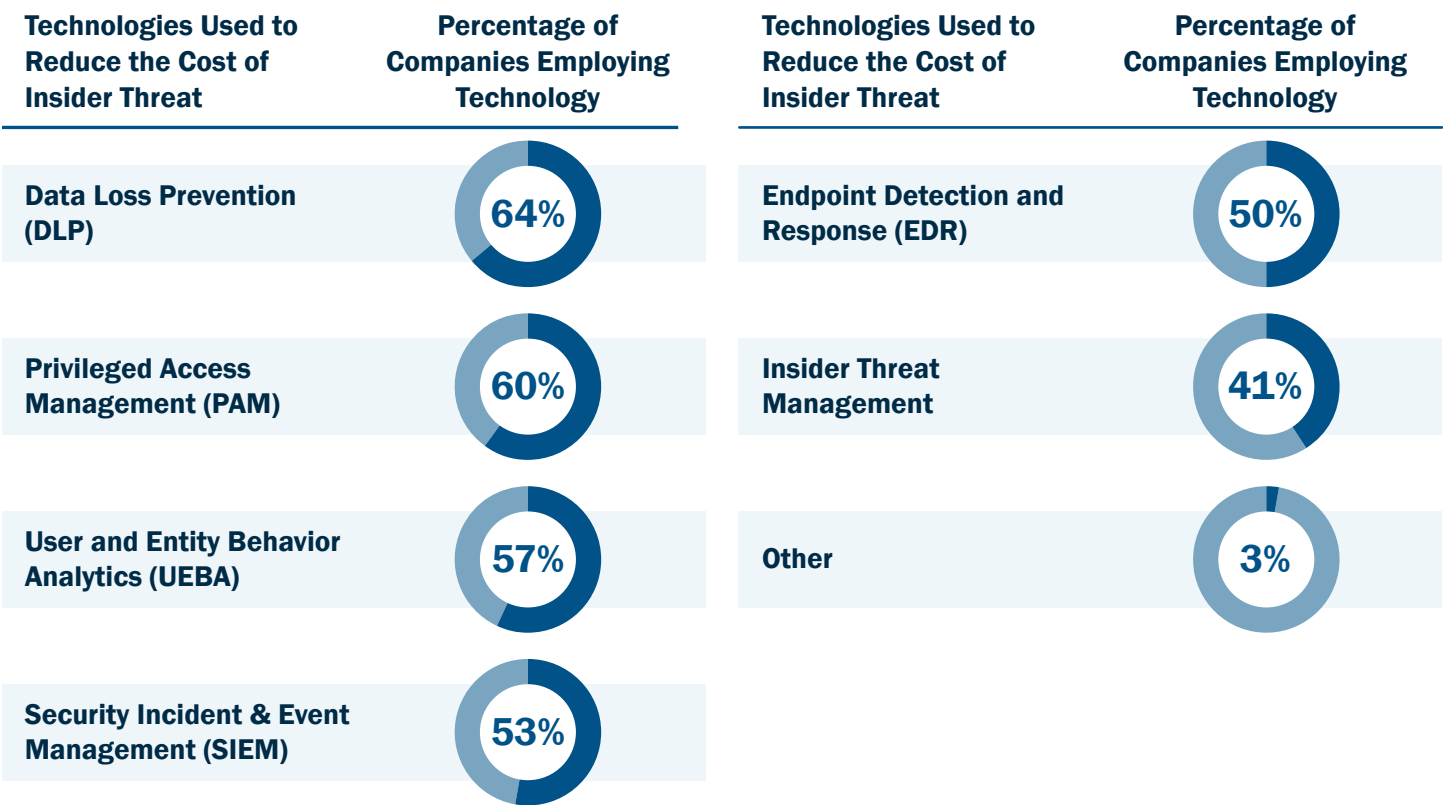


Figure 10. Tools and Activities Employed³¹

31 “2022 Cost of Insider Threats Global Report,” Ponemon Institute, 2022, accessed on October 14, 2025, available at https://go.proofpoint.com/rs/309-RHV-619/images/Ponemon_2022Report_A4_Final_UK.pdf, 20.





e) Establish a Risk Rubric and Threat Assessment Methodology

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

Individuals who commit malicious acts often follow a predictable pathway. As a best practice, organizations can begin their threat assessment by using a general risk tool to determine if an individual is on a path to committing an insider threat incident. Next, they can 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 over-reliance on risk rubrics or data analytic tools. Organizations are encouraged to have a threat management team to analyze an individual’s predispositions, behavioral indicators, and stressors to determine whether they are on a path to insider incident and, if so, how fast they are moving and if intervention is possible.

Organizations should consider the Factors Along the Critical Path to Insider Risk (*Figure 11*), to assess if an individual poses a general risk to an organization. The Figure 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 the individual’s concerning behaviors.³²

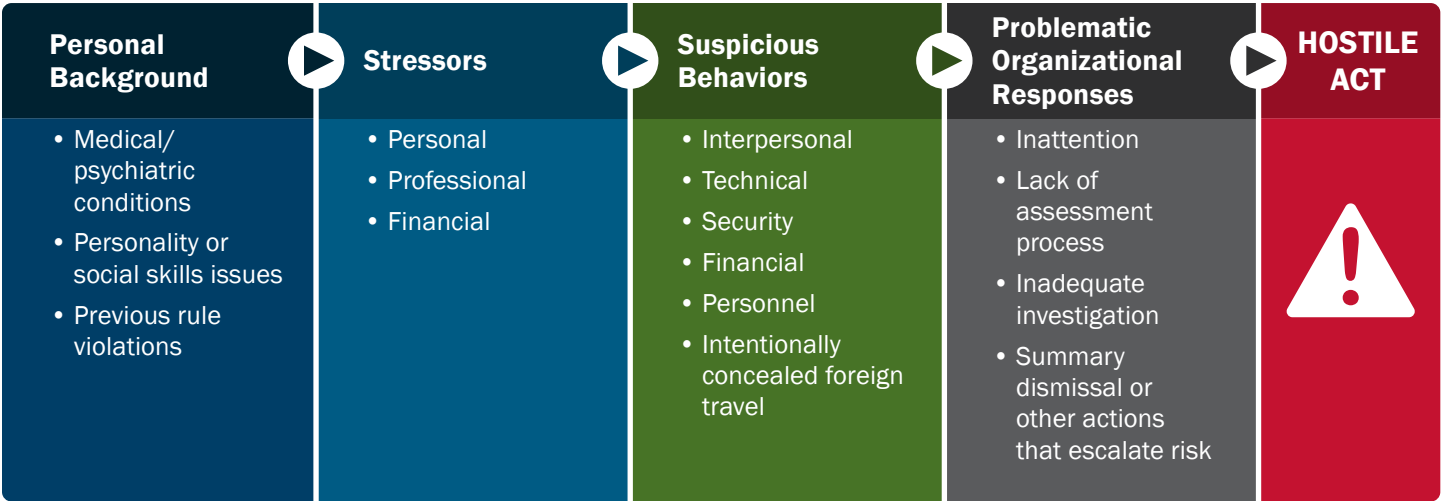


Figure 11. Factors Along the Critical Path to Insider Risk

32 Adapted from Shaw and Sellers, “Application of the Critical Path Method,” 2.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

– Risk Rubrics

Risk rubrics are evaluation tools that use a rating or categorization system to determine 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 an individual'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 an individual has been identified and is demonstrating behavior consistent with progressing towards an insider incident.

Establishing baseline behaviors will enable deviations to stand out from normal activities. *Figure 12* is an example of a notional scale risk rubric for determining a general risk to an organization.³³

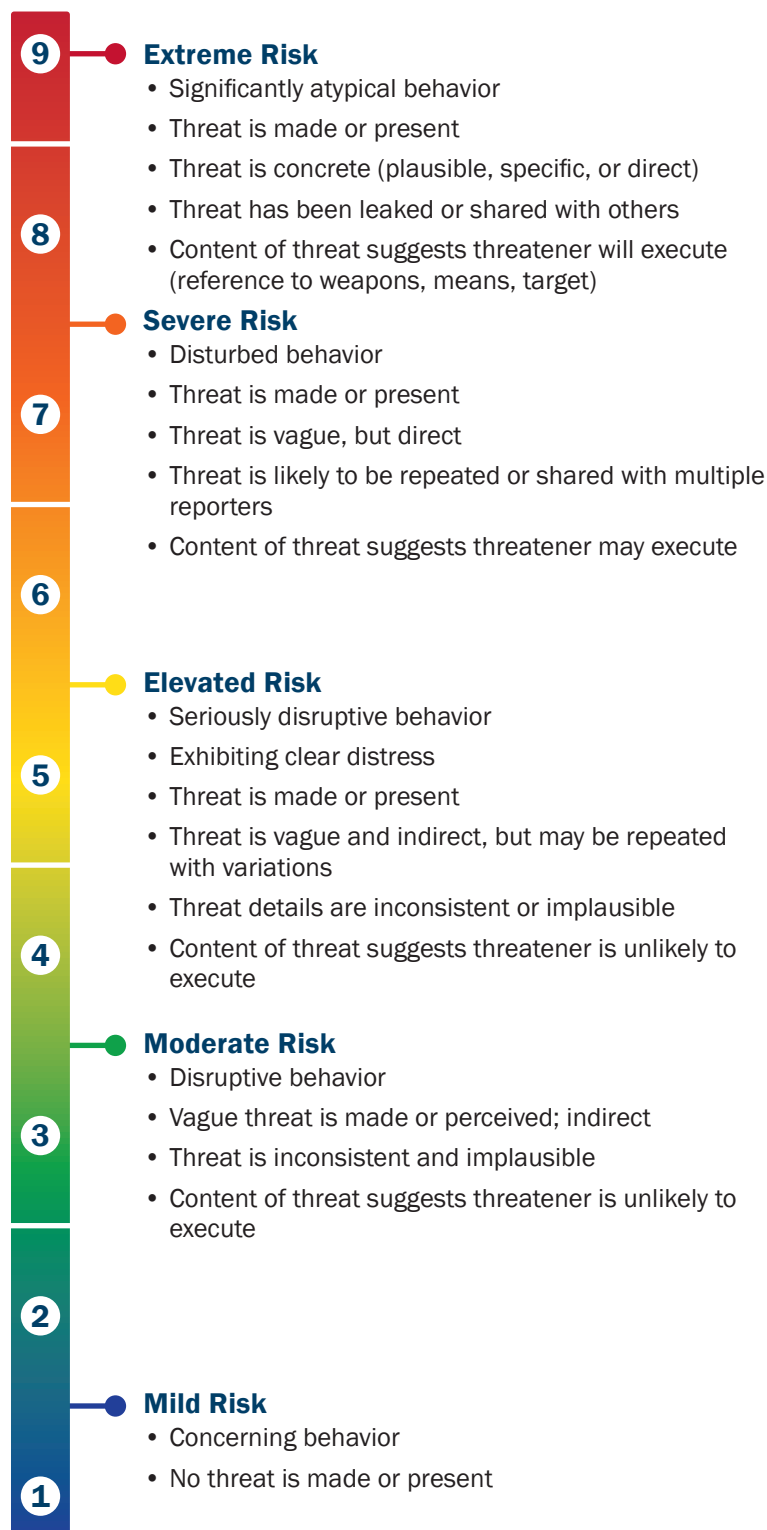


Figure 12. Notional Risk Rubric

³³ Adapted from "2019 NaBITA Whitepaper: The NaBITA Risk Rubric," National Behavior Intervention Team Association (NaBITA), 2019, accessed October 14, 2025, available at https://www.missouristate.edu/DOS/_Files/Nabitariskrubric.pdf.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

f) Establish a Multidisciplinary Threat Management Team

A multidisciplinary threat management team is the single most important feature of an effective insider threat mitigation program. The threat management team is responsible for running the organization's insider threat program. They will enact the policies and procedures established by the governance group. A team with a well-rounded composition of members provides a versatile group of practitioners who bring a variety of perspectives, capabilities, and backgrounds to address concerns.³⁴ The team's effectiveness depends on reliable data and an accurate analysis of the current state.

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

- Leverage 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. The team should have experienced individuals, including those with investigative backgrounds, who can understand the thought processes of potential insiders who seek to threaten the organization. Team members should value integrity, be creative, have a curious mindset, and a strong desire to protect the organization.

Each of these team members plays a key role in the insider threat program as each has access to information or a perspective that others in the organization may not. Together, the team will be able to contextualize anomalous behavior and determine the most appropriate response actions. *Figure 13* provides an example of a notional insider threat management team.

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. Legal counsel should be involved in this process and organizations should arrange for regular, and even unannounced, audits from an external team to ensure that individual information and privacy is protected.

– Team Name, Formation and Operation

The perceptions of the organization's members or employee workforce are an important consideration when establishing the threat management team. The name selected for the threat management team can inform the perceptions and participation of the workforce. A name that reinforces the helping nature of the program is advisable. For example, consider names such as the Incident Management Team or the Case Management Team.

The team should have a designated leader and a regular schedule to consider new developments and manage cases. It is 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.

³⁴ "Making Prevention a Reality," FBI, 71.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

Notional Threat Management Team

Members may include but are not limited to:

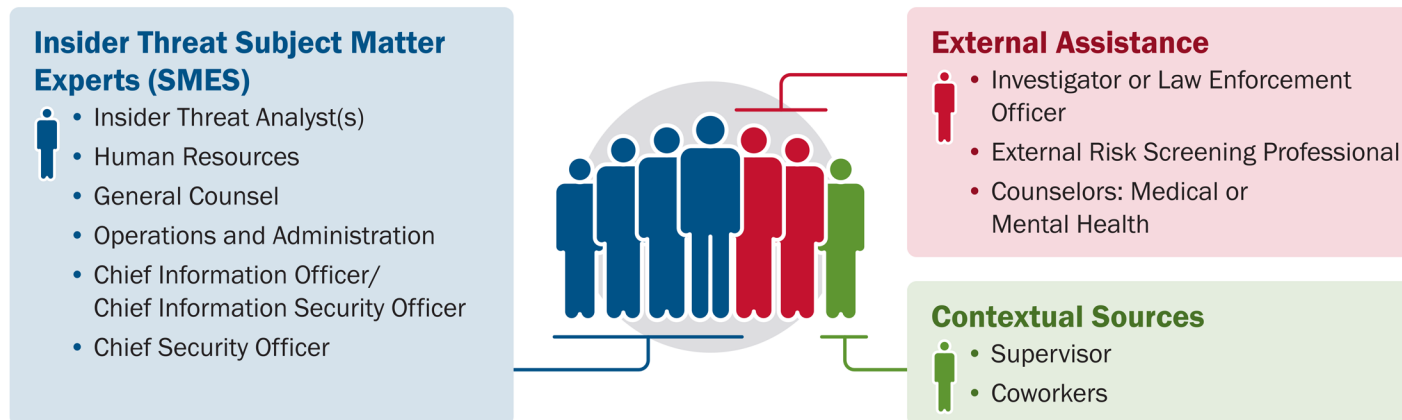


Figure 13. Notional Insider Threat Management Team

When scoping the threat management team's abilities, keep in mind that:

- 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 individual 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 an insider, 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 an insider incident.

Assessments should consider that:

- Risk factors, concerning behaviors, stressors, precipitating events, the environment, and may all be factors leading to an incident.
- 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.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

Threat management teams are effective because of the following:

- No one individual is positioned to see every single risk factor, warning behavior, or mitigator, nor is a single person positioned to manage a threat.
- When a threat management team receives a new case for review, individuals on the team may recognize an important detail due to their particular skill set, whereas other team members may not initially realize its importance.
- 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.³⁵

– Use of a Behavioral Health Professional on a Threat Management Team

As noted in detail later in this *Guide*, the use of a behavioral health professional specifically trained in the assessment of potential insider threats is a best practice for insider threat teams. They are uniquely qualified to determine the potential significance of psychological or personality disorder issues, previous violations, and stressors on an individual. It is critical that this behavioral consultant have specialized training in insider risk assessment methods, including violence risk assessment. Too often in organizations, an individual is referred to a therapist who is not trained in violent risk, such as an Employee Assistance Program therapist. In addition, oftentimes the therapist is provided with limited information on the concerning behaviors, resulting in a missed or poorly assessed threat. As with other specialized skill sets, support from a behavioral health professional may be obtained on an as-needed basis to support threat management team activities. To understand the roles and contributions of a behavioral health professional in insider threat assessment, see the descriptions included in [Chapter 5](#), Assessing Insider Threats.

– Training for Threat Management Teams

Threat assessment professionals require specialized training. Whether using in-house subject matter experts 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.³⁶ Training for a threat management team should include detailed and comprehensive training covering the behavioral or psychological aspects of insider threats, violence (workplace and domestic), 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 courses on 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 to be an effective team. 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.

³⁵ “Making Prevention a Reality,” FBI, 70.

³⁶ “ISC Violence in the Federal Workplace: A Guide for Prevention and Response,” CISA, 2019, accessed October 14, 2025, available at www.cisa.gov/publication/isc-violence-federal-workplace-guide, 9.

3. Building an Insider Threat Mitigation Program



Plan



**Organize
& Equip**



Train &
Execute



Evaluate &
Improve

On-the-job training should include tabletop exercises covering an array of simulated threats to allow the team to talk through the process of recognizing behaviors, assessing an individual, suggesting intervention strategies, and understanding their roles and responsibilities during a case. There are a range of training resources available with tools offered from Department of Homeland Security (DHS) agencies, such as CISA Exercises, FEMA, and United States Secret Service (USSS); Center for the Development of Security Excellence (CDSE); and the NITTF. See Appendix C of this *Guide* for useful tools and resources that can be integrated into training.

– Documentation and Record Keeping

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 and in accordance with any applicable federal and state laws. These policies should address retention, disposition, and access to the records as well as security and auditing.

A program should use a system of centralized record keeping, 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 hard copy 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. CISA provides Insider Threat Reporting Templates that can assist organizations in this process. A previous assessment that did not warrant a response can also be relevant data set in the event of any follow-on concerns or reports.

Accurate historical records are also beneficial if an individual moves out of their immediate area, especially if the individual 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.



Train and Execute



a) Market the Program

Successful programs require committed support from all levels within an organization. Marketing 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 personnel in support of a program.

b) Encourage a Culture of Safety, Awareness and Support

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 empathy creates an intervention opportunity when people see something or say something, paving the way for the early detection and identification of possible insider threats.³⁷

According to accounts from some of the most devastating insider threat incidents, people often knew something was wrong but did not report their suspicions

or concerns. Approximately two million people each year report some type of workplace or organizational violence, yet estimates are that 25 percent of violence goes unreported.³⁸ 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 and confidential reporting
- Developing multiple mechanisms for reporting, including 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
- Responding as necessary and appropriately when threats are reported so employees know reports are taken seriously

37 "If You See Something, Say Something®," U. S. Department of Homeland Security (DHS), accessed October 14, 2025, available at www.dhs.gov/see-something-say-something.

38 "Workplace Violence Statistics 2018," AlertFind.



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

Putting monitoring programs in place may cause employees to feel uncomfortable. There are several 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:³⁹

- Maintaining transparent and open documentation concerning the monitoring.
- Asking that employees or organizational members sign non-disclosure agreements when making a report.
- Securing union support (where applicable) for their insider threat program to bolster employee confidence the program is security-focused versus punitive.
- Ensuring 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.

c) Implement a Formal Training and Awareness Program

Training employees is a key process in an effective insider threat program. All organizational personnel, including 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 or unusual behaviors.

As noted previously, most insider threats are unintentional in nature, and are often the result of simple mistakes, or possibly negligence on the

part of employees. Due to this, it is recommended that organizations incorporate basic physical and cybersecurity best practices into their training programs, to ensure employees are educated on these topics. This will enhance both their own personal security, and help prevent any unintentional/negligent insider threat instances. Additionally, organization-specific training regarding remote and hybrid work may also enhance employee awareness when working at external locations. This training could include a broad range of topics such as using a Virtual Private Network (VPN), document storage and filing systems, and how to travel with organizational equipment.

39 "A Preliminary Examination of Insider Threat Programs in the U. S. Private Sector," Cyber Council: Insider Threat Task Force, Intelligence and National Security Alliance (INSA), 2013, accessed October 14, 2025, www.nist.gov/system/files/documents/2017/06/08/20131213_charles_alstrup_insa_part4.pdf.





Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

– Training to Incorporate

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:

- **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 explains the organization's policy on how to confidentially report suspicious 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 an acceptable use policy and non-disclosure agreements as well as the content of these agreements.⁴⁰

The governance group and the threat management team should receive additional specialized training on:



The laws and regulations regarding the collection, integration, retention, and safeguarding of sensitive data



Civil liberties protections and privacy laws



How to refer to investigations and request prosecution



The Insider Threat Response Plan



Threat awareness training based on functional roles

– Training Cadence and Timeline

Insider threat awareness and mitigation training should be continuous. It should begin as soon as an individual has been granted access 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.

See Appendix A of this *Guide* for useful tools and resources that can be integrated into training.

40 E. Kowalski, D. Cappelli, B. Willke, and A. Moore, *Insider Threat Study: Illicit Cyber Activity in the Government Sector*, CMU/SEI Technical Report (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2008), accessed October 14, 2025, available at [insights.sei.cmu.edu/library/insider-threat-study-illicit-cyber-activity-in-the-government-sector/](https://seis.cmu.edu/library/insider-threat-study-illicit-cyber-activity-in-the-government-sector/).

Evaluate and Improve



a) Conduct Exercises

Organizations should use exercises to evaluate the training and effectiveness of their insider threat program and insider threat 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. Agencies within DHS, such as FEMA and CISA, offer cyber and physical exercises on several topics including insider threats. CISA also provides downloadable tabletop exercise packages on [CISA.gov](https://www.cisa.gov).⁴¹ FEMA's Homeland Security Exercise and Evaluation Program serves as a useful guide for the design, execution, and evaluation of progressive exercises.⁴² FEMA also offers independent online training courses for exercise design and development as well as how to serve as an exercise evaluator.

– 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, response plans, 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, information and insights are obtained, and priorities are adjusted.

41 "CISA Tabletop Exercise Packages (CTEPs)," CISA, last modified January 3, 2024, accessed October 14, 2025, available at www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.

42 "Homeland Security Exercise and Evaluation Program (HSEEP)," Federal Emergency Management Agency (FEMA), last modified January 27, 2025, accessed October 14, 2025, available at www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

3. Building an Insider Threat Mitigation Program



Plan



Organize
& Equip



Train &
Execute



Evaluate &
Improve

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

b) Provide Oversight and Compliance: Internal Audits

An important concept in insider threat mitigation is ensuring that there is a means in the organization to provide oversight. 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.



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

Starting up the company's program began by obtaining support from corporate leadership through describing 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 combine 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, they developed a database of successful cases, 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 for theft.

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.

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.

Key Points

Principles and Keys for Success

- » Promote a protective and supportive culture throughout the organization
- » Safeguard organizational valuables while protecting privacy, rights, and civil liberties
- » Remain adaptive as the organization evolves and its risk tolerance changes
- » Focus on prevention and helping people versus just catching wrongdoing
- » Follow the guidance of Plan, Organize and Equip, Train and Execute, and Evaluate and Improve



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.

Potential insider threat perpetrators evolve over time and often exhibit multiple, overlapping, detectable, and observable behaviors. Insider threat researchers have 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. Personnel within an 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.

Four Core Behavioral Principles to Consider:

- 1** The probability of any specific individual becoming an insider threat is not randomly distributed across a population. **Certain individuals who exhibit specific behavior are more likely to pose threats.**
- 2** **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.⁴³

Most offenders do not threaten their targets directly but display identifiable behaviors that reflect 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 (e.g., hostile emails or other digital communications).

Visitors

Insider threats can arise not only from full-time members of an organization but also from visitors granted temporary or limited access to the organization and its facilities.

Examples of visitors may include:

- Individuals with whom the covered facility has business (such as suppliers, customers, and inspectors)
- Individuals or groups who visit a covered facility for personal or educational, technical, or scientific reasons
- Individuals or groups specifically sponsored by or representing the government
- Individuals or groups on guided tours to selected portions of the covered facility in the interest of public relations

43 S. L. Jaros, *A Strategic Plan to Leverage Social and Behavioral Sciences to Counter the Insider Threat*, PERSEREC-TR-18-16, OPA Report No. 2018-082 (Alexandria, VA: Office of People Analytics, Department of Defense, 2018), accessed October 14, 2025, available at www.opa.mil/research-analysis/personnel-security/insider-threat/a-strategic-plan-to-leverage-the-social-behavioral-sciences-to-counter-the-insider-threat/, 12.

Visitor Identification

By implementing identification and control mechanisms for visitors, organizations can help mitigate the potential insider threat risks posed by visitors seeking authorized access to facilities with malicious intent.

Identification measures help personnel quickly determine whether an individual is permitted access to a facility or a restricted area. Examples of personnel identification measures to consider may include:



Positively identifying visitors at facility entrance using government-issued photo IDs



Validating their visit by contacting appropriate facility personnel



Using visitor sign-in sheets documenting names, signatures, arrival time, departure time, and purpose of visit



Providing additional identification badges for restricted areas



Using visitor cards, badges, and escort requirements

Visitor Screening

Organizations should consider implementing visitor screening protocols to mitigate the likelihood of an insider threat from a visitor to their facility. There are several ways to implement tools and methods into screening protocols for individuals seeking access to the facility that can accommodate varying levels of security. Consider the following list as a starting point for suggestions to implement into screening procedures:



Bag Searches: Manually search bags (potentially of a certain size or larger) for prohibited items



Walk-Through Metal Detectors (WTMD):

- *Single Zone WTMDs* can identify an anomaly; they do not narrow down the location of the alarm annunciation on the visitor
- *Multi-Zone WTMDs* have multiple transmit and receive indicators, quickly allowing the screener to assess from where the alarm annunciation is generating a signal



Hand-Held Metal Detectors: A general screening device that can be used as either a primary or secondary screening tool



X-Ray Machines: A system that penetrates items with x-rays and produces an image of the contents displayed on a video monitor

All searches should be conducted professionally and courteously with the consent of the individual. Determine appropriate protocols for those refusing required screenings before entry into the facility. Establish secondary screening areas for people or items that are deemed suspicious for further investigation away from others so as not to disturb facility entrance points.

Visitor Escorts

Organizations should consider employing authorized personnel (i.e., escorts) to physically supervise and manage visitors within controlled spaces. It is advisable for organizations to develop local security escort policies and procedures tailored to their specific operational requirements, organizational culture, and assessed risk tolerance. Visitors requiring an escort should be processed in accordance with local security policies and procedures prior to being granted access to the facility. Organizations may choose to provide a verbal or written brief to visitors prior to entering the facility, advising them of what actions are not permitted within the premises.

The visit sponsor, their designee, or the designated organizational escort should be responsible for accompanying individuals within the facility. Personnel escorting visitors should maintain a visual line of sight, physical proximity, or other means of control over the visitor. Escorts must be knowledgeable about behaviors and actions that are not permitted by visitors according to organizational policy, and what steps to take if a visitor commits an unauthorized act. Escorts should also have sufficient understanding of the facility's sensitive assets and

areas to be able to identify when a visitor engages in suspicious or unauthorized activity in or around those assets and areas.

An appropriate ratio of visitors to escorts should be determined in consultation with the organization's security officials and other relevant stakeholders, considering organizational risk tolerance, location of critical assets within the facility, and relevant information that can inform the number of visitors an escort can reasonably monitor and supervise. It is recommended that all visitors to a facility sign for and wear a temporary visitor badge, clearly indicating their status and whether they require an escort for the duration of their visit.

Visitors can be asked to surrender a form of photo identification when signing out a visitor badge, which can be retrieved when they return their badge at the conclusion of their visit.

Organizations can enhance their security and mitigate potential insider threats by implementing identification, screening, and visitor escort procedures for individuals conducting authorized visits to their facilities.⁴⁴

44 Adapted from "Facility Access Control: An ISC Best Practice," CISA, 2020, accessed October 14, 2025, available at www.cisa.gov/resources-tools/resources/isc-best-practices-facility-access-control; adapted from "Public Venue Security Guide: Commercial Facilities Sector," CISA, 2021, accessed October 14, 2025, www.cisa.gov/sites/default/files/publications/Public%2520Venue%2520Security%2520Screening%2520Guide_508.pdf; and "Engineering Security: Protective Design for High Risk Buildings," New York City Police Department, 2009, accessed October 14, 2025, www.nyc.gov/assets/nypd/downloads/pdf/nypd_engineeringsecurity.pdf.

Threat Detectors

The Human Component of Threat Detection

Coworkers, peers, friends, neighbors, family members, and casual observers are the human component of 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 share their plans or grievances with others before acting.

Some insiders 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.

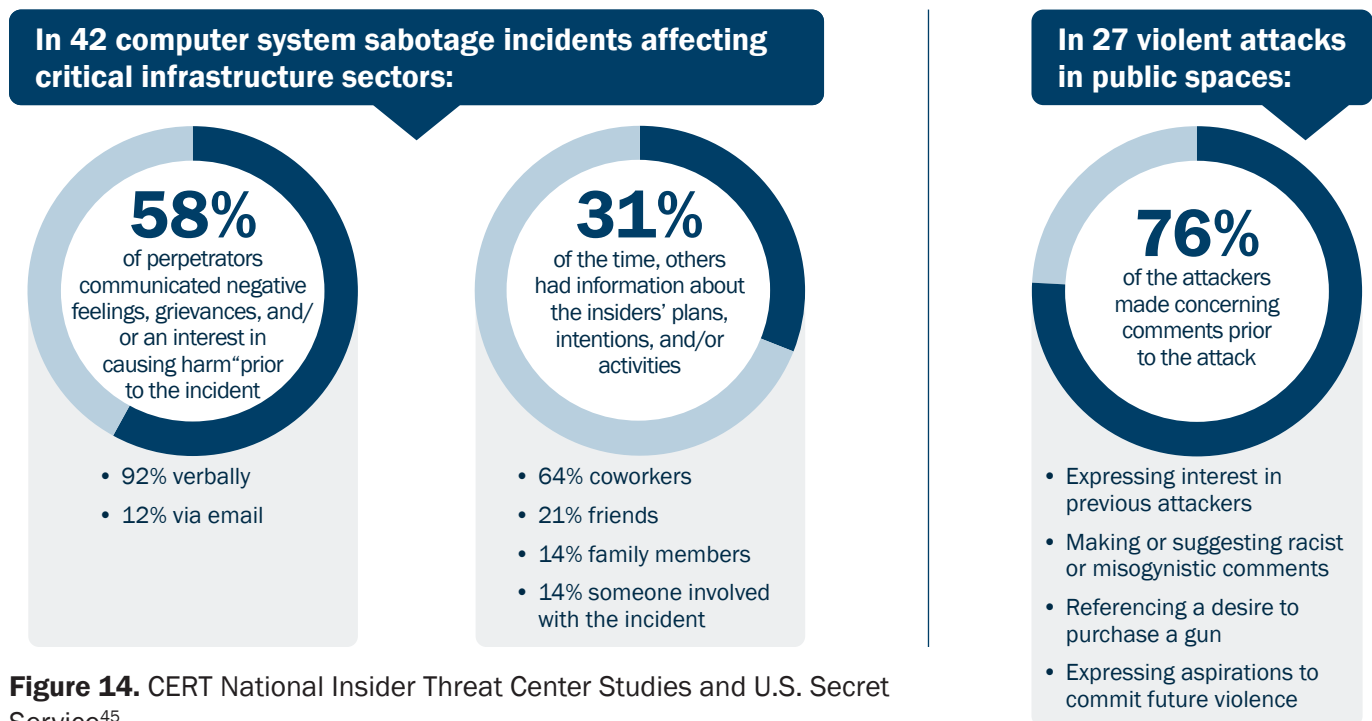


Figure 14. CERT National Insider Threat Center Studies and U.S. Secret Service⁴⁵



Figure 15. Considerations in Observing Behavior

⁴⁵ M. Keeney, E. Kowalski, A. Moore, and T. Shimeall, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* (Washington, DC: United States Secret Service (USSS), CERT Coordination Center, and SEI, CMU, 2005), accessed October 14, 2025, available at nsarchive.gwu.edu/document/22499-document-03-michelle-keeney-et-al-united-states, 16 and 20; and "Mass Attacks on Public Spaces: 2016-2020, U. S. Secret Service," National Threat Assessment Center (NTAC), 2023, accessed October 25, 2025, available at www.secretservice.gov/newsroom/reports/threat-assessments/mass-attacks-public-spaces/details-1, 58.

4. Detecting and Identifying Insider Threats

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 concerning behaviors and stressors—as well as the data on the likelihood of an insider sharing their plans to help them understand the role each person can play in detecting and identifying warning signs.

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

- » Visually observe those around you. 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.⁴⁶ Individuals who hear concerning comments, threats, plans, or see social media posts or observe hostile behavior should take them seriously and pursue proper reporting to supervisors, organizational leadership, senior managers, HR, or law enforcement, as appropriate.

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. It is important to understand 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 individual. 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; they are not all inclusive.

Remember:

The presence of some, or even all, threat indicators does not mean an insider is they are threat, nor does a lack of threat indicators guarantee an insider is not an insider threat.

⁴⁶ "Making Prevention a Reality," FBI, 99.

Personal Indicators

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

Personal 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 personal indicators, such as narcissism, a history of aggression or violence, psychopathy, or self-injury, can place individuals at higher risk for hostility, anger, violence, or suicide.

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 discreet 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.⁴⁷

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.

Personal Stressor Examples

- Serious health concerns
- Financial need
- Address change/move
- Death among family or friends
- Untreated 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
- Significant ongoing legal issues

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
- Termination⁴⁸

⁴⁷ "Insider Threat 2018 Report," Cybersecurity Insiders, accessed

⁴⁸ M. Kont, M. Pihelgas, J. Wojtkowiak, L. Trinberg, and A. Osula, *Insider Threat Detection Study* (NATO Cooperative Cyber Defense Center of Excellence (CCDCoE), 2014), 33-38, accessed October 14, 2025, available at ccdcoe.org/library/publications/insider-threat-detection-study/.

4. Detecting and Identifying Insider Threats

Professional stressors have the additional effect of creating potential grievances against an employer, organization, co-workers, 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 they may identify or observe.

Background Indicators

Background indicators are events that happen before an individual is hired by an organization or prior to an individual gaining access to a company's facility or networks. 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.

An in-depth background check may be necessary to acquire the information needed to identify a potential insider threat. 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. CISA's [Resources for Onboarding and Employment Screening Fact Sheet](#) provides information for consideration when conducting pre-employment background checks. 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.⁴⁹

Background Indicator Examples

- 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
- Untreated addiction (alcohol, drugs, gambling, etc.)
- Spending exceeding income
- Criminal record
- Concerning business relationships

49 Kont et al., *Insider Threat Detection Study*, 31-32.

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 individual's life, behavioral indicators are directly observable by peers, HR personnel, supervisors, and technology.

Behavioral Indicator Examples

- Unwillingness to comply with established rules, procedures, or organizational policies
 - Observable resentment with plans of retribution
 - Excessive or unexplained use of data copy equipment (e.g., scanner, copy machine, cameras)
 - Making contacts with competitors and divulging trade secrets or proprietary information
 - Excessive overtime work, or working odd or late hours without reason or authorization
 - Making offensive statements that do not adhere to an established anti-harassment policy
 - Unexplained social withdrawal
 - Disgruntlement toward peers due to perceived injustice
 - Increasingly erratic, unsafe, or violent behavior
 - Repeated breaches of rules, procedures, or organizational policies
 - Exploitable behavior (e.g, 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 United States
 - Efforts to conceal foreign travel and contacts⁵⁰
- *These examples should only be considered when present without a reasonable explanation

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 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.⁵¹

Most insider threat incidents require little technical sophistication to execute. In the banking and finance

sector, most attacks were simple and did not require much technological skill, carried out 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.

The examples below are not a definitive list, but provide a generic structure of potential insider threat indicators and a starting point for organizations to identify threat indicators appropriate for their specific, unique characteristics and concerns.

⁵⁰ Kont et al., *Insider Threat Detection Study*, 29-32.

⁵¹ Kont et al., *Insider Threat Detection Study*, 33-34.

Technical Indicator Examples

- Sending email messages with unusually large amounts of data or engaging in direct correspondence with competitors and outside organizations
- Using activity masking tools, downloading and using prohibited software, or connecting unidentified devices to workstations (e.g. USB, external hardware drive)
- Triggering alerts for key words or phrases in emails
- Attempting to print or copy protected or restricted documents and/or attempting to take sensitive information outside of the workplace
- Triggering authentication failures, failed login attempts, and/or user account usage alerts from unidentified devices

Employees or organizational members may pose a higher risk of insider threat when they have been terminated or expelled from a previous position under contentious circumstances. In 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. Specialized technologies should be used in conjunction with human observations and perceptions to detect and prevent insider threats. Technological detection tools can mine diverse datasets for anomalies, such as physical or computer access records, keystrokes or mouse clicks, or communication recordings.



Detection Tools:

- User Activity Monitoring software
- User Behavior Analytics software
- Facility access control system
- Video surveillance
- Web monitoring tools
- Security Information and Event Management tools
- Data Loss Prevention tools

Organizational/Environmental Indicators

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

Environmental factors in an organization can contribute to the potential of insider threats. 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 the issues that become part of the individual'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 to commit an attack

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, either financial or contractual
- Recent merger/acquisition
- Lack of risk assessment process
- Apparent indifference to complaints of harassment or discrimination
- Under-trained 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, 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

- 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/suicide⁵²

52 Adapted from "ISC Violence in the Federal Workplace," CISA, 68.

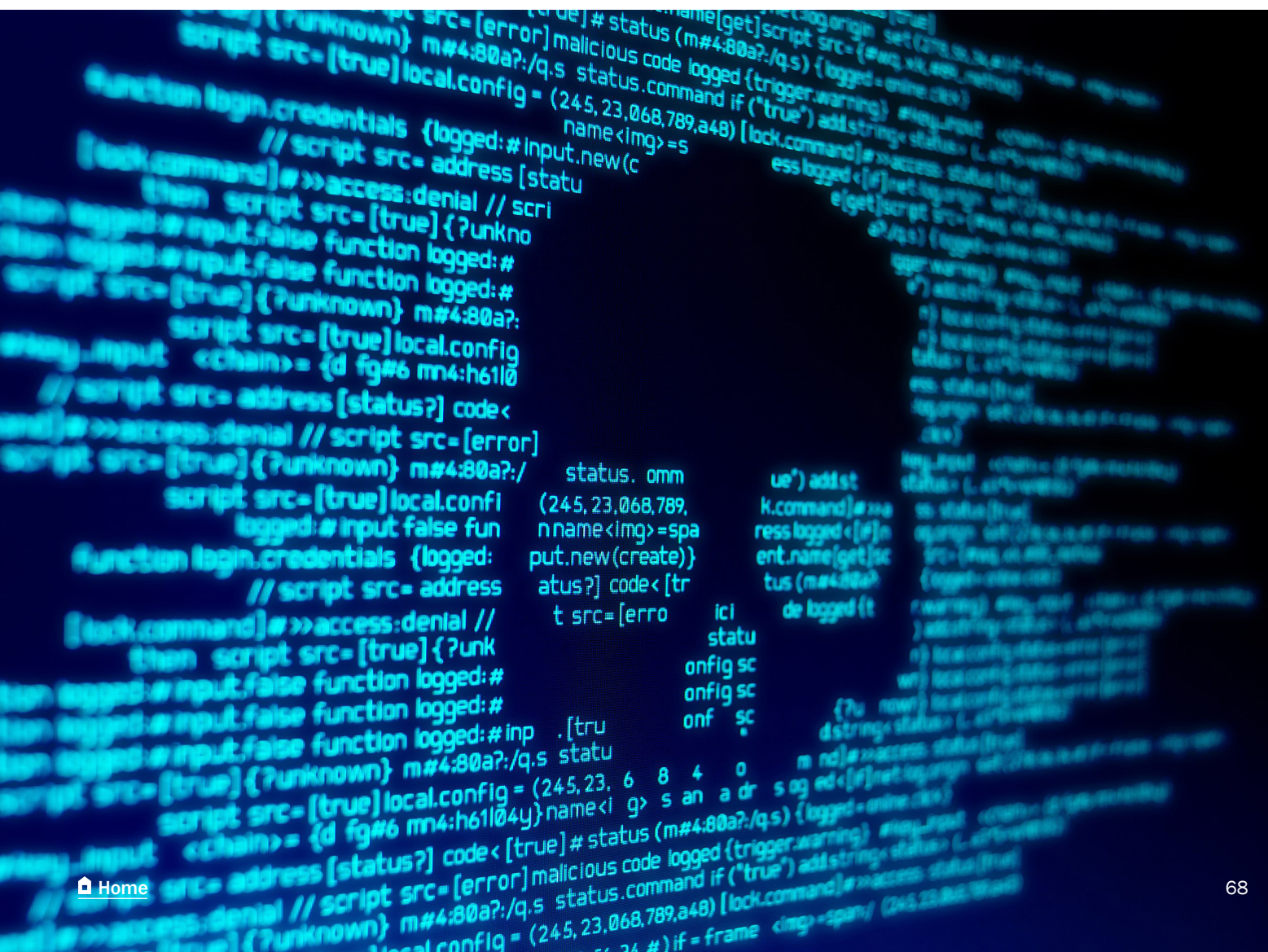
Terrorism/Hate Crime Indicator Examples

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 hate crime is a criminal

act committed against people or groups on the basis of specific characteristics that are defined by the law. Hate crimes can be committed by insiders against others within their organization.

Some indicators may involve constitutionally protected speech that may violate organizational policy but does not rise to criminal behavior. Examples of some common terrorism and hate crime indicators include the following:

- Expressing hatred toward a race, religion, disability, sexual orientation, or sex
- 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



Recognizing the Warning Signs

What Happened

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 social media account through which he communicated under a pseudonym.

Stressors leading up to the incident are believed to have begun a year prior 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 a new military installation, and he was again 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 his workplace to commit his act of violence, first targeting 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.

Concluding Thoughts

As described throughout this chapter, there are a range of observable behaviors that can serve as warning signs for an individual who is on a pathway to an insider threat 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 to recognize the behavioral signs that an individual may be on the pathway to violence

and other forms of insider threats. Organizations should establish a culture of shared responsibility for reporting incidents and their warning signs, including training 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 potential malicious or worrisome behaviors that could lead to an incident, setting the stage for successful insider threat mitigation.

Key Points

- » A successful program will account for the fact that the insider threat evolves over time and exhibits multiple overlapping detectable and observable behaviors.
- » 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.
- » 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 acts within the organization. These indicators are directly observable by peers, HR personnel, supervisors, managers, and technological systems.
- » Well-trained and vigilant people are key 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 share their plans or grievances. An individual 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 take protective steps when violence threatens to intrude on the workplace or organization.



5 | Assessing Insider Threats

Threat assessment is the process of compiling and analyzing information about an insider who may have the motive, intention, and capability of causing harm to an organization or personnel.

A primary purpose of an assessment process is to inform decision-making on how to manage an individual, with the goal of preventing an insider incident in any of its expressions.

Threat assessment is a complex discipline that requires an investment in training and preparation to develop proficiency. Given that there is no demographic profile of an insider threat, an objective assessment of threat-enhancing and mitigating circumstances as well as a contextual assessment of the behaviors exhibited by an individual 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.

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:

- » Implementing the threat assessment process
- » Recognizing the indicators for violence in threat assessment
- » Understanding that no set profile in threat assessment exists
- » Distinguishing the difference between making a threat vs. posing a threat
- » Applying the concept 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 health professional 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, including:

- » Is there evidence to suggest the individual poses a threat?
- » What type of threat does the individual pose?
- » Is the individual 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:

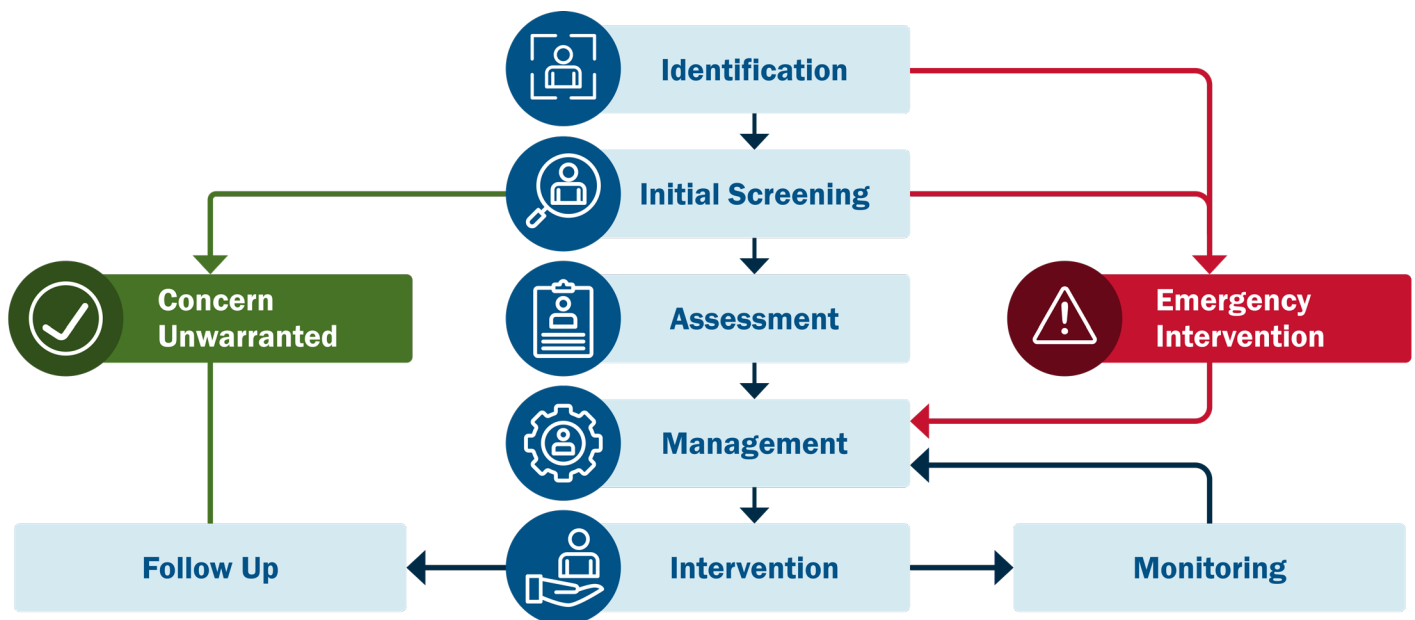


Figure 16. Threat Assessment Process⁵³

Initial Screening



Organizations should establish a clear, safe, and accessible process for reporting suspicious threats. 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 an initial screening is to ascertain in a 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 warranted, 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.

