A CISO's Guide to Rethinking Insider Risk

The nature of insider risk is evolving. Traditional models focused on malicious, negligent, and compromised employees are no longer sufficient for organizations that are increasingly deploying a digital workforce of AI agents. These non-human insiders operate with trusted credentials and deep access to sensitive systems, creating a new and significant vector for data loss and privilege misuse. This guide provides a modern framework for CISOs to rethink their insider risk programs. It moves beyond a narrow focus on prevention to a more effective, analytics-driven approach. By embracing behavioral detection for both human and non-human insiders, security leaders can gain the visibility needed to distinguish between normal activity and true threats, allowing them to secure their entire workforce and protect critical data from the inside.

Insider risk is one of the most complex and sensitive challenges you face as a cybersecurity leader. While external actors cause the majority of breaches, nearly a third (32%) now involve an internal actor, a steady increase over previous years, according to the Verizon 2025 Data Breach Investigations Report (DBIR).[1] This represents a significant and often underestimated attack vector.

However, many in the cybersecurity community recognize another truth: Insider incidents are often far more costly and damaging. The average cost to remediate an insider-driven incