KASEWARE

Guide to Creating a Proactive Insider Threat Strategy

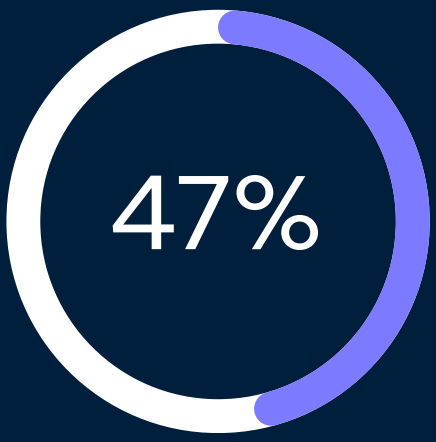
Everything You Need to Deter, Detect, & Mitigate Risk from Insider Threats

2024

Table of Contents

Insider Threats are On the Rise

Increasing layoffs, remote work, digitalization of business processes, and access to data through personal devices are increasing threats to organizations of all types and sizes. Add to that more sophisticated cyber crimes, malware, and social engineering tactics and it's no wonder insider threats are on the rise.



There's been a 47% increase in insider threats in the last two years.[1]

60% of cybersecurity attacks are carried out by insiders.[2]

Insider threats refer to security risks posed to an organization's data, systems, personnel, or operations by individuals who have authorized access to the organization's resources. These individuals could be current or former employees, contractors, partners, or anyone else granted access.

[1] Trellix, Threat Prediction Report, 2024
[2] IBM, Cyber Security Intelligence Index, 2016

The Cost of Insider Threats

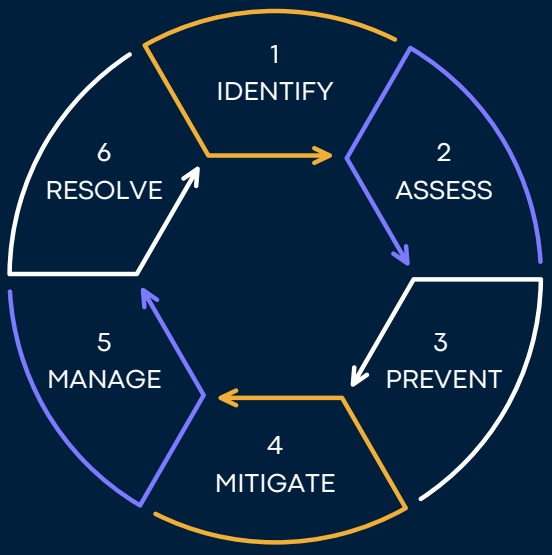
It's hard to say what the average cost of an insider threat is because it can depend on a wide range of factors from type of threat to organizational size to time it took to resolve, etc. However, data shows an average of $184,548 is spent to contain the consequences of a single insider threat event. The average cost is even higher for organizations in North America.

This doesn't take into account the intangible, peripheral costs associated with an incident, such as the damage to the brand and reputation, impact on employee morale, or causing strain on customer and partner relationships.

Unfortunately, insiders can be the most difficult threats to detect and prevent. As a result, organizations need a structured insider threat program that is proactive about preventing, deterring, and mitigating threats. This guide is designed to help you do just that.

Follow this guide's steps to build an insider threat program focused on identifying, assessing, preventing, mitigating, managing, and resolving threats.

$184,548
AVERAGE COST OF A SINGLE THREAT



[3] 2022 Cost of Insider Threats Global Report, Protectra

How to Create a Proactive Insider Threat Program

To identify and mitigate insider threats, you have to develop a plan. Relying solely on technology to mitigate insider threats exposes companies to potential risks. Instead, organizations need a balanced approach that integrates **people**, **processes**, and **technology**. This means starting with an internal task force or cross-functional team dedicated to protecting your organization.