⁵³ Adapted from “Behavioral Threat Assessment and Management.: An Investment in the Future of Targeted Violence Prevention and Public Safety,” DHS, National Threat Evaluation and Reporting Program Office, 2024, accessed on October 14, 2025, available at www.dhs.gov/publication/behavioral-threat-assessment-and-management-investment-future-public-safety.

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 the individual(s) who raised the initial concern(s) and the identified insider.

Investigation and Assessment



Alternatively, if the threat management team determines that the individual potentially poses a threat and may have the 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.

The Consultative Process

All relevant data must be in hand in order to assess risk. These are unlikely to be available to threat managers faced with a need to quickly assess a rapidly changing situation. This is why threat managers work best in teams. The consultative process allows for discussion and consensus. Ultimately, a team will arrive at a conclusion on a level of concern and will recommend management strategies based upon the particulars of the case.⁵⁴

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 Insider Threat Incident Response Plan.

In the event of physical violence or sabotage, the threat management team should initiate the organization's insider threat Incident Response Plan, skip the initial screening, contact the appropriate authorities, and begin investigating 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.

⁵⁴ "Making Prevention a Reality," FBI, 40.

Assessment Process

After the threat management team has determined that an assessment is necessary, they initiate a deeper investigation into the individual, 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 individual. A successful investigation of an individual and any insider incidents or potential incidents requires the collection and analysis of available information gathered from all potential sources, including the individual, coworkers or associates, family or neighbors, and IT-related or online material.

» During the assessment process, the threat management team should give careful consideration to several factors in the inquiry, including deciding whether the incident intake will be conducted by internal, trained staff or outside law enforcement, determining 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.⁵⁵

» The team should collect evidence from different departments in the organization. Such evidence 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, cataloged, 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 individual and/or any witnesses to their behaviors, history, or stressors. It is essential that the key facts of an assessment are corroborated, with appropriate attention given to 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. Determining whether to interview the individual 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.⁵⁶

Threat management team members should consider asking the following key questions to both the individual and corroborating sources (e.g., 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 individual is progressing toward a malicious act.

⁵⁵ "ISC Violence in the Federal Workplace," CISA, 41.

⁵⁶ "ISC Violence in the Federal Workplace," CISA, 43-45.

Questions to Ask in a Threat Assessment

- Why, at this particular time, has the individual made comments or actions that have been perceived by others as threatening?
- What is happening in the personal life of the individual 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 individual cope with disappointment, loss, or failure?
- How does the individual interact with coworkers or associates?
- Has the individual received unfavorable performance reviews or been reprimanded?
- Is the individual experiencing financial problems, high personal debt, or bankruptcy?
- Has the individual spoken of homicide or suicide?
- Does the individual have a planned course of action, and, if so, is the plan reasonable and specific?
- Does the individual 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.⁵⁷

Determine an Individual's Baseline Behavior

A change in behavior for an individual 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 individual's behaviors, and then collect information from multiple reliable sources to detect and identify changes in that behavior.⁵⁸

To allow comparisons to baseline behavior, the assessor should:

- » Write detailed descriptions of the initial behavior(s) and concern(s) that supported the determination that the individual was a threat.
- » Monitor the trajectory of the individual's behavior by using a pre-determined risk rubric to understand if their concerning behavior is resolving, or escalating.
- » Remain alert during a long-term assessment and during post-intervention for any new information or behaviors that could require additional action, either with respect to the specific situation remove or the organization in general.
- » Implement and coordinate measures to assess and manage any risk of violence, considering that the choice of measures will be dependent on the level of perceived risk.⁵⁹

57 "Workplace Violence: Issues in Response," DOJ, FBI, National Center for the Analysis of Violent Crime (NCAVC), 2003, accessed October 16, 2025, available at www.fbi.gov/file-repository/stats-services-publications-workplace-violence-workplace-violence/view, 31-32.

58 "2019 NaBITA Whitepaper: The NaBITA Risk Rubric," NaBITA.

59 R. A. Fein and B. Vossekujl, *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials*, NCJ 179981 (Washington DC: DOJ, National Institute of Justice, 1998), accessed October 16, 2025, www.ojp.gov/pdffiles1/nij/179981.pdf, 55-57. Decompensating is to lose the ability to maintain normal or appropriate psychological defenses, sometimes resulting in depression or anxiety.

Analyze

Once the threat management team has collected enough evidence to cover the full scope of an assessment, they should begin to analyze the information to determine if the individual 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:

- 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 individual have the intent, motivation, and ability to carry out the threat?
- Has a law been broken?
- What is the individual's history?
- What are the behavioral and technological indicators?
- Does the individual have any stressors/personal predispositions?⁶⁰

As noted in [Chapter 3](#), a variety of evaluation frameworks or models, risk rubrics, and data analytic tools can be customized to an organization's threat criteria and risk tolerance and used in threat assessment depending on the type of threat in question (e.g., violence, cyber-attacks, theft of intellectual property, etc.). 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.⁶¹ 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 an individual 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 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.

⁶⁰ "Workplace Violence: Issues in Response," FBI, 18-19.

⁶¹ "2019 NaBITA Whitepaper: The NaBITA Risk Rubric," NaBITA.

5. Assessing Insider Threats

At a minimum, a threat assessment report should include:

- The individual's historical documents (e.g., HR report, background check, health records, previous assessments)
- A list of warning signs, including indicators, stressors, and triggers
- 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 individual, 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 individual is tending toward a violent act. [Chapter 6](#) contains additional management strategies.

Violence Indicators in Threat Assessments

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 DHS Interagency Security Committee categorizes workplace or organizational violence into four types:



Criminal Intent: No relationship between the perpetrator, business, or employees exists, and the incident is related to another crime like robbery or trespassing.



Customer or Client: Violence occurs between a customer or vendor and an employee. This category of workplace violence is the most common.



Worker-on-Worker: Violence occurs between two current or former employees in the workplace. The individual 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 individual 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.⁶²

62 "ISC Violence in the Federal Workplace," CISA, 3, and 9-10.

Terrorism/Hate Crimes

Terrorist threats do not always come from outside an organization, sometimes they are already an established, trusted insider. Insiders, when acting with terroristic motives, 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.

Hate crimes remain a significant concern in the United States. According to FBI statistics, over 14,000 individuals have been victims of such crimes in recent years. More than 75% of these incidents are driven by factors related to race, ethnicity, ancestry, and religion.⁶³

Threat management teams should be well informed of the indicators of terrorism and hate crimes 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. More information on these trends can be found through the websites of regional Fusion Centers, local police departments, the FBI, and the U.S. Department of Justice (DOJ).

63 "FBI Releases 2024 Hate Crime Statistics," DOJ, 2024, last modified September 24, 2025, accessed November 17, 2024, available at <https://www.justice.gov/hatecrimes/hate-crime-statistics>.



Example Questions to Ask in the Assessment of a Potentially Violent Threat

A threat management team should consider asking the following questions during a threat assessment to both the individual and corroborating sources, especially when the threat is potentially violent.⁶⁴

What motivated the individual to make the statement or take the action that brought them to attention?

Is there evidence that the individual has engaged in menacing, harassing, and/or stalking behaviors?

What, if anything, has the individual communicated to others, including their target, law enforcement, family, friends, colleagues, or associates?

- Has the individual shown an inappropriate interest in weapons or violent or extremist ideas/groups? Has the individual recently acquired a weapon?

How organized is the individual?

Has the individual engaged in suspicious behavior that may predicate an attack? 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 (potentially while armed)
- Attempting to circumvent security
- Assaulting or attempting to assault a target

Can the individual plan and execute a violent action against a target?

Is the individual's story consistent with their actions?

What factors in the individual's life and/or environment might increase or decrease the likelihood that they will attempt to attack a target (or targets)?

Is there evidence that the individual is experiencing desperation and/or despair? Has the individual experienced a recent personal loss and/or loss of status? Is the individual now, or has the individual ever been, suicidal?

Are those who know the individual worried that they might act based on inappropriate ideas?

⁶⁴ Fein and Vossekuil, *Protective Intelligence and Threat Assessment Investigations*, DOJ, 50-51.

Making a Threat vs. Posing a Threat

The central question in threat assessment is whether an individual poses a threat, not whether the individual has already 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. However, determining that an individual poses 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.

It is widely understood that insider threat incidents are rarely sudden, impulsive acts. Individuals do not normally 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*. Although some individuals will follow through on their stated threats, it's important to note that:⁶⁵

- Not everyone who makes a threat will carry it out
- Some dangerous individuals will act without an overt warning

Determining if an individual poses a threat will sometimes require monitoring an individual's workplace communications. Organizations should consult with legal counsel as part of the planning process before taking these monitoring steps.

Nevertheless, organizations should investigate all credible threats. Whether there is 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.

65 "Making Prevention a Reality," FBI, 15.



Warning Signs in Targeted Violence

According to a study on targeted active shooter violence conducted by the FBI, most perpetrators communicated their intention to cause harm to others before carrying out their attacks.⁶⁶ In most cases, these threats or expressions of intent to commit violence were made verbally. Direct threats are communications of an intent to do harm delivered directly to a potential victim in person (i.e., confrontation) or other means such as text, email, telephone, social media, etc. Direct threats to a victim are generally 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, an individual will communicate their threat, idea, or plan for a possible attack to a friend, acquaintance, or peer. 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, such as 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. Insider threat analysis shows that in past cases, many individuals knew about an attacker's threats, ideas, and plans before an act of targeted violence was carried out. However, individuals very rarely reported that information ahead of time.

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.

66 J. Silver, A. Simons, and S. Craun, "A Study of the Pre-Attack Behaviors of Active Shooters in the United States Between 2000-2013," DOJ, FBI, 2018, accessed October 16, 2025, www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view, 17-21.



Awareness of Scrutiny

At some point in the investigative process, an individual may become aware of investigative scrutiny. A threat management team should expect behavioral changes once an individual 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 mitigate any plans for malicious intent by making them more difficult to carry out undetected.

On the other hand, this awareness can cause the individual to engage in impression management (i.e., 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 an individual is beginning or continuing down a pathway to a malicious incident. As with any behavior, change is notable, and identifying that change and interpreting its meaning is important.

Use of a Behavioral Health Professional

The use of a behavioral health professional in the assessment of potential insider threats is a best practice for insider threat teams, especially in larger organizations. These experts are best positioned to determine the possible contribution(s) of any psychological or personality disorder issues, previous violations, and stressors on an individual. 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 health professionals are uniquely qualified to offer insights on mitigation strategies and determine their potential 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.

Organizations should consult legal counsel and, when applicable, a union representative before requesting an individual's medical or diagnostic records, when using a behavioral health professional, and/or 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 an individual'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, during which 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 health professional may be able to determine the personality characteristics of unknown insider threats based on their writings in cases of anonymous threats or leaks. A behavioral health professional may also be able to help determine the best intervention and/or termination strategies based on an individual's emotional and psychological state, or determine if they need 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.

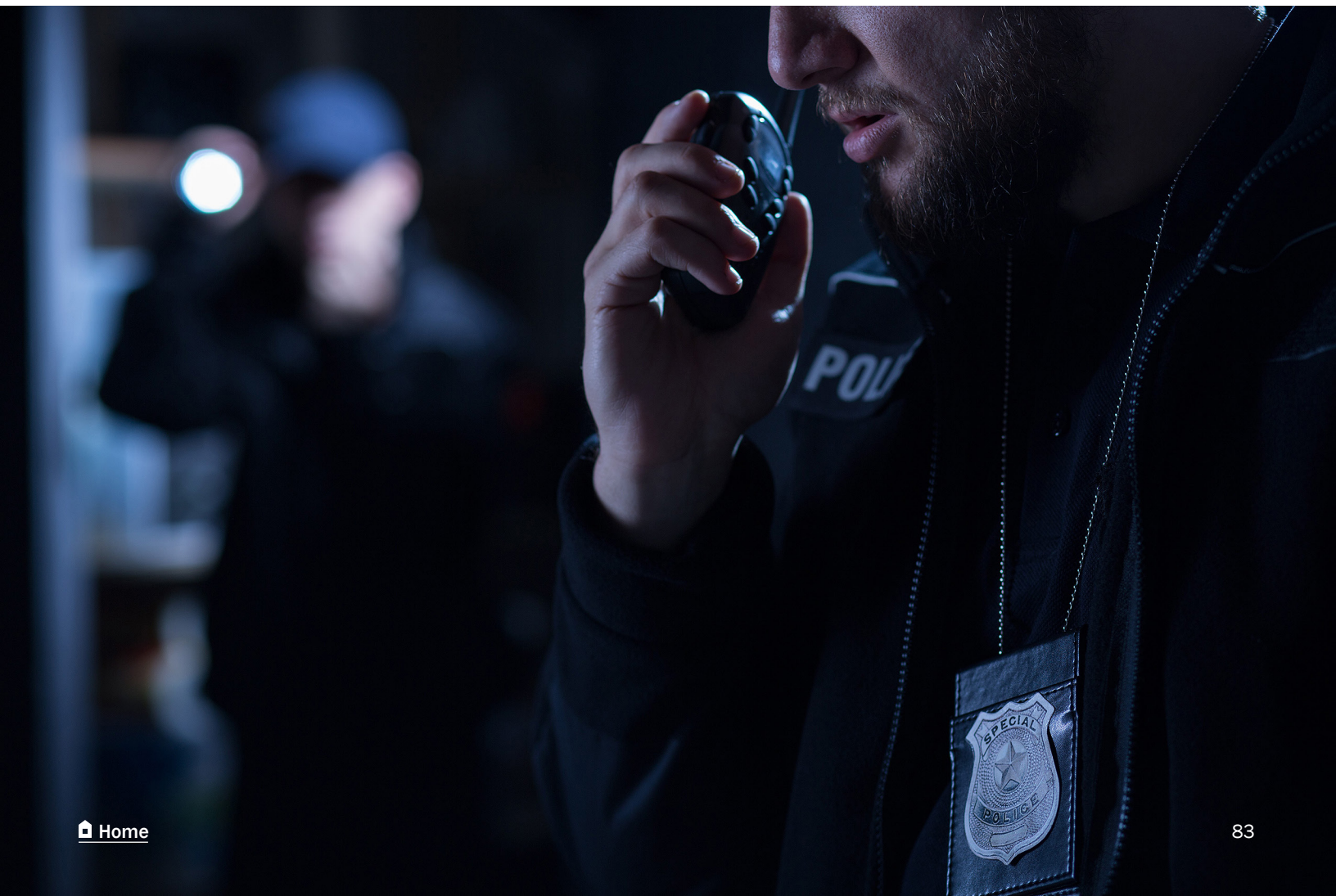
Case Considerations for the Involvement of Law Enforcement

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 involve law enforcement early in the process when a potential crime has been committed to ensure that any subsequent investigation can be conducted properly.

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



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. Targeted violence is rarely impulsive.⁶⁷ These acts are planned and often involve observable behaviors influenced by life stressors that were not reported to 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 the 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) 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 prior arrests, including 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.

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 their attack plan to at least one person. This type of reporting is important to threat assessments because of the frequency with which individuals reveal their plans to others.

67 G. A. Holden, B. Vossekuil, R. A. Fein, *Threat Assessment: An Approach to Prevent Targeted Violence*. National Institute of Justice; Research in Action, NCJ 155000 (Washington DC: DOJ, Office of Justice Programs, 1995), accessed October 16, 2025, available at <https://nij.ojp.gov/library/publications/threat-assessment-approach-prevent-targeted-violence>.

Concluding Thoughts

Threat assessment is a unique discipline requiring a team of individuals to evaluate an insider and determine the scope, intensity, and possible consequences associated with a potential threat. Threat assessment is based on behaviors, which are variable in nature. The ultimate goal of a threat assessment is to prevent an insider incident, whether intentional or unintentional.

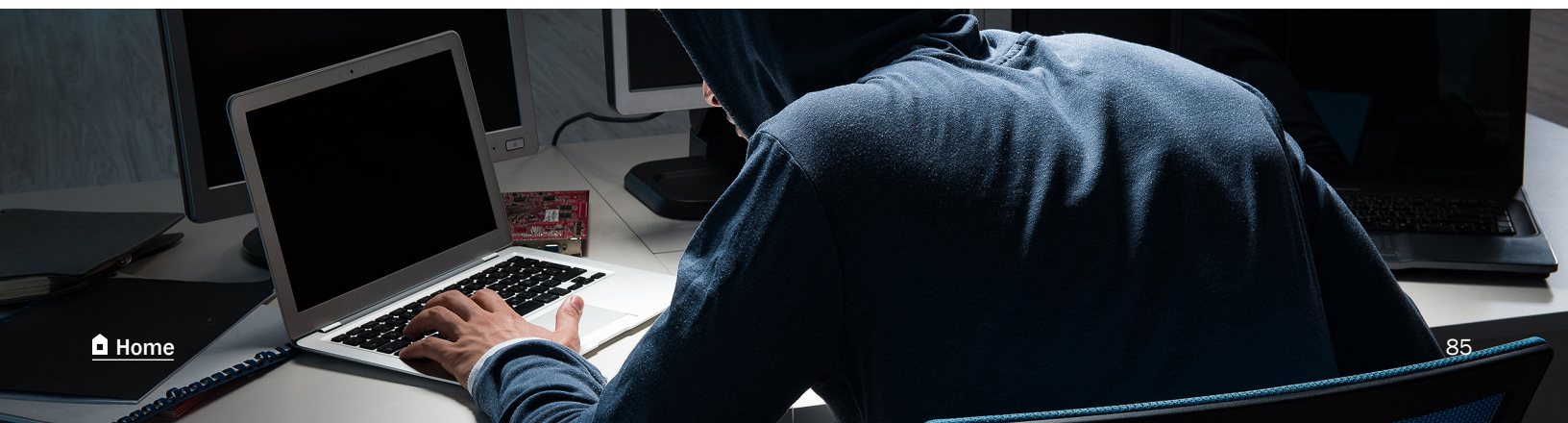
To successfully prevent an incident, a threat management team must determine whether an individual poses a threat. It is important to note that individuals may not pose a threat just because they make a threat or behave in a concerning manner. A threat management team will need to analyze an

individual's predispositions, behavioral indicators, and stressors to determine whether they are on a path to violence and, if so, how fast are they moving and whether intervention is possible. As such, the threat management team should be multidisciplinary in composition 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 individual, recommending intervention strategies to prevent an insider incident.

Key Points

- » Threat assessment is the process of compiling and analyzing information about an individual who may have the interest, motive, intention, and capability of causing harm to an organization or personnel.
- » The assessment process is intended to inform decision-making regarding how to manage an individual, with the goal to prevent an insider incident in any of its expressions, not necessarily to make an arrest or enforce policy with disciplinary measures.
- » The ultimate question to answer in a threat assessment is whether an individual is on a path to action, and, if so, how fast they are moving and where intervention may be possible.
- » In investigative and assessment planning, steps include determining the use of trained internal staff or outside law enforcement for incident intake, evaluating 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.
- » 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 an individual poses a threat, the team should generate 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.
- » 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.



6 | Managing Insider Threats

Recognizing that an insider poses a threat and may be on a pathway to violence or other malicious activity is an important first step. Assessing threats and determining an insider'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 balance between protecting the organization and caring for the individual. 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 an insider, 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. The organization could also opt to monitor the individual more closely for changes in mitigating factors that could increase the individual's risk, perhaps with assistance from family and/or others close to the individual. The threat management team could also achieve the organization's prevention and protection goals by improving an individual'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 an individual, 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 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 an insider 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 individual, 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 individual 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, threat management will be tailored and unique in each instance.



Figure 17. Focus Areas for Managing the Insider Threat

Management Strategies:

- » Are holistic, considering the individual, potential victims or targets, and the organizational setting or environment
- » Leverage multiple concurrent intervention strategies as necessary
- » Require accurate and effective communication with affected stakeholders
- » Require continual reassessment, adjustment, and follow-through
- » Allow each team member to offer a solution based on their specific discipline and resources
- » Are flexible and adapt as required

Known or previously used intervention strategies may not provide the answer. 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.⁶⁸

It is critically important to understand the personality and decision-making style of insiders 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 these interpretations may encourage future violations. A best practice when developing intervention strategies is to avoid triggering an individual's breaking point by unintentionally validating their grievance(s) or creating new ones. When designing and implementing intervention strategies, the organization should consider how their decisions, actions, and delivery could affect an individual's life, employment status, relationships, and dignity.

Contact your local law enforcement or call 9-1-1 if you have concerns about a potential immediate threat of violence in your workplace.

⁶⁸ "Making Prevention a Reality," FBI, 61.

Intervention Strategies

Considering the Insider

There are a range of intervention strategies that threat management teams should consider when recommending a course of action for an individual, including the following:

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

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

Legal actions, such as restraining orders or trespass warnings

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

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

Report of criminal activity to law enforcement

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

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 an individual. 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 individual 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.

Address the grievance. This intervention strategy can potentially alter an individual'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). 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 including:

- Allowing them to be heard
- Extending deadlines
- Finding a way to preserve their dignity
- Approving a transfer, position change, or work from home
- Reducing stress or tension

Set specific boundaries and limits to get the individual “in check.” This approach is an especially important consideration when the organization plans to allow the individual 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 assessment⁶⁹

69 “Making Prevention a Reality,” FBI; and Keeney et al., “Insider Threat Study: Computer System Sabotage,” USSS, and SEI, CMU.

Considering the Victim or Target

Victims and/or potential targets may also require management intervention, especially if the individual 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.⁷⁰

Intervention strategies include:

- Increasing vigilance
- Being alert to virtual stalking or research on public and private networks
- Changing work or participation hours
- Relocating a workspace
- Varying routes, routines, and activities
- Employing parking lot escorts
- Ceasing communication with the individual, if necessary
- Conducting personal safety planning

Considering the Organizational Setting and/or Environment

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 individual are limited.⁷¹

Examples include:

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

⁷⁰ “Making Prevention a Reality,” FBI, 58.

⁷¹ “Making Prevention a Reality,” FBI, 63-64.

Domestic Violence Concerns

Domestic violence has the potential to impact critical infrastructure by raising the likelihood of violence at their facilities. According to the Centers for Disease Control and Prevention, the lifetime economic cost associated with medical services for domestic violence-related injuries, lost productivity from paid work, criminal justice and other costs is \$3.6 trillion. The cost of domestic violence over a victim's lifetime was \$103,767 for women and \$23,414 for men.⁷² With the rise in popularity of remote and hybrid work, it is especially important to be aware of domestic violence concerns.

