Insider Risk Management

A Framework for the Modern Enterprise

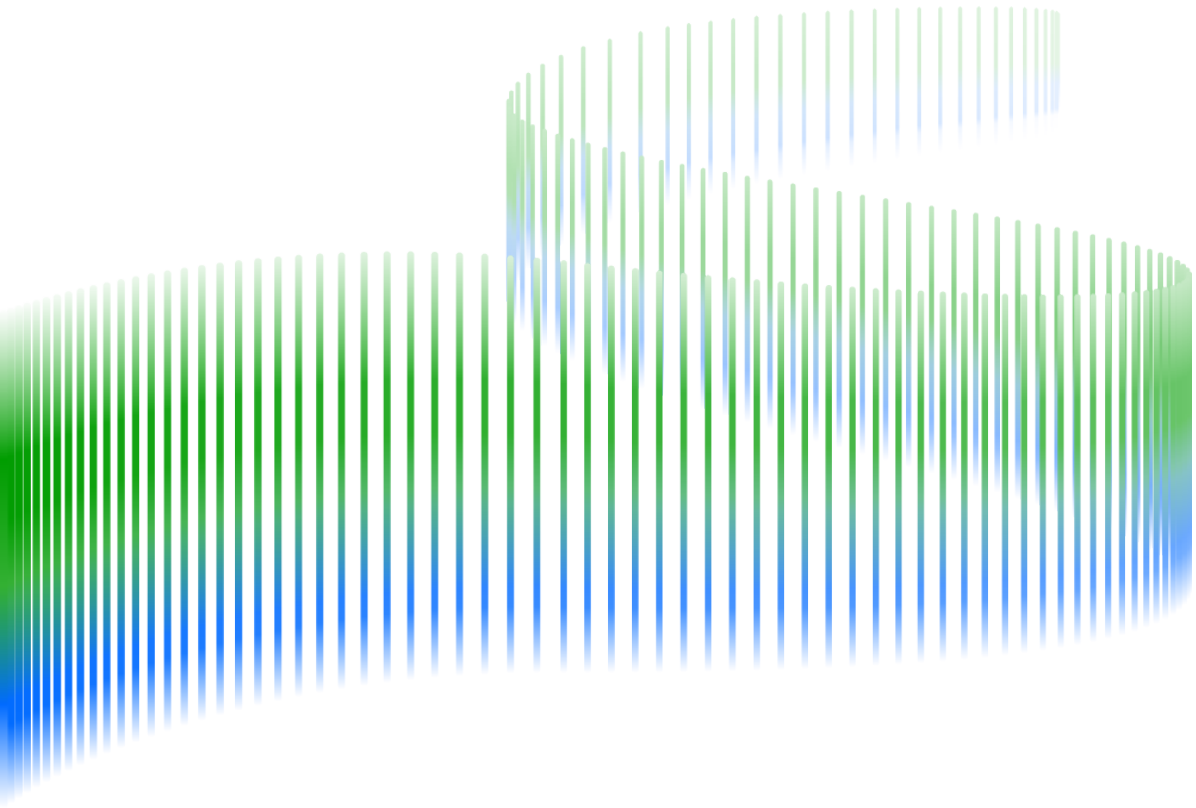

Table of Contents

Foreword

Today it's harder than ever to protect critical assets, and the threats from insiders continue to grow in both frequency and cost.

With a workforce that is more distributed than ever—employees working remotely, storing information in the cloud, and accessing corporate systems from nearly anywhere—sensitive data can be downloaded or exfiltrated in seconds, often without raising suspicion.

Why This Matters

According to the 2025 Verizon Data Breach Investigations Report (DBIR), compromised credentials and other forms of user activity play a role in most breach types, contributing to around 60% of all incidents, with credential abuse appearing in roughly 22% of breaches overall. Insider attacks can involve malicious intent or negligent mistakes by individuals who have been granted legitimate access. Employees are often the most common source, but you also need to consider contractors, vendors, and service providers.

The term insider threat often refers to damaging or illicit online actions, but it also covers a wide range of events including intellectual property theft, economic espionage, sabotage, workplace violence, and accidental misconfigurations.

Insider risk spans intentional and unintentional activity. A disgruntled employee might deliberately disable systems to harm the organization's reputation, while a contractor may inadvertently fail to reset passwords, leaving a vulnerability open for external exploitation.

Most incidents stem from the abuse of access rights, whether physical or digital. In its simplest form, this could mean an employee browsing unsecured file shares for sensitive information. In the case of a compromised insider, attackers may escalate privileges by exploiting flaws in applications or systems to gain unauthorized access.

The rise of generative AI and autonomous agents adds a new dimension. These digital "users" often operate with privileged access and can act on behalf of humans, but they are subject to drift, misuse, or compromise. Like human insiders, they may inadvertently or deliberately expose sensitive data or be manipulated into actions that put organizations at risk.

The Changing Nature of Insider Threats

Insider threat personas and event types keep expanding, but for you, credential theft is still the top concern. The 2025 DBIR reports that stolen credentials are among the leading causes of breaches, appearing in more than one in five incidents. For many organizations, the possibility of an attacker using valid employee credentials to gain access to systems is the highest-priority risk. Negligent insiders often play a role in these compromises, whether by mishandling passwords, falling for phishing attempts, or failing to follow security practices.

Shadow IT adds another dimension. The use of unsanctioned applications and the proliferation of unmanaged IoT devices introduce vulnerabilities that can be exploited for data loss or unauthorized access. For many organizations, the risks from these unmanaged assets are second only to credential misuse.

Email also continues to be a common avenue for data exfiltration. Insiders may forward sensitive information to personal accounts or external parties, including competitors or criminal groups. Because so much confidential data still resides in email, it remains a persistent target.

The challenge is compounded by the growing volume of insider-related activity and the extended time it often takes to detect and contain such incidents. Addressing the problem requires tools and processes that not only capture data from across the environment but also analyze it effectively to spot misuse and respond quickly.

Recognizing Insider Warning Signs

You can improve your chances of detecting insider threats by monitoring behaviors both inside and outside the workplace, including on-network and off-network activity as well as publicly available information. Taking a proactive approach can help identify malicious insiders before data is exfiltrated or operations are disrupted. It can also reveal negligent insiders whose mistakes may have equally damaging consequences.

Watch for workplace signals that should grab your attention. These include an employee showing interest in information outside the scope of their role, accessing systems during unusual hours without authorization, frequent visits to job sites, or consistently negative commentary about the organization on social media. More broadly, behaviors that deviate from established patterns for an individual or peer group may indicate emerging risk.