1 Create a cross-functional team dedicated to identifying risks before they occur

A successful proactive insider threat program requires a multidisciplinary team. In addition to security, the team could include your HR, IT, and even the legal team depending on the nature of your organization. Ideally, any function that can compliantly and appropriately report on your organization's employee data and behavior should be included.

The goal of this team is straightforward: **identify the risks before a threat occurs and divert the risk into a more positive outcome** by creating policies, procedures, and training for incident identification, response, and mitigation.

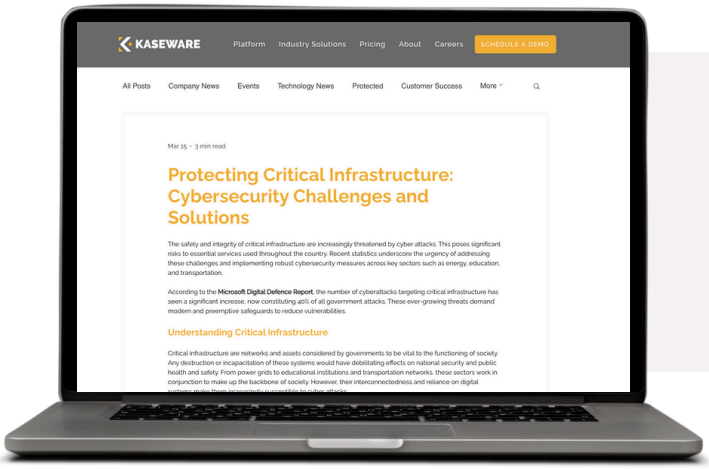
This team is also responsible for helping create a culture of trust, safety, and transparency so that employees feel comfortable reporting and helping prevent threats.

2 Use tools to identify behavioral indicators of potential insider threats

If you think of insider threat incidents and the events leading up to them, it's easy to recognize why the incident occurred — hindsight is 20/20. But proactively identifying them can be far more challenging than you might think. However, doing so is a key factor to mitigate risk.

The goal in creating a proactive strategy is to recognize the move from right of boom to left of boom. Left of boom is all about the preemptive measures you can take to prevent an insider threat.

There are a variety of tools and strategies designed to help identify potential insider threats. One such approach is the **Critical-Path Method by Eric Shaw and Laura Sellers**.



Critical infrastructure and cybersecurity challenges

Read Now

THE CRITICAL-PATH METHOD

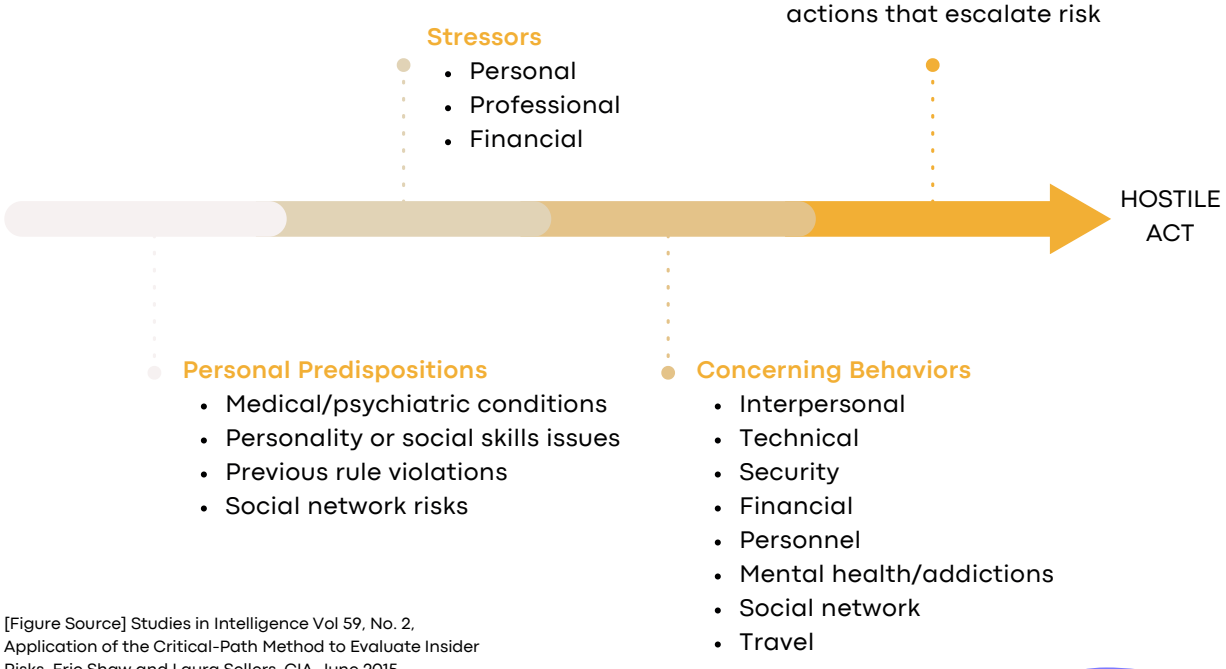
The Critical-Path Method is a valuable tool to assess insider risk as it takes into account the accumulation of factors over time. However, assessing and determining risk is still an evolving science. The ability to predict a person's behavior is challenging. But if you align your data analytics and monitoring tools that detect suspicious activities to this method, it may make it easier to identify risk.

For example, using an OSINT tool could identify a disgruntled employee who is sharing negative content about their employer online. Then combined with internal IT monitoring of privileged access management (PAM) systems it's found this employee had been accessing sensitive information. In this case, this employee is showing a personal predisposition and concerning behavior.

If the organization can divert the employee's behavior into a more positive outcome, it could avoid additional risk and a hostile act. Such examples of diverting behavior include:

- Revoking this person's access to sensitive systems, data, or resources to prevent further unauthorized activities.
- Scheduling a meeting to gather feedback, assessing their emotional state, and addressing underlying issues that may be causing their frustration — and evaluating if additional stressors exist.

FACTORS ALONG THE CRITICAL PATH TO INSIDER RISK



[Figure Source] Studies in Intelligence Vol 59, No. 2, Application of the Critical-Path Method to Evaluate Insider Risks, Eric Shaw and Laura Sellers, CIA, June 2015

Additional Resources

THREAT IDENTIFICATION RESOURCES

Security Information and Event Management (SIEM)
Surface real-time alerts of anomalous cyber-related behaviors

Identity and Access Management (IAM)
Help surface anomalous access-related data, both physical and cyber

Privileged Access Management (PAM)
Ensure people have only the necessary levels of access to do their jobs

User Behavior Analytics (UBA)
Monitor and alert to any actions that are unauthorized or suspicious

Data Loss Prevention (DLP)
Protect intellectual property, see how people are interacting with data, and comply with privacy laws

Open-Source Intelligence (OSINT)
Provide insights into security threats, market trends, and online behavior of individuals

RISK ASSESSMENT RESOURCES

The RA Standard
From ASIS International

Insider Risk Mitigation Program Evaluation (IRMPE)
From the Cybersecurity & Infrastructure Security Agency (CISA) & Carnegie Mellon University's Software Engineering Institute

3 Establish a process for assessing risk and prioritizing threats

Identifying insider threats through risk involves assessing the likelihood and potential impact of insider-related security incidents within an organization. After understanding the factors that contribute to insider threats and getting the tools in place for identifying them, the next step is to **evaluate risks and the associated costs to prioritize mitigation efforts effectively.**

The first step to prioritizing potential threats is to assess them in the context of your organizational infrastructure. Consider factors such as industry, size, culture, risk tolerance, data sensitivity, and insider access levels.

How complex your organization is, how interconnected it may be with other organizations, how outdated your systems are, whether or not you have dedicated resources to address threats, and other aspects all influence your critical infrastructure and how at risk your company or organization may be to different threats.

4 Create actionable policies, procedures, & processes to prevent incidents

The most impactful aspect of your insider threat program will be this step — without it, there is no means to take action. Here are some best practices for documenting your policies, procedures, and processes:

- Develop policies that outline the purpose, scope, and procedures for identifying, assessing, and responding to potential insider threats. Specifically, develop policies tailored to insider threats, covering areas such as access control, data protection, and employee monitoring. Ensure alignment with relevant legal and regulatory requirements.
- Define procedures for conducting impartial and thorough investigations into potential insider threats, ensuring the collection of evidence, analysis of digital trails, and interviews of relevant parties. Establishing a standard workflow is also helpful for compliance purposes.
- Establish criteria for assessing the severity and credibility of potential insider threats and determining appropriate response actions, including disciplinary measures, employee counseling, or additional security controls.
- Document all actions taken during the insider threat response process, maintaining accurate records and logs for compliance, auditing, and future reference purposes.
- Regularly review and update insider threat response policies and procedures based on lessons learned, emerging threats, and organizational changes, conducting periodic exercises to test effectiveness and identify areas for improvement.

CREATE THE RIGHT CULTURE

One of the more underrated ways you can prevent incidents is by creating a workplace culture that fosters transparency and trust. This is why having a multidisciplinary team supporting your insider threat program is so important.

Having policies and procedures that focus on the well-being of employees can play a big part in successfully diverting negative behavior that could result in a threat.

Ways to create a culture that helps combat insider threats:

- Create open communication channels for employees to report suspicious behavior or security concerns without fear of retaliation.
- Lead by example, with senior leadership demonstrating a commitment to security and compliance with organizational policies.
- Regularly communicate updates and reminders about insider threat awareness and prevention efforts throughout the organization.
- Solicit feedback from employees on ways to improve the workplace culture and enhance security measures to combat insider threats.
- Establish clear expectations regarding acceptable use of company resources and the consequences of violating security policies.
- Provide resources and support for employees facing personal or professional challenges that may contribute to insider threats.
- Reward and recognize employees who demonstrate exemplary adherence to security practices and contribute to the prevention of insider threats.

5 Focus on mitigation techniques as soon as possible

Insider threats are going to occur and eventually result in an incident. The focus should then be on mitigating the threat and the extent of damage as much as possible.

The potential expression of threats — or how a threat is acted upon — can vary, usually based on the motivation behind the threat:

MITIGATION TECHNIQUES

Here are four mitigation techniques you can leverage to limit the impact of an insider threat:

1. Access Control Management: Limit or revoke the insider's access to sensitive systems, data, or resources to prevent further unauthorized activities. This may involve modifying user permissions, disabling accounts, or implementing more granular access controls based on the principle of least privilege.
2. Incident Response Planning: Activate the organization's incident response plan to effectively manage and mitigate the insider threat incident. This involves following predefined procedures for containing the threat, preserving evidence, notifying relevant stakeholders, and coordinating with Internal teams and external authorities as needed.
3. Psychological Support and Intervention: Offer psychological support and intervention services to the insider if they are experiencing personal or professional issues that may have contributed to their actions. Provide access to counseling, mental health resources, and employee assistance programs to address underlying issues and reduce the risk of further insider threats.
4. Legal and Disciplinary Actions: Initiate legal and disciplinary actions against the insider as appropriate, based on the severity and impact of their actions. This may involve pursuing criminal charges, civil litigation, or internal disciplinary measures in accordance with organizational policies and legal requirements.

[Figure Source] Insider Threat Mitigation Guide, CISA, 2022

6 Manage and resolve incidents

Insider threats will happen, so you will need a plan for how to manage the potential damage whether you can prevent, deter, or mitigate them or not.

This is where it's critical to have an investigative case management system that can bring together all of the tools, resources, policies, procedures, and people into one location to make it easy to proactively manage insider threats.

Leveraging Investigation Case Management Software from Kaseware

An insider threat program cannot rely on technology alone. It is important to get your people, processes, and technology to work in tandem. However, **multiple, disparate platforms cause compliance, productivity, and efficiency issues.** A system that can integrate and bring everything into one will save your organization money and time — among many other benefits.

Kaseware is designed with people and processes in mind and is highly configurable to individual teams and workflows. So whatever insider threat program and procedures you establish, we can customize our platform to fit those needs.

Kaseware helps your organization mitigate the risk posed by insider threats by:

- Bringing all your data into one system through integrations and providing the tools to enrich and analyze the data through tools like link analysis and graphing
- Creating one common case file that includes all your disparate data so you get a holistic view of incidents, helping identify insights to solve cases faster
- Establishing a workflow and organizing and cataloging your processes and documents to maintain compliance and justify legal actions taken against a threat
- Reporting and sharing investigative work across teams and stakeholders to eliminate data silos and improve response times

What you get with Kaseware:

- A public portal for employees to report and share suspicious behavior
- Customized access control settings across your workflow, teams, and individual users
- Saved searches and alerts when something matches your search for quicker response times
- A variety of integrations and APIs set up to easily consolidate all your data and systems into one

Schedule a Demo

Proving the ROI of Your Insider Threat Program

Need help getting your organization's support for a dedicated insider threat program?

A 2019 Ponemon Institute report concluded that organizations with active threat management programs in place averaged a cost savings of $1.2 million per incident prevented. Take into consideration those cost savings versus the average cost of a threat ($184,548), and the return on investment is pretty good. An insider threat program will provide more benefits beyond just preventing an incident.

$1.2
MILLION
AVERAGE COST SAVINGS

Tangible benefits:

- Enhanced security overall: By proactively identifying and addressing insider threats, you can strengthen your overall security posture and reduce the risk of unauthorized access, data breaches, and other incidents.
- Cost savings: Preventing and mitigating insider threats can help you avoid costly security breaches, legal fees, regulatory fines, and damage to brand reputation.
- Risk mitigation and compliance: An insider threat program also helps organizations proactively identify and address security risks, thereby reducing the likelihood of compliance violations, legal liabilities, and reputational damage.

An insider threat program also offers intangible advantages such as increased trust, cultural transformation, and organizational resilience.

Organizations can strengthen their reputation, engage employees, and mitigate risks by fostering a culture of security awareness, accountability, and collaboration. A proactive insider threat program demonstrates a commitment to safeguarding sensitive information, promoting innovation, and maintaining industry leadership, positioning organizations for long-term success and sustainability in an evolving threat landscape.

A strong insider threat program is a competitive advantage

Organizations with robust insider threat programs are better positioned to protect their intellectual property, maintain customer trust, and preserve their competitive advantage in the marketplace. By prioritizing security and risk management, organizations can differentiate themselves from competitors and attract business partners and clients who prioritize data protection and security.

Kaseware Can Help You Enhance Your Insider Threat Program

Kaseware supports your security organization by consolidating your processes and technology into one system, accelerating and enhancing insider threat investigations. Schedule a demo to learn more.

Schedule a Demo

KASEWARE

Our secure case management platform easily handles your operations, cases, records, evidence, and more, while providing convenient features like dashboards, link analysis, the ability to work securely from any location, and intelligent forms so you never have to fill out duplicate information again. **Our goal is to make your job easier and the world a safer place.**

Backed by Expertise

Kaseware was founded by former Special Agents in the FBI who created Sentinel — the investigation case management software still used by the FBI today.

Advanced Technology

Our link analysis and graphing capabilities are second to none. With Kaseware, your teams get the analytical tools needed for intelligence and insights.

Highly Configurable

Kaseware is designed to be easily modified and configurable to the needs of your organization or agencies and even individual units and users.

For all business inquiries, contact our sales team

www.kaseware.com
salesteam@kaseware.com
+1 (844) 527-3927

Respond • Investigate • Resolve