Domestic abuse can be physical, emotional, economic, sexual, technological or physiological, according to the Department of Justice.

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 at-risk individual.

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

Domestic violence abusers and targets may also require organizational and law enforcement 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.⁷³ Both abusers and at risk individuals can be found throughout organizations.

Indicators of Concern

Special considerations are necessary for managing an abuser. The following questions can be helpful in assessing the level of concern:

- Did the abuser harm or threaten a family member or intimate partner within the same organization?
- Did the abuser use organizational resources to harm or threaten a family member or intimate partner?
- Did a victim make a report to the threat management team, managerial staff, or leadership?

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 an appropriate course of action.

72 "Lifetime Economic Burden of Intimate Partner Violence Among U.S. Adults," American Journal of Preventative Medicine, 2018, accessed October 16, 2025, available at <https://pmc.ncbi.nlm.nih.gov/articles/PMC6161830/#:~:text=The%20estimated%20intimate%20partner%20violence,U.S.%20adults%20with%20victimization%20history>.

73 "Fatal Occupational Injuries in 2016 (Charts)," BLS, 2017, Slide 10, accessed October 17, 2025, www.bls.gov/iif/oshwc/cfoi/cfch0015.pdf.

Considering the Victim

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. Action is not an invasion of privacy if a threat management team determines that a potential domestic abuse situation could involve the workplace or organizational site.

It is also important to manage these situations with sensitivity; organizations should treat those affected by domestic abuse with care and concern. Organizations should make it clear to victims that their privacy will be preserved, only disclosing information about their circumstances to those who need to know due to their role protecting people and the organization from further potential violence.

When an individual is identified as being in danger from an abusive partner, a threat management team can recommend a variety of steps, including:

- Distributing the suspected abuser's photograph to security personnel, receptionists, and coworkers
- Denying the suspected abuser's entry into the work or organizational site, especially if a restraining or protective order exists
- Designating a parking space closer to the entrance for the victim; providing a security escort to the vehicle or public transportation
- Changing the victim's working hours to peak times
- Removing the victim's name from telephone directories and websites, and screen incoming phone calls
- Relocating the victim to another business or organizational location, if possible
- Referring the victim to outside agencies for care and counseling

The threat management team should document every report of domestic violence or threatened abuse 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. If an employee is the potential victim of domestic abuse, work with representatives from HR to determine best next steps. Work with them to determine how to best address their needs and provide safety.



Mental Health as a Factor

Mental illness is among the most common health conditions in the United States, with an estimated more than 1 in 5 adults experiencing some form of mental illness each year.⁷⁴ While some may assume that those with a mental health condition may act violently toward others, data indicates that a person with mental illness is more likely to be a victim of violent crime than a perpetrator.⁷⁵ In the case of insider threat, malicious threat actors looking for patterns of emotional vulnerability can become aware of or actively seek to obtain mental health-related information to identify and exploit potential targets.⁷⁶ For example, individuals experiencing periods of heightened stress, grief, or hardship could be manipulated or blackmailed into divulging sensitive information or engaging in risky behaviors.

The coexistence of both a mental health disorder and a substance use disorder further complicates the insider threat risk, as co-occurring disorders can amplify threatening behaviors and make early detection more challenging. According to a recent Substance Abuse and Mental Health Services Administration (SAMSHA) survey, approximately 21.5 million adults in the United States have a co-occurring disorder and people with mental illness are at a high risk of abusing substances.⁷⁷ Because of this complex landscape, organizations should avoid simply assuming that mental health issues directly lead to insider threats and recognize instead that risky behaviors may be symptomatic of deeper psychological distress.⁷⁸ Each person displays a unique

baseline set of behaviors, and it is deviation from this baseline behavior that may be cause for concern and the focus of attention. Remember, mental health and stress issues should not be assumed to indicate insider threat behavior; such assumptions can create harmful stigma and overlook real indicators.

As part of a holistic approach to insider threat mitigation, behavioral health responses encompass care for vulnerable individuals to prevent traumatic stress, and are used as interventions to assist in recovery from traumatic stress, accelerate recovery, restore function, and maintain health and welfare⁷⁹. Behavioral health professionals can recognize early indicators of concern without stigmatizing individuals. Insider threat programs should incorporate behavioral health professionals to identify anomalies and monitor changes in mental health or behavior.⁸⁰ Careful monitoring and consultation can reduce the risk of emotional manipulation by malicious actors.

Mental health concerns associated with insider threats are complex and 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 individual.

It is a best practice to secure the advice of a qualified threat assessment professional in the early stages of incident management for those who may be dealing with a known or suspected mental health disorder.

74 "Mental Health by the Numbers," National Alliance on Mental Illness (NAMI), last modified January 30, 2025, accessed November 17, 2025, available at www.nami.org/about-mental-illness/mental-health-by-the-numbers/.

75 N. Ghiasi, Y. Azhar, and J. Singh, *Psychiatric Illness and Criminality* (Treasure Island, FL: StatPearls Publishing, 2024), accessed October 16, 2025, available at www.ncbi.nlm.nih.gov/books/NBK537064/.

76 "Emotional Vulnerability," Forscie Insider Threat Matrix, last modified April 25, 2025, accessed October 16, 2025, available at insiderthreatmatrix.org/articles/AR1/sections/MT012/subsections/MT012.004.

77 "Co-Occurring Disorders and Other Health Conditions," Substance Abuse and Mental Health Services Administration (SAMSHA), last modified March 29, 2024, accessed October 16, 2025, available at www.samhsa.gov/substance-use/treatment/co-occurring-disorders.

78 "Insider Threat Indicators," CDSE, 12.

79 "ISC Violence in the Federal Workplace," CISA, 64.

80 *Understanding the Role of Behavioral Scientists in Insider Threat Programs*, PERSEREC 2019-035, RN-19-01 (Alexandria, VA: OPA, 2019), accessed October 16, 2025, available at www.opa.mil/research-analysis/personnel-security/insider-threat/understanding-the-role-of-behavioral-scientists-in-insider-threat-programs/, 1-2.

Considering the Individual in Question

There are a range of strategies that organizations should consider with the advice of a behavioral health professionals, qualified mental health professional and/or legal counsel. These include:

- Referring the individual for professional help, such as mental health or personal counseling, and encouraging them to attend appointments regularly
- 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)
- Placing the individual on medical leave
- Providing employees with comprehensive mental health benefits
- Engaging law enforcement for situations involving imminent threat

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

If (or when) an individual is assessed by a qualified mental health professional and does not pose an insider threat risk, consider allowing this person to return to work after conducting 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 individual participates, organizations should seek legal counsel when requesting a fitness-for-duty examination.

Organizations should seek the advice of a mental health professional and legal counsel regarding all applicable laws, duties, and protections for both the individual 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. As such, legal counsel should be engaged prior to

reaching out to law enforcement in the absence of an actual criminal violation. 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 individual

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, ensuring the police have correct information about an organization in its dispatch system, aiding in gaining additional support during periods of increased risk, and better preparing the organization for emergencies.



Involuntary Employee Separations

An employee who separates under contentious or involuntary circumstances may represent a potential security risk to the organization, its data, facilities, and personnel. This risk is heightened if the separation is not managed with diligence and care. To mitigate the possibility of a separating employee presenting an insider threat during this process, it is recommended that organizations take precautionary measures. Organizations should implement strategies during involuntary separations to provide for the wellbeing of the departing employee, the security of the organization, and the protection of other employees, including those directly involved in the separation process.

Laws and regulations govern employee separations. Sometimes the separation process can be lengthy, and it is important to synchronize any security or risk management actions to ensure they are complementary to the employee separation process. The process should treat employees facing separation with dignity and respect. It is important to recognize that the separation of an employee is a stressful situation for management, staff, and the employee. Developing a concise plan and timeline, which includes time and place of notification of separation, will assist in providing a smooth transition. Consider the following additional key points when separating an employee:

Plan and prepare for the notification of separation meeting:

- Consider the best people to deliver the notification of separation. Keep participants to a minimum but not less than two individuals, preferably individuals from outside the employee's immediate work group, other than the individual's supervisor.
- Before the meeting, prepare a written separation letter outlining the reasons for the separation and next steps. Ensure that all necessary documents, such as the employee's contract, performance evaluations, and any relevant HR or security policies are prepared before the meeting.
- Notify IT and the Security Office of the date and time of the notification of separation meeting and remove all physical and logistical access at an appropriate time based on risk. Remove the ability of the employee to access systems remotely.

Conduct the meeting in a private, safe, and respectful location:

- Choose a quiet and private location where you can discuss the separation without interruptions or distractions. Pick a location away from high traffic areas, where people naturally congregate, and away from the employee's immediate colleagues.
- If possible, pick a location near an exterior wall and exit. Arrange seating to ensure those delivering the news can exit if necessary.
- Have a place outside of the room for personal belongings such as backpacks, coats, etc. Do not allow these items into the room.
- Begin the meeting by expressing your appreciation for the employee's contributions, if applicable and if it will not compromise an administrative or investigative action. Alternatively, acknowledge the time the employee has been with the organization.
- Explain the reason for the separation in a timely, clear, and concise manner.
- Consider having building security notified if there is potential for an adverse reaction.

Be honest, empathetic, and non-combative:

- Communicate the decision with honesty and empathy and avoid blaming or criticizing the employee.
- Listen to their perspective and respond with compassion and understanding.
- Avoid responding to or allowing a separated employee to lure an argument.

Provide clear information about post-separation arrangements:

- Discuss the employee's final paycheck, and, if applicable, severance pay, health benefits, and any other post-separation arrangements. Where possible and if applicable, extend benefits to help the employee achieve a less stressful transition. Understand the employee may take some time to process the notification of separation and may not be able to absorb a lot of information. A best practice is to provide this information in written form for the employee to consider later.
- Answer questions and provide a copy of the separation letter and any relevant documents.
- Prepare and communicate a plan for the employee's personal belongings if located in the organization's facility. If allowing the employee to gather belongings, consider the day and time to preserve dignity and minimize risk. Do not allow unescorted access. Consider mailing personal belongings to the employee in a manner that is secure, insured, and provides proof of delivery and acceptance.

Recover Documents and Equipment:

- Prepare a plan for handling the return of department and agency documents and processing those documents once collected or returned.
- Obtain credentials, card readers, organizational ID Cards, keys, IT systems, any other identification cards, and building or parking passes and remove employee from access control system(s).

After the separation, respect the employee's privacy and confidentiality by not discussing the details of the separation with other employees. However, organizations should inform team members and key personnel the employee has separated to prevent unauthorized access and encourage reporting if the employee tries to return.⁸¹

By taking proactive steps before, during, and after the involuntary separation of an employee, organizations can mitigate the potential of insider threats, workplace violence, or other harm to the organization and its employees, while simultaneously respecting the dignity, rights and privacy of the separating employee.

81 "Managing Risk of Adverse/Involuntary Employee Separations: An ISC Guide - 2024 Edition," CISA, 2024, accessed October 16, 2025, available at www.cisa.gov/resources-tools/resources/isc-guide-managing-risk-adverseinvoluntary-employee-separations, 6.

Monitoring and Closing a Case

If an insider 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. Consider implementing an elevated protection posture or additional mitigation measures.

Organizations should begin threat monitoring immediately after terminating an insider. Threat monitoring is a management strategy that allows an organization to continue to have contact with an individual 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 individual'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 an individual'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 team initially determined that an individual posed a threat
- Document the changes in the individual's thinking and behavior that negate the original concerns
- Describe why the individual 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 individual and keep it in accordance with organizational policy. Refer to CISA's [Insider Threat Reporting Templates](#) for a downloadable template to document insider threat incidents and lessons learned.

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



Avoiding Common Pitfalls

Threat management can be short-term or long-term, with an open case ranging in duration from days to years. 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 an individual 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 responsibility for both the case and the individual and will serve to protect both organizations.⁸²

82 “Making Prevention a Reality,” FBI, 22-23, 76, and 78-79.



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. 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 individual, nor will each strategy work as intended. Effective approaches implement multiple, complementary solutions that affect the individual, the potential victim, and the organizational environment. They should be holistic, respectful, and prevention-focused, and they should use case-specific solutions. Intervention strategies should be a careful balance between protecting the organization and caring for the individual.⁸³

An important consideration is avoiding a circumstance where the management strategies selected become an individual's breaking point by validating their grievance(s) or creating new ones. When implementing intervention strategies, the organization should consider how their decisions, actions, and delivery could affect an individual'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 individual, and they provide clear guidance and oversight for those implementing solutions. They continually reevaluate active cases, reengage when necessary, and understand that patience and persistence may be needed throughout the process.

83 “A Preliminary Examination of Insider Threat Programs,” INSA, 2.



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 an individual. 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 an individual, 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 individual has been removed from the organization. In this example, an employer followed a defined threat management process after identifying an individual 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 United States 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.

A Successful Threat Management Strategy (Continued)

Second Intervention Strategy

When employees covering his job asked for the password to the automated safety control system for the plant, he refused to provide it. He also 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 individual. 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 the individual.
- » Manage insider threats through interventions intended to reduce the risk posed by an individual, always keeping in mind that the prevention of an insider threat incident and protection of the organization and its people are the ultimate goals.
- » Preserving the dignity of an individual 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 multidisciplinary approach.
- » 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 an individual's trajectory toward violence or mitigate 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 individual will aid and encourage intervention and will enable the threat management team to continue monitoring.
- » 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. Removal of an individual from the organization does not mean the person can no longer pose harm. Grievances may persist after termination.
- » Once an assessor has determined an individual'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. Some cases that appear to be resolved may end up requiring reassessment as new facts and circumstances appear.
- » If an individual 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 individual 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 proven best practices and recommendations as an aid for organizations to use to prevent and mitigate the insider threat.

The costs of workplace violence, loss of reputation, employee turnover, decreased productivity, intellectual property theft, and espionage are felt in innumerable ways, including the loss of life, decline in mental health, 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. As stated at the beginning of this guide, the costs of insider threat continue to rise and workplace violence remains a pervasive threat.



7. Conclusion

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 wellbeing 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 reporting
- » 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 multidisciplinary 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 in recognizing insider threats and reporting 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 individual, 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.



Appendix A

Tools and Resources

DHS 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.

CISA Resources

CISA Insider Risk Mitigation Program Evaluation Tool

Provides organizations with a tailored assessment of their strengths and vulnerabilities to strengthen insider threat programs. www.cisa.gov/resources-tools/resources/insider-risk-mitigation-program-evaluation-irmpe

CISA Assembling a Multidisciplinary Insider Threat Management Team

This infographic guides stakeholders in forming a comprehensive, holistic, multidisciplinary insider threat management team comprising personnel from various sectors of the organization. <https://www.cisa.gov/resources-tools/resources/assembling-multi-disciplinary-insider-threat-management-team>

CISA Insider Threat Mitigation Workshop

Offers a two-hour workshop that provides an overview of how to build an effective insider threat mitigation program. www.cisa.gov/resources-tools/training/insider-threat-mitigation-workshop

CISA Insider Threat Reporting Templates

Provides downloadable templates organizations can implement into their insider threat mitigation programs that provide employees with a reporting pathway and the governance group with a method to track previous incidents. www.cisa.gov/resources-tools/resources/insider-threat-reporting-templates

CISA Involuntary Employee Separations: An Interagency Security Committee

Offers recommendations for a risk-based removal and exiting security checklist. www.cisa.gov/resources-tools/resources/isc-guide-managing-risk-adverseinvoluntary-employee-separations

CISA Pathway to Violence Factsheet

Provides information regarding the behavioral indicators that assailants often demonstrate before a violent act. www.cisa.gov/resources-tools/resources/pathway-violence

CISA Preventing Workplace Violence: Security Awareness Considerations Infographic

Provides actionable recommendations and resources intended to prevent and mitigate workplace violence by cultivating a culture of awareness and support in the workplace. www.cisa.gov/resources-tools/resources/preventing-workplace-violence-security-awareness-considerations-infographic

CISA Resources for Onboarding and Employment Screening Factsheet

Provides critical infrastructure stakeholders with resources to conduct thorough background checks before extending an offer of employment. www.cisa.gov/resources-tools/resources/resources-onboarding-and-employment-screening-fact-sheet

CISA Tabletop Exercise Packages (CTEPs)

Provides downloadable exercise packages, including scenarios, discussion questions, and templates to plan and execute insider threat exercises. www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

CISA Violence in the Federal Workplace: A Guide for Prevention and Response

Provides guidance on how agencies can develop a workplace violence program capable of preparing for, preventing, and responding to incidents of workplace violence. www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide

Partner Resources

Carnegie Mellon University (CMU), Software Engineering Institute (SEI)

“An Insider Threat Indicator Ontology,” a technical report encouraging the use of ontology to bridge the gap in the insider threat community. www.sei.cmu.edu/library/an-insider-threat-indicator-ontology/

“Common Sense Guide to Mitigating Insider Threats, Seventh Edition,” a technical report offering recommendations based on ongoing analysis and research on the impacts of insider threats across various industries. www.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/

“Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls,” a discussion on potential issues that could arise within an Insider Threat Program. www.sei.cmu.edu/library/effective-insider-threat-programs-understanding-and-avoiding-potential-pitfalls/

“Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors,” where the authors aim to address gaps in the literature that hinder organizations’ understanding of insider threats. www.sei.cmu.edu/library/secret-service-and-cert-release-report-analyzing-acts-of-insider-sabotage-via-computer-systems-in-critical-infrastructure-sectors/

“Insider Threats: Your Questions. Our Answers,” provides a webinar and slides where experts present ongoing research and answer questions on the evolving nature of insider threats. www.sei.cmu.edu/library/insider-threats-your-questions-our-answers/

“Navigating the Insider Threat Tool Landscape: Low-Cost Technical Solutions to Jump-Start an Insider Threat Program” includes news, publications, events, and podcasts. www.sei.cmu.edu/library/navigating-the-insider-threat-tool-landscape-low-cost-technical-solutions-to-jump-start-an-insider-threat-program/

“Workplace Violence and Insider Threat Podcast,” discusses workplace violence, insider threat, and technologies to detect an employee’s intent. Audio and transcript are available for download. www.sei.cmu.edu/library/workplace-violence-and-insider-threat/

Center for the Development of Security Excellence

“Insider Threat Job Aids,” provides resources for risk indicators, reporting procedures, law examples, and policies. www.cdse.edu/resources/insider-threat.html

“Insider Threat Training Videos,” provides security training videos available on a variety of subjects, ranging from behavioral indicators of an active shooter to cybersecurity. www.cdse.edu/resources/videos/insider-threat.html

“Toolkits,” provides resources to help with a vigilance campaign. www.cdse.edu/toolkits/insider/cyber.html

Department of Homeland Security (DHS)

DHS Headquarters

“If You See Something, Say Something®” is part of a national campaign to raise public awareness in two primary areas: encouraging individuals to recognize signs that may indicate a potential nexus to terrorism, and to report suspicious activity to appropriate law enforcement authorities. www.dhs.gov/see-something-say-something

Federal Emergency Management Administration (FEMA)

“Comprehensive Preparedness Guide 101: Developing and Maintaining Emergency Operations Plans Developing and Maintaining Emergency Operations Plans,” provides guidelines on developing emergency operations plans and promotes a common understanding of planning to help planners examine threats or hazards and produce integrated, coordinated, and synchronized plans. www.fema.gov/emergency-managers/national-preparedness/plan

“Homeland Security Exercise and Evaluation Program (HSEEP),” provides common exercise policy and program guidance that constitutes a national standard for homeland security exercises. www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

National Threat Evaluation and Reporting (NTER) Program Office

“NTER Resources,” equips homeland security partners with resources to identify and mitigate threats of terrorism and mass violence to keep the nation safe. www.dhs.gov/nter-resources

U.S. Secret Service (USSS)

“Enhancing School Safety Using a Threat Assessment Model – An Operational Guide for Preventing Targeted School Violence,” provides fundamental direction on how to prevent incidents of targeted school violence. www.secretservice.gov/node/4464

Federal Bureau of Investigation (FBI)

“Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks,” examines how law enforcement officers and others may identify, assess, and manage the risk of future planned violence. www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

“The Company Man: Protecting America’s Secrets,” a video that launched as part of a Nationwide Awareness Campaign. The video discusses economic espionage, the cost, and how it puts the nation at risk. www.fbi.gov/news/stories/economic-espionage/economic-espionage

“Workplace Violence: Issues in Response,” addresses prevention, intervention, threat assessment and management, crisis management and critical incident response. www.fbi.gov/file-repository/stats-services-publications-workplace-violence-workplace-violence/view

National Counterterrorism Center (NCTC)

“First Responder’s Toolbox, Threat Assessment Threat Management,” a brief reference guide about Threat Assessment and Threat Management (TATM). This resource can be found along with a variety of other counterterrorism guides on the NCTC website. www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/jcat-products-resources

National Insider Threat Task Force (NITTF)

“Insider Threat Program Maturity Framework,” aligns with the existing Minimum Standards. www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

Office of People Analytics (OPA)

“A Strategic Plan to Leverage the Social & Behavioral Sciences to Counter the Insider Threat,” provides lessons for researchers who want to contribute to insider threat detection, prevention, and mitigation efforts. www.hsdl.org/?abstract&did=818886

“Overview of the Structured Professional Judgment Tools (SPJ) Reference Guide,” provides a framework for assessing risks related to insider threats and violence. www.opa.mil/research-analysis/personnel-security/insider-threat/overview-of-the-structured-professional-judgment-tools-spj-reference-guide/

Appendix B

Terms and Acronyms

Terms

Assess: To evaluate or estimate the nature, ability, or quality of an individual or situation.

Assessment Process: To utilize a set of operational activities that combine investigative processes and information-gathering strategies with operationally relevant questions to determine if an individual 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 ability of the organization or cause a severe negative impact on its ability to support essential missions and functions.

Cyber: Relating to or characteristic of systems 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): The 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: To prevent the occurrence of a hazard.

Due Process: Formal procedures for the fair treatment of an individual 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, including violence, espionage, sabotage, theft, and cyber expressions.

Financial Crime: A sub-category of 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 a 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, including 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.

Insider Threat Mitigation Guide: A guide containing best practice and recommendations 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.

Manage: To direct interventions focused on the individual in question, the target, and the situation or setting.

Malicious: Intending or intended to do harm.

Mitigate: To make less severe, serious, or painful.

Multidisciplinary Governance Group: A team of stakeholders or personnel from components or offices in an organization whose disciplines place 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).

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 reaction 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 not complying with maintenance or IT procedures, contaminating 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 an individual 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

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

EAP: Employee Assistance Programs

FBI: Federal Bureau of Investigation

FEMA: Federal Emergency Management Agency

FOID: Firearm Owners Identification

HR: Human Resources

IT: Information Technology

IRM: Incident Response Management

LEO: Law Enforcement Officer

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

SAMHSA: Substance Abuse and Mental Health Services Administration

SEI: Software Engineering Institute

SIEM: Security Incident and Event Management

UAM: User Activity Monitoring

UBA: User Behavior Analytics

USB: Universal Serial Bus

USSS: United States Secret Service

VPN: Virtual Private Network