Risk is not limited to people. Devices, laptops, service accounts, and other entities can also exhibit unusual behavior. Examples include ports suddenly becoming active after long periods of inactivity, unexpected spikes in traffic, or anomalous activity that may suggest lateral movement following the compromise of legitimate credentials. In the case of AI agents, misconfigurations or manipulations such as prompt injection can lead to actions outside their intended scope.

Organizations that formalize insider risk management programs and adopt structured approaches to behavioral monitoring have demonstrated stronger outcomes. By building processes that account for both human and non-human signals, it becomes possible to detect threats earlier and reduce the impact of insider incidents.

Introduction

Insider risk management is often discussed but frequently misunderstood.

Some security practitioners view the insider problem strictly as a threat issue, treating all employees as potential adversaries. Others approach it mainly as a compliance exercise focused on closing gaps against frameworks such as NIST, ISO, or MITRE ATT&CK®. However, the most effective approach is to treat insider activity as a risk management challenge. By considering insiders in terms of asset impact, vulnerabilities, and threats, organizations can better understand their true risk posture.

The purpose of this eBook is to share best practices for managing insider risk through a structured model that emphasizes both human and digital insiders. It is organized into three sections:

1. **Framing the Problem:** Highlights the prevalence and impact of insider threats and common management challenges
2. **Understanding the Context:** Explores shifting motivations, workplace culture, and new technologies that influence insider risk
3. **Strategies for Action:** Outlines solutions and approaches for reducing insider risk, including practical steps for improving any program

Section One: The Problem

The principle of insider risk management begins with people and systems that have been granted access. This includes employees, contractors, partners, and increasingly, autonomous AI agents. Each can impact an organization in multiple ways: positively through productivity and innovation, or negatively through misuse, negligence, or malicious action. This section defines key terms and challenges to set the foundation for understanding insider risk.

Insider Risk Management: More Than Just a Threat

In many organizations, people shy away from talking about insider risk. You may hear terms like "insider trust" or "employee enablement," but those phrases can obscure the real goal: managing risk.

To be effective, insider risk must be understood in the proper context. Focusing only on the harmful actions of insiders results in a reactive posture where every employee is treated as a potential threat. This approach misallocates resources and prevents the development of an actionable program. Instead, focus on which insiders in your environment could have the greatest impact and on building programs that address assets, vulnerabilities, and threats together.

Understanding Risk

Risk management is the practice of evaluating harm to assets by considering three elements:

1. **Impact:** The potential harm to the organization if an asset is compromised
2. **Vulnerability:** The weaknesses that could allow a threat to succeed
3. **Threat:** The actors and actions that could exploit those vulnerabilities

Risk exists at the intersection of these three elements. Removing any one of them prevents a full risk assessment. Too often, "risk" and "threat" are used interchangeably, which leads to mischaracterization and flawed strategy.

For example:

- A NIST or ISO control assessment that identifies and scores gaps is a **vulnerability assessment**.
- A review of likely threat actors and their capabilities is a **threat assessment**.
- A business impact assessment that determines the level of harm from asset compromise is an **impact assessment**.

Each assessment type is valuable, but only when combined do they represent true risk.

The Risk of Applying Traditional Risk Models to Insider Threats

Imagine investing heavily in security only to find out that an employee has walked away with your most valuable intellectual property and given it to a competitor. The consequences (loss of R&D, reputational damage, and reduced goodwill) can be devastating. Despite billions spent on traditional defenses, such compromises continue.

Misplaced Focus

Most security programs are built to defend against external attackers. Yet many breaches succeed by exploiting basic security gaps, such as unpatched systems or default credentials, and by manipulating insiders through social engineering. According to the 2024 Ponemon Cost of Insider Threats Global Report, both the frequency and cost of insider incidents continue to rise, with credential theft among the fastest-growing contributors.

Focusing only on external actors overlooks the fact that insiders often play a central role, whether through negligence, poor practices, or intentional action. Intellectual property theft, for example, is committed predominantly by trusted insiders.

Misunderstood Risk

Legacy approaches often reduce risk to a single factor—threats, vulnerabilities, or a simplistic combination of the two. This leaves out the broader context. As outlined earlier, true risk is only understood when all three elements are considered together: impact, vulnerabilities, and threats. Ignoring any one of these leads to incomplete or misleading conclusions.

Risk is the likelihood that a specific asset could be compromised by a defined threat exploiting an existing vulnerability. Without all three elements, the concept of risk is incomplete.

Limitations of Traditional Assessments

Frameworks such as NIST, COBIT, and ISO offer important ways to measure organizational and network-centric risk, but they do little to illuminate insider risk. These assessments often emphasize vulnerabilities without addressing the unique ways insiders interact with critical assets. As a result, security leaders may be left with gaps when trying to prioritize protections for their most valuable resources.

Applying an Asset-Focused Insider Risk Model

An effective insider risk program requires prioritization. Not all threats, vulnerabilities, or assets carry equal weight. A practical model should:

1. Identify critical assets and determine the potential impact of compromise.
2. Map relevant threats and vulnerabilities for each asset.
3. Measure the specific risks to each asset.
4. Develop mitigation strategies based on prioritization.

By focusing on the interaction between insiders and assets, organizations can direct resources more efficiently and strengthen their overall risk posture.

Challenges: You're Not Alone

One of the most common challenges in insider risk management is determining ownership. Without a clearly defined executive sponsor, programs often stall. When everyone is responsible, no one is truly accountable.

What's needed is not a "czar" with absolute authority, but a senior leader with the mandate to foster collaboration across functions, bolster capabilities, and measure progress. In government programs, this role is often described as the "senior official" for insider risk. In the private sector, it may fall to a Chief Risk Officer (CRO), Chief Security Officer (CSO), Chief Information Security Officer (CISO), or, in some structures, a Chief Administrative Officer (CAO), General Counsel, or Human Resources leader. Each comes with advantages and limitations:

- **Chief Risk Officer (CRO):** CROs who focus on both strategic and operational risk are well positioned to sponsor insider risk programs. They typically report at a high level (CEO or board) and maintain strong cross-functional relationships. CROs focused solely on strategic risk, however, may lack the operational visibility needed.
- **Chief Security Officer (CSO):** Often a strong candidate, especially when no CRO exists. CSOs usually have relationships across HR, legal, IT, and security. Even if they don't directly manage technical tools, they can drive collaboration and coordination.

- **Chief Information Security Officer (CISO):** A traditional choice since insider risk has long been viewed as part of cybersecurity. However, CISOs are often focused on digital security, which may narrow the scope of an insider program. Reporting lines to the CIO can also create conflicts of interest, as CIO priorities may not always align with insider risk needs.
- **Chief Administrative Officer/General Counsel/HR:** In some organizations, insider risk oversight falls here due to reporting structures. This model can succeed if supported by strong security leadership but may lack technical depth without close collaboration.

The specific title matters less than ensuring clear accountability, authority to act, and the ability to bridge across security, HR, legal, and business functions.

Messaging

Clear communication is one of the most important success factors for an insider risk management program. Before executive sponsorship or governance can take shape, decision makers need to understand the program's purpose and value.

Effective messaging requires tailoring the story to the organization's culture, leadership style, and preferences. Some leaders want concise in-person briefings; others prefer written strategies or slide decks. The key is to understand how leadership absorbs information and shape the delivery accordingly.

A strong partnership with the communications team is a valuable starting point. They can help frame and deliver messages in ways that resonate. However, messaging should not be limited to executives. It must also extend across functions and reach the wider workforce.

By aligning communication with audience needs and organizational objectives, insider risk management programs can build the awareness and support required to succeed.

Balancing Security and Privacy

A proactive insider risk strategy requires balancing security needs with privacy rights. Policies should protect employees without restricting legitimate security efforts, and security controls should follow a least-restrictive approach. To achieve this balance, policies and procedures must be jointly developed with legal and privacy teams, ensuring protections are fair, transparent, and aligned with organizational values.

Defining the Program Scope

Many insider risk efforts remain narrowly focused on investigations. While investigative processes are important and often well defined, insider risk management goes far beyond responding to alerts or anomalous behavior. Without broader governance structures, critical elements of an insider risk program, such as prevention, awareness, and asset protection, are often overlooked.

Identifying Critical Assets

The core purpose of insider risk management is to safeguard the assets that give an organization its competitive edge. This requires a clear understanding of what those assets are. Critical assets can be physical or digital and include facilities, systems, source code, equipment, payment platforms, and operational technologies. Without a complete inventory and prioritization of these assets, organizations cannot effectively defend against insider or external threats.

Insiders Are Threats

From a business perspective, the source of harm, whether from outsiders, insiders, negligence, organized crime, nation-states, or AI agents, matters less than the fact that harm occurred. Both external and internal threats must be addressed to adequately protect the organization. Yet, insider risk is often minimized or dismissed as primarily an HR issue, rather than treated as a core security challenge.

What the Data Shows

Insider incidents are increasing. Most organizations report more cases in the past year and acknowledge they are not fully prepared to prevent, detect, or manage them. Research consistently shows that insiders account for a significant share of security events, often linked to employees who are departing the organization. Many of these cases involve unintentional actions—errors, negligence, or policy violations—that traditional security tools are not designed to detect.

How Insider Risks Differ From External Threats

External attackers typically seek disruption or data theft, often through denial-of-service attacks, ransomware, or the theft of personal data for sale. Their access is usually limited to network entry and exit points. Insiders, however, already have legitimate access to systems, data, and facilities. This gives them multiple ways to exfiltrate sensitive information such as trade secrets, intellectual property, customer data, or business plans. They may also disrupt operations through sabotage, fraud, or other misconduct. Because of this access, the potential impact of insider activity is often greater than that of external attackers.

Perceived vs. Actual Risk

Many organizations acknowledge that insider risk is a concern, but their perception of the problem often doesn't align with reality. Surveys show that leaders feel highly vulnerable, but relatively few have put comprehensive controls in place. Meanwhile, data from recent studies points to insiders being responsible for a significant share of incidents.

Key findings include:

- Insider incidents continue to rise year over year.
- Insiders account for a substantial portion of security events, often more than organizations assume.
- Many companies lack dedicated insider risk controls, leaving them exposed despite awareness of the issue.

Why Insider Risk Is So Difficult to Manage

Addressing insider risk requires recognizing why it is such an elusive and complex problem. Security teams are asked to protect corporate assets from people who already have legitimate access. Insiders may work in the office or remotely, use corporate or personal devices, and access data across networks, applications, and cloud platforms. This creates multiple opportunities for data theft or misuse.

Motivations also vary. Some insiders act out of financial gain, frustration, or revenge. Others are triggered by life events such as job changes, layoffs, or missed promotions. In some cases, bribery or external influence plays a role.

Privacy concerns further complicate insider risk programs. Many organizations are hesitant to deploy monitoring tools or behavioral analytics because of real or perceived impacts on employee privacy. Without the ability to detect early warning signs, security leaders face an uphill battle.

Effective programs require cross-functional collaboration across HR, security, risk, business units, and legal. Yet silos and conflicting priorities often limit coordination. You've probably noticed that employees today have more access to apps and data than ever, yet your monitoring and mitigation resources haven't kept pace.

Section Two: The Context

Employee loyalty is declining, while privacy concerns often outweigh security considerations. Organizations must adapt by building resilient security programs that evolve from a trust-but-verify mindset to a zero-trust security model.

This section examines the broader context of insider risk: the emergence of new types of insiders, their motivations, common personas, typical events, and key trends shaping insider risk management.

Defining the Scope of Insider Risk

Organizations often fail to properly define the insider threat problem. As a result, their security strategies, objectives, and tools miss the mark. Insider risk is broader than intentional theft of intellectual property. It also encompasses unintentional actions and a wide range of harmful activities, including fraud, sabotage, unauthorized disclosures, and workplace violence.

How an organization defines insider risk directly shapes the scope of its program. A narrow or ambiguous definition can create confusion around objectives, roles, responsibilities, and funding. This lack of clarity often undermines collaboration and leads to program failure.

A best practice first step is to establish a clear definition of insider risk by identifying which personas and event types the organization intends to address.

Insider Threat Personas

Leakers

Leakers represent a newer type of insider. Employee loyalty has eroded as job mobility, offshoring, cost-cutting, and unstable corporate environments have weakened long-term commitment. Leakers may act out of protest, personal gain, or desire for notoriety.

Types of Leakers

- **Conscientious objector:** Opposes the organization's actions, purpose, or philosophies
- **Sympathizer:** Misuses systems to support an external cause without intent to harm the employer
- **Activist:** Strongly motivated supporter of a cause
- **Self-aggrandizer:** Seeks personal publicity or recognition
- **Profiteer:** Sells access or credentials for personal profit.

Careless

Careless insiders account for the largest share of insider incidents, responsible for 56% of events (Ponemon). Phishing alone causes two-thirds of these cases, and 18% stem from credential theft by external groups.

Types of Careless Insiders

- **Reckless:** Deliberately circumvents safeguards for convenience without intent to harm
- **Negligent:** Carelessly or unknowingly compromises assets, often by falling victim to phishing

Disgruntled

Disgruntled insiders are driven by negative triggers that erode their connection to the organization. They can be difficult to identify because the causes are common workplace or life stressors.

Common Triggers

- **Unmet expectations:** Denied promotions, bonuses, or recognition
- **Work events:** Conflict, HR issues, layoffs, reorganizations, or mergers
- **Life events:** Financial stress, divorce, substance abuse, or mental health crises

Opportunists

Opportunists seek to better themselves at the organization's expense. While not always motivated by profit, they may misuse access to advance new ventures, join competitors, or secure a new role internally.

Types of Opportunists

- **Seeking a new job internally:** Misuses data to support candidacy for another role
- **Starting a new company:** Uses proprietary or customer information to gain an advantage
- **Joining a competitor:** Transfers intellectual property or sensitive data for leverage

Thieves

Thieves are motivated purely by profit and will steal any valuable asset, digital or physical. This includes intellectual property, personal data, financial records, or even hardware. They often collaborate with external groups to monetize stolen assets.

Conspirators

Conspirators aim to deliberately harm the organization. Motivations vary, but profit is typically secondary. These actors often operate in coordination with external groups.

Types of Conspirators

- **Competitors:** Seek to damage rivals and gain market advantage
- **Nation-states:** Well-funded actors capable of major disruption
- **Organized crime:** Sophisticated syndicates seeking financial gain
- **Terrorists:** Use violence or extreme actions to advance a political agenda

AI Agents

AI agents are a new type of insider. They can log into systems, access sensitive data, and take autonomous actions on behalf of users. While designed to improve efficiency, they also introduce risk. Misaligned, hijacked, or jailbroken agents may exfiltrate data or act outside intended boundaries. Organizations should treat AI agents as non-human insiders, incorporating them into monitoring, governance, and risk assessments.

Common Insider Threat Events

Insider risks manifest through a variety of harmful actions, whether intentional or unintentional. These events range from data leaks to sabotage and credential theft.

Leak (Unauthorized Disclosure)

Leaking of intellectual property or data. Causes may include carelessness, unfamiliarity with security protocols, circumvention of controls, or intentional disclosure.

Examples include:

- Providing information in a phishing attack
- Sharing sensitive information with unauthorized individuals
- Leaving confidential documents exposed
- Posting confidential details to social media

Misuse

Use of enterprise resources in ways that violate policies, bypass safeguards, or cause harm, whether intentional or not.

Examples include:

- Using enterprise servers for personal gain
- Printing large quantities of personal materials on company printers
- Downloading pirated media to company devices

Using an enterprise server inappropriately for personal gain.Using the enterprise printer to print hundreds of wedding invitations. Downloading pirated movies onto an enterprise laptop.

Fraud

Leveraging insider access to divert financial resources or commit financial crimes.

Examples include:

- Steering contracts to suppliers with personal ties
- Submitting fraudulent expense reports
- Engaging in insider trading using confidential information

Physical Theft

Stealing tangible property rather than digital assets.

Examples include:

- Taking devices such as laptops, servers, or mobile phones
- "Borrowing" equipment without authorization

Violence

Acts of physical harm or threats to individuals or the organization.

Examples include:

- Using threats or violence to coerce employees
- Assaulting a supervisor or colleague
- Making general threats against people or the organization

Sabotage

Deliberate destruction or corruption of enterprise resources, including IT systems.

Examples include:

- Breaking components of critical machinery
- Contaminating a secure environment
- Installing logic bombs or malware in software
- Misconfiguring systems to cause outages

Intellectual Property Theft

Stealing information such as source code, designs, or customer data. Theft may involve copying (enterprise retains access) or removing it entirely (enterprise loses access).

Examples include:

- Downloading design files before leaving for a competitor
- Exfiltrating sales figures, customer lists, or roadmaps

Corporate Espionage

Systematic, targeted extraction of confidential information to benefit a competitor or outside group.

Examples include:

- Selling prototypes to a rival
- Sending confidential personnel files to a handler
- Completing taskings for external actors

Credential Theft and Access Enablement

Credential theft incidents have doubled since 2021, with average costs exceeding $800,000 per incident (Ponemon, 2024). Hackers and ransomware groups often target insider credentials to gain unauthorized access.

Examples include:

- Employees tricked by phishing into revealing credentials
- Insiders social engineered to provide server access
- Insiders advertising access for sale on the dark web

Insider Threat 3.0: The Changing Mindset

Employee loyalty has shifted significantly over the past several decades. In the past, many employees spent most or all of their careers with a single organization. Benefits such as pensions, stable wages, and alignment with company values reinforced loyalty and encouraged employees to prioritize the organization's interests above their own.

Today, loyalty is weaker and more transactional. With pensions replaced by 401(k) plans, outsourcing of jobs, and relatively stagnant wages, employees are more likely to change employers frequently. Many insiders can be described as opportunists who see the "grass is greener" elsewhere. Self-interest has become the dominant factor, and organizational loyalty no longer serves as a natural safeguard against misconduct.

This change has produced two prominent mindsets:

- **Opportunists** focus on advancing their own careers or ventures, often at the expense of the organization.
- **Leakers** not only act out of self-interest but also justify their actions as serving the public interest. Unlike legitimate whistleblowers, leakers often bypass legal channels and disclose sensitive data on their own terms.

A newer and growing concern is insiders who are solicited by external actors to sell credentials or access, often via dark web forums. In some cases, insiders openly advertise their access for sale. This trend is especially dangerous because it involves the use of valid credentials, making detection more difficult. Such incidents often lead to lateral movement and data exfiltration or ransomware attacks.

The risk is particularly acute during employee departures. Departing employees are statistically the most likely to take sensitive data with them. With average tenure dropping to about four years, and closer to two years for millennials and technical staff, organizations face more frequent points of exposure.

A Culture of Disclosure

The way information is shared has changed dramatically. Traditional print and broadcast media once acted as gatekeepers, controlling what reached the public. Today, a fragmented mix of social media platforms, blogs, video channels, and independent voices has replaced that model. Anyone with a social account can now collect, publish, and distribute information.

This cultural shift has created new motivations for insiders to leak information. Platforms such as WikiLeaks not only provide outlets for disclosure but also encourage individuals to collect and publish sensitive material, positioning it as an act of public service. This has contributed to a "leaker mindset," where individuals feel emboldened to take and share information they believe serves a greater good.

The consequences extend beyond government. Corporate insiders have also been influenced by this environment, leading to damaging leaks of proprietary or sensitive business information. Organizations must recognize that cultural factors now play a role in shaping insider behavior, normalizing the idea of disclosure and making it harder to rely on loyalty or discretion as safeguards.

Insider Risk in a Perimeterless Workplace

The workplace has shifted rapidly. Traditional norms of working at a single physical location are giving way to hybrid and remote models. As of the first quarter of 2025, approximately 40% of U.S. jobs offer some amount of remote work.

In a perimeterless environment, data is the new endpoint. Protection can no longer rely solely on physical offices, managed devices, or network boundaries. Instead, security must focus on the data itself, ensuring that information is persistently protected at rest, in transit, and throughout its lifecycle.

Legacy perimeter-based approaches are costly, resource-intensive, and limited in effectiveness. High-profile breaches demonstrate that traditional network defenses are not enough. A modern insider risk model requires shifting attention from guarding the perimeter to monitoring and controlling how insiders interact with data.

This shift is significant. Just before the pandemic, only about 20% of the workforce worked remotely at least part of the time. Now, around one in five Americans work remotely. Managing insider risk in this new environment is significantly more complex than in the traditional workplace.

Compounding Insider Risks

The convergence of shifting mindsets, cultural changes, and new workplace environments has created conditions where insider risk is amplified. Security leaders face these pressures while also contending with limited budgets, staffing, and expertise.

Although many of these changes are outside their direct control, organizations can take practical steps to reduce exposure:

1. **Implement and enforce need-to-know policies.** Limiting access to only what employees require reduces the likelihood of unnecessary data exposure.
2. **Apply role-based access controls.** Standardizing access by role helps enforce least-privilege principles across the organization.
3. **Examine ingress and egress methods**. Evaluate how and where employees access and transfer data, and restrict high-risk pathways.

4. **Monitor insider behaviors and data interactions.** Visibility into how people use data, networks, and systems is essential to spotting risky activity early.
5. **Detect lateral movement.** Monitoring for lateral movement is critical because attackers increasingly exploit legitimate credentials for stealthy access. According to the Verizon DBIR 2025:
   - Credential theft remains a dominant threat, cited as the most common initial access vector, accounting for 22% of breaches, surpassing both vulnerability exploitation and phishing.
   - Among basic web application attacks, 88% involved stolen credentials
   - 60% of breaches involve human interaction—through phishing, credential misuse, or social engineering.
   - Attackers often use valid credentials or built-in tools to pivot and move laterally across the network undetected.

Management Trends

Insider risk management is still a developing discipline. More organizations are now formalizing their programs, broadening training, and exploring new operational models. Several trends stand out as shaping the future of insider risk management:

Formal Insider Risk Programs

You need to think beyond just deploying tools like DLP, SIEM, or user activity monitoring when it comes to insider risk. Many are now creating formal programs led by designated senior executives (often at the SVP or Executive Director level). Formalization includes clear strategies, documented policies, and cross-functional governance, giving programs the authority and structure needed to succeed.

Expanding Training and Awareness

Traditional security awareness training is expanding to cover insider risk. These programs teach employees to recognize behavioral indicators and common triggers, while also emphasizing how to avoid becoming an unwitting insider. Integrating insider risk awareness into existing training builds support and reinforces the importance of the program.

Centralized Operational Hubs

Mature programs are adopting centralized "hubs" that combine insider threat analysts and investigators. This model streamlines triage, accelerates investigations, and improves collaboration between teams. It also supports the refinement of tool policies and rules for more effective detection.

Email as a Persistent Risk

Email is still the most common vector for insider-related incidents. Risks include misdirected messages, phishing, and intentional exfiltration of sensitive data. Organizations are increasingly adopting layered approaches that combine secure email platforms, DLP strategies, and data classification to reduce exposure.

Employee Departures as a Risk Point

Departing employees continue to represent one of the greatest risks to insider data loss. Many organizations are now prioritizing exit workflows, monitoring, and access controls to reduce this exposure. These measures include closer oversight of data transfers during notice periods, more rigorous offboarding processes, and early-warning indicators to identify potential flight risks.

Solutions Over Tools

You should demand more than just tools. They expect guidance on building programs, integrating existing cybersecurity capabilities, and fostering cross-functional collaboration. Effective insider risk management requires solutions that combine people, processes, and technology, not just point products.

Section Three: The Solution

Managing insider risk requires a full-spectrum approach. This includes both technical and non-technical processes integrated into a cross-functional program. This section outlines common objectives, governance frameworks, and metrics for insider risk management, highlighting best practices and a model roadmap for program maturity.

Setting the Stage: Who's on First?

Whether you're running a small business or a global enterprise, protecting your assets, intellectual property, and people should be a primary business objective. Competitors, nation-states, and cybercriminals all seek to exploit innovations and human capital for their own advantage.

Insider risk management requires an ecosystem of cross-functional components. Key starting points include:

Define a Governance Structure

An insider risk program should be overseen by a cross-functional committee that includes the CSO, CISO, CRO, and legal/privacy leaders. Operational governance should be managed by the CSO or CRO as program owner, supported by a working group that provides input and ensures collaboration.

Define the Program

Each organization will tailor its program to its structure and needs, but a solid foundation typically includes:

- Governance and strategy
- Personnel assurance
- Training and awareness
- Asset management ("crown jewel" program)
- Access control
- Monitoring
- Analysis
- Investigation
- Insider risk assessment
- Oversight and compliance

Define the Scope of Insider Risk Management

As established earlier, risk is the combination of impact, threats, and vulnerabilities. Insider risk is the potential harm posed by individuals with authorized access to assets. Organizations should apply this true risk model to prioritize areas of greatest impact.

Insider risk generally falls into three categories:

- **Security risks:** Harm caused intentionally or unintentionally by employees, including negligence, harassment, workplace violence, or malicious action.
- **Productivity risks:** Harm caused by behaviors that reduce efficiency or disrupt business processes.
- **Compliance risks:** Harm caused by violations of laws, regulations, or internal policies.

Leverage Existing Cybersecurity Capabilities

Most organizations already have security capabilities that can support insider risk management, though they may be reactive or siloed. A baseline capability assessment can identify gaps and opportunities. Existing tools such as SIEM, DLP, email security, and web proxies can be tuned for insider-focused use cases.

Define Privacy and Security Equities

Balancing privacy and security is essential. Employees should not be subjected to intrusive monitoring that undermines trust, yet organizations must protect people, information, facilities, intellectual property, and reputation. Policies should apply the least restrictive means possible while still enabling effective risk management.

Goals and Objectives: Measuring Capability

Metrics are essential if you want to manage insider risk effectively. Too often, you may find yourself asking the wrong questions, focusing on activity counts rather than program capability. An insider risk program should aim to protect assets before they are compromised, supported by specific goals in four central domains: Awareness, Understanding, Visibility, and Response.

Awareness

Awareness focuses on building a trusted workforce and a culture of responsibility. Programs should foster transparency, provide resources, and establish workflows that surface behaviors of concern.

Insider Population
Organizations must know who has access to what. This begins with pre-employment screening, continues with ongoing assessments, and includes grouping insiders by access level (e.g., privileged users, Crown Jewel access holders).

Insider Enablement
You need to make sure employees understand how important it is to protect your sensitive assets and how to do it. Training should cover insider personas, common events, and expected behaviors. Clear expectations set during onboarding are critical.

Transparency and Responsibility (H4)
A formal insider risk policy should establish program purpose, structure, and oversight. Employees must understand their responsibilities, reporting options, and duty to protect colleagues and assets.

Risk Workflows
Threat information should feed into cross-functional workflows that identify, assess, and mitigate behaviors that may put the organization at risk.

Understanding

You need a firm grasp of your critical assets and the potential impact if they're compromised. This way, you can prioritize protections effectively.

Crown Jewel and Critical Asset Identification
Create a formal process to define assets, owners, users, access methods, and locations. Crown Jewels are those whose compromise would be catastrophic.

Prioritization
Develop a repeatable methodology to rank assets by impact level.

Movement and Use
Map how assets move and who uses them to understand risk exposure.

Risk Workflows
Incorporate asset information into workflows that guide risk assessment and mitigation.

Visibility

Visibility ensures that insider behaviors, interactions, and asset movements are monitored and analyzed.

Insider Behaviors
Use both technical and non-technical methods to detect concerning behavior. Threat ontologies should align with monitoring tools and be coordinated with privacy/legal review.

Asset Interactions
Monitor how users access, store, and share assets. Establish baselines and alerts for abnormal activity.

Asset Access and Movements
Adopt a data-centric monitoring approach that tracks who accessed which assets, when, and how.

Case Study #1: Can You See Me Now?

Client

A global pharmaceutical company with operations in more than 100 countries.

Problem

As a market leader, the client needed to protect its products, operations, and reputation. Insiders represented the greatest risk, including employees, contractors, and partners. The majority of incidents involved negligent, reckless, or malicious insider activity.

The most pressing challenge was a lack of visibility into how insiders accessed and interacted with critical assets. Without this insight, leadership could not make informed business decisions or adequately protect intellectual property and customer data.

Solution

The client implemented a comprehensive insider risk management program, anchored by the New-Scale Security Operations Platform.

Objectives:

1. Classify normal user and machine behavior across a highly diverse environment.
2. Detect compromised credentials within a trusted insider population.

New-Scale SIEM, powered by behavioral analytics and automation, provided the required visibility. Smart Timelines automatically correlated sequences of activity into contextualized cases, enabling faster, more accurate threat hunting. By aggregating events, logs, HR data, network flows, and threat intelligence, the client gained a unified view of insider behavior across the enterprise.

With this foundation, the client applied Exabeam to multiple use cases, including malicious insiders, compromised users, and advanced persistent threats.

Response

To operationalize the program, the client established an Insider Risk Center of Excellence to centralize alerting, analysis, and response. The hub integrated Exabeam analytics with governance workflows, ensuring that security, HR, and legal teams worked from a unified process.

- **Oversight and compliance:** Quarterly reports and formal metrics kept leadership, privacy, and legal stakeholders aligned.
- **Unified workflows:** Integration of HR, CSO, and CISO workflows provided a single operational picture, reducing duplication and improving efficiency.

As a result, the client not only achieved its initial goals of behavior classification and compromised credential detection but also built a scalable insider risk capability that protects critical assets and business operations worldwide.

A Unified Approach to Risk

Effective risk management requires integration of cross-functional components around a unified strategy and purpose. Too often, threats are treated as separate categories. While each requires unique solutions, all must be managed within a full-spectrum risk management approach.

This strategy must align with a defined risk management process. Strategic directives, goals, and objectives should be logically organized to protect assets. Monitoring for threat information or identifying assets is of limited value unless done through a repeatable process that provides visibility into true organizational risk.

The process involves three steps:

1. Identify the elements of risk (asset impacts, vulnerabilities, and threats) along with supporting factors and indicators.
2. Assess this information in the proper risk management context.
3. Communicate risk information to program personnel and stakeholders to enable mitigation and informed executive oversight.

Identify

Assets

Critical asset identification is foundational. A Crown Jewel Program Manager should be assigned responsibility for maintaining the Crown Jewel Program. This includes collecting and updating asset information semi-annually and incorporating it into an insider risk registry.

Vulnerabilities

Vulnerability reflects the susceptibility of an asset to harm. It is shaped by three factors: ingress, controls, and egress. A designated owner should document vulnerabilities for each critical asset group within a repeatable framework.

Threats

Threats reflect the likelihood that insiders could use authorized access to harm the organization, intentionally or unintentionally. Threat assessment has two components:

- Ability: The level of ingress and egress opportunities available to an insider for a given asset
- Action: Observed behaviors, detected through tools (UAM, DLP), HR investigations, or security investigations

Owners should be assigned to document access levels, monitor alerting behaviors, and record findings across both security and HR sources.

Case Study #2: Departing Employees = Departing IP

Client

A global software company

Problem

Following multiple mergers and acquisitions, the client undertook a corporate restructuring that required significant layoffs. The compressed schedule limited HR and IT's ability to monitor exiting employees. Departing staff pose one of the greatest insider risks, and the client needed a way to identify and prevent unauthorized exfiltration of intellectual property.

Solution

The client used the New-Scale Security Operations Platform to create a watchlist of departing employees. Within this group, more than 10 individuals were identified attempting to leave with corporate data. Exabeam provided detailed activity records, including the exact files downloaded.

HR, IT, and Legal used this evidence to negotiate severance agreements contingent on data being returned.

Exabeam's capabilities—behavioral analytics, Smart Timelines, alert prioritization, and automated incident response—helped the client rapidly detect insider threats, data exfiltration, and lateral movement. Smart Timelines highlighted normal versus abnormal behavior, while risk scoring elevated high-risk alerts to the top of the queue. Automated workflows reduced time-to-respond and minimized errors. The client estimated $450,000 in savings from efficiency gains during this round of layoffs.

Response

The client established an Insider Risk Center of Excellence to assess and communicate insider risk in a structured way:

- **Assess:** Formal risk assessments identified both case-specific threats (e.g., employees attempting to steal IP) and broader program-level gaps. This dual view provided clarity to stakeholders and decision-makers.
- **Communicate:** Risk findings were escalated to executives through an Insider Threat Working Group and shared with legal and privacy stakeholders. Formal reporting processes ensured accountability and oversight, with feedback loops to strengthen governance and improve program maturity.

Building Visibility Into Insider Risk

Visibility is critical to insider risk management, yet many organizations struggle to achieve it due to legal, technical, and process constraints. Effective programs require baseline data points, integrated monitoring, and repeatable processes that place risk information into the proper context for mitigation and oversight.

Asset Management

Identifying and protecting "crown jewels" is foundational. Data sprawl makes this challenging, so structured governance is required.

- **Formulate ground rules:** Implement continuous processes to identify and protect critical assets.
- **Assign crown jewel owners:** Ensure every critical data set has a designated owner responsible for its protection.
- **Map data flows:** Document how data moves across systems and how classifications change as it is transformed.

Data Protection

Security must extend across digital and physical assets, wherever they reside.

- **Persistent:** Apply controls that remain effective across devices, networks, and storage locations.
- **Top-down enforcement:** Apply policies consistently at enterprise, system, and user levels.
- **Granular:** Implement controls at the lowest practical level for maximum precision and governance.

Access Control

Access must be carefully managed to avoid overexposure. Two common risk drivers are excessive privileges and unmanaged devices.

- **Non-hostile threat:** Most insider incidents are unintentional, underscoring the need for visibility across access points.
- **Non-static insiders:** Contractors, partners, and temporary staff must be monitored as they move across roles.
- **Remote employees:** Remote and hybrid work environments increase decentralization and expand access points.

Risk Indicators and Best Practices

Organizations should monitor for key signals that often precede insider incidents.

- **Unauthorized downloads:** Certain downloads, such as encryption tools, should trigger alerts.
- **Recurring threat events**: Divisions with repeated incidents warrant enhanced monitoring.
- **Screen capture and keylogging**: While privacy-sensitive, these tools provide unique insights when used in targeted investigations.
- **Scraping activity:** Large-scale data collection by an insider with legitimate access is a strong risk signal.
- **Employee transitions:** Job searches, résumé updates, and resignation activity are clear early-warning indicators.
- **Access removal:** Procedures must ensure immediate credential revocation for all departing employees and contractors.

Case Study #3: Closing the Back Door

Client

A global apparel company

Problem

The client experienced an increase in data theft from departing employees through cloud-based applications. Inefficient account termination processes left former employees with active access, creating a major vulnerability and exposing the company to data loss.

Solution

The client deployed the New-Scale Security Operations Platform to detect and prevent unauthorized access.

Exabeam integrated with the client's HR system to automatically flag terminated employees and associated accounts.

The platform identified anomalous GitHub activity tied to former employees, alerting security teams to ongoing unauthorized access attempts.

By analyzing user behavior across multiple systems and correlating events, Exabeam prevented further data loss.

The New-Scale Platform uses a risk-based approach that elevates high-risk alerts through risk scoring and behavioral analytics, ensuring analysts focus on the most urgent threats. Smart Timelines automatically stitch together relevant events, enabling faster and more accurate detection of insider threats, data exfiltration, and lateral movement.

Response

With Exabeam in place, the client closed critical gaps in its offboarding process. Security, HR, and IT teams collaborated to streamline account termination procedures, reducing the likelihood of future incidents. The program now incorporates automated account monitoring and cross-functional oversight, creating a stronger safeguard against data theft by departing employees.

Managing Insider Risk Beyond the Perimeter

Remote and hybrid work have made traditional perimeter-based security models less effective. Insiders now access corporate data from home offices, personal devices, cloud platforms, and SaaS applications. To adapt, insider risk programs must shift from protecting locations and networks to protecting data itself wherever it resides or moves.

A modern approach should reframe the four objectives of insider risk management for this environment.

Awareness

Organizations must create a trusted workforce by equipping insiders with resources and training that reflect today's work realities. Training should cover secure behavior in public spaces, proper use of personal and corporate devices, risks of file-sharing sites, and phishing awareness. Reporting mechanisms should extend beyond in-office workflows, including hotlines and digital reporting tools.

Understanding

Critical assets must be identified, prioritized, and mapped to workflows. In the perimeterless workplace, insiders themselves often act as asset holders, storing and transmitting data across personal devices, collaboration tools, and cloud services. Risk models must account for this expanded footprint and include IoT and consumer-grade devices that increasingly intersect with work.

Visibility

Monitoring must extend beyond corporate networks to personal devices, SaaS applications, and open-source data sources. Enterprise mobility management tools can enforce consistent monitoring, while open-source intelligence can surface early indicators of stressors or risks that are less visible in remote environments. Used appropriately, such insights support early intervention while balancing privacy.

Protection

Data is now the endpoint. Protection must be persistent and data-centric, relying on encryption, policy enforcement, and granular controls applied at the asset level. Security measures should safeguard data across its lifecycle—from creation to storage to transmission—regardless of application, device, or operating system.

Three key requirements for protection:

1. **Persistent:** Policies and encryption remain in effect wherever the data moves.
2. **Top-down:** Policies are applied consistently across the enterprise and down to specific users and assets.
3. **Granular:** Controls protect data at the lowest possible level, ensuring security, compliance, and productivity.

Open-source information can provide valuable context in a perimeterless world. Financial records, legal data, and social media activity may reveal stressors or attitudes that indicate potential risk. Used responsibly and in compliance with privacy guidelines, this information can enhance early detection.

Strategic Foundations for Insider Risk Management

Organizations face a changing risk environment, competitive pressures, and the constant need to protect their most valuable assets. Many insider risk management programs are still nascent, leaving organizations vulnerable. Strengthening these capabilities requires a clear, enterprise-wide strategy supported by analytics, governance, and cross-functional collaboration that accounts for both human and digital insiders.

The Approach

An insider risk strategy should treat the organization as a single ecosystem. The workforce now includes employees, contractors, partners, and AI agents. Strategies must explicitly include these non-human insiders in governance models and risk planning, ensuring they are subject to the same visibility, accountability, and controls as human users.

AI agents can interact with enterprise systems, access sensitive data, and even take autonomous actions on behalf of users. While they can increase efficiency, they also create a new category of insider risk. Misaligned, hijacked, or jailbroken agents can misuse valid credentials and permissions just like a human insider.

The strategy should:

- Propose organization-wide goals that transcend individual business units.
- Leverage distributed strengths while enabling bottom-up innovation.
- Align insider risk management with enterprise risk management to support broader business objectives.
- Explicitly include non-human insiders, such as AI agents, in governance, monitoring, and risk models.

As organizations grow, whether through revenue goals, new hires, or acquisitions, the level of insider risk also grows. This challenge creates an opportunity to embed stronger insider risk capabilities as part of institutional strategy. Rather than treating security purely as a cost center, insider risk management should be viewed as a business enabler that protects innovation, people, and brand value.

The Aspiration

The overarching aspiration is to manage the greatest amount of risk at an acceptable cost, while balancing employee and security equities. Two guiding principles support this aspiration:

1. **Focus** – Make insider risk management an enterprise capability aligned with business objectives.
2. **Collaboration** – Build connectivity among stakeholders, breaking down silos and fostering cross-functional integration.

Strategic Directives

A successful strategy should proactively protect assets through four directives:

- **Awareness:** Build a trusted workforce, equip insiders with resources, foster transparency, and establish workflows to surface concerning behaviors.
- **Understanding:** Identify and prioritize critical assets, define asset workflows, and integrate this knowledge into risk models.
- **Visibility:** Monitor insider behaviors, log asset interactions and movements, and analyze patterns to detect risks.
- **Response:** Balance employee and security equities through governance, unified workflows, and efficient risk management processes.

Business Enablement

An insider risk strategy is not only about reducing harm. It enables business outcomes by supporting:

- Employee safety and security
- Protection of corporate assets
- Workforce productivity
- Compliance with external regulations and internal policies

When embedded into business operations, insider risk management strengthens the organization's capacity to innovate, grow, and inspire its workforce.

The Model

The four strategic directives (Awareness, Understanding, Visibility, and Response) are supported by three primary goals. These goals establish the foundation for an insider risk management program.

Build a Framework

Establish the structures, processes, and governance that underpin insider risk management.

- Define governance and organizational structure.
- Create an implementation plan.
- Develop policies, procedures, roles, and responsibilities.
- Identify legal and regulatory parameters.
- Stand up a Critical Asset Management Program.
- Expand monitoring tools to support visibility.

Enhance Capabilities

Strengthen the program's capacity to identify, assess, and mitigate insider risk.

- Increase collaboration between HR, security, and risk functions.
- Create a formal insider risk assessment policy.
- Establish an Insider Risk Center of Excellence.
- Adopt a "zero trust" or "verify then trust" approach to access.
- Build feedback loops for oversight.
- Move monitoring from reactive to proactive.

Optimize Operations

Focus on continuous improvement and measurable outcomes.

- Maintain visibility of critical assets (crown jewels).
- Identify and monitor the riskiest insiders.
- Expand and modernize training programs.
- Improve insider engagement and communication.
- Mature the risk assessment process for a holistic view.
- Expand analytics resources to strengthen detection and response.

The Roadmap

The directive–goal–objective structure provides a logical pathway to implementation. The roadmap translates the model into actionable steps with detailed processes, ownership, and measures of effectiveness.

Build a Framework

Create a clear foundation for program operations.

- **Align strategy and policy with business objectives:** Insider risk must be defined independently from broader cyber risk. Policies should address human, physical, digital, and AI agent insiders alike. Align strategy with business planning and budget cycles.
- **Develop an insider risk ecosystem structure:** Move beyond siloed investigative models. Establish a coordinated cross-functional ecosystem with clear scope, authority, and shared responsibilities.

Core Components

An effective program integrates cross-functional components with defined mission statements:

- **Governance and strategy:** Set objectives, policies, and oversight.
- **Personnel assurance:** Vet employees, contractors, and partners pre-access; monitor for behavioral risks once onboard.
- **Training and awareness:** Deliver ongoing education tied to insider personas and scenarios.
- **Asset management (crown jewels):** Identify, classify, and prioritize critical assets.
- **Access control:** Enforce least privilege; monitor directories and credential systems.
- **Monitoring and analysis:** Correlate data across sources; baseline normal activity; detect anomalies.
- **Investigation:** Scope and resolve incidents within legal and policy limits.
- **Insider risk assessment:** Combine impact, vulnerability, and threat to prioritize risks.
- **Oversight and compliance:** Review regularly for adherence to legal, privacy, and regulatory requirements.

Establish program roles and responsibilities: Assign component owners; create an Insider Threat Director role to lead the Working Group and report to senior leadership.

Clarify legal and regulatory parameters: Work with legal and privacy to define monitoring and investigative authority, balancing employee rights and organizational security.

Develop a critical asset management program: Use automated and manual methods to identify, catalog, and monitor crown jewels. Assign a program manager for continued oversight.

Create an implementation plan: Develop a playbook with milestones, dependencies, and success criteria.

Enhance Capabilities

Strengthen functional capacity through process, policy, and technology.

Fully leverage monitoring and analysis tools: Deploy UAM, UEBA, and DLP in parallel to build a complete view of insider and asset activity. Include AI agents and service accounts in monitoring baselines.

Strengthen HR-Security collaboration: Integrate HR case systems with security workflows; ensure early notification of employee transitions; automate alerts to security.

Develop a formal insider risk assessment policy: Define how signals are collected, assessed, and escalated to decision makers.

Create an Insider Risk Center of Excellence: Centralize triage and analysis functions; maintain playbooks and continuous improvement.

Ensure pre-access vetting: Apply background checks and assurance to all insiders before granting access, including contractors, partners, and AI agents.

Optimize Operations

Mature the program and measure its effectiveness.

Ensure full visibility of the crown jewels: Focus on the most critical assets first, expanding coverage as capabilities mature.

Expand training: Move beyond generic awareness campaigns to include insider personas, use cases, and early indicators.

Foster insider engagement: Communicate expectations clearly, reinforce with consistent policies, and educate insiders on their role in protecting assets.

Develop effective metrics: Create a framework for assessing progress that combines quantitative and qualitative measures, with annual independent reviews.

From Strategy to Solution: The Exabeam New-Scale Security Operations Platform

The strategies in this eBook give you a framework for building and maturing your insider risk management program. To put them into practice, you need technology that unifies your data, applies behavioral analytics, and automates response. You can do that with the Exabeam New-Scale Security Operations Platform, sold as New-Scale Fusion.

New-Scale Fusion

New-Scale Fusion combines log management, behavioral analytics, automation, and AI in a single cloud-native platform. With the New-Scale Platform, you can detect, investigate, and respond to insider threats faster and at enterprise scale.

The platform integrates with your existing environment, including Google Cloud, Google Workspace, and Wiz, so you can correlate detections across both cloud and on-premises systems. This unified view helps you see suspicious behavior in context and respond before an incident escalates.

New-Scale SIEM

New-Scale SIEM gives you cloud-scale log management with fast search and correlation across billions of events. It provides the foundation for visibility into credential use, account activity, and system access. By centralizing this telemetry, you can spot the early signs of credential misuse, privilege abuse, and lateral movement that traditional tools miss.

New-Scale Analytics

New-Scale Analytics applies behavioral analytics to users, entities, and AI agents. Powered by Exabeam Nova multi-agent AI, New-Scale Analytics establishes baselines of normal behavior and uses adaptive risk scoring to surface anomalies linked to high-risk activity. Automated timelines reconstruct events across weeks or months, giving you the context to see how an incident unfolded.

Why New-Scale Fusion Matters for You

By combining these capabilities, the New-Scale Platform lets you:

- Detect insider threats earlier with behavioral analytics and Exabeam Nova agents.
- Investigate faster with automated timelines that connect evidence across systems.
- Respond more effectively with automation that reduces manual effort and human error.
- Correlate detections across cloud and on-prem environments for a complete view of your organization's risk.

New-Scale Fusion operationalizes the four directives from this eBook (Awareness, Understanding, Visibility, and Response) so you can reduce insider risk and protect your most critical assets.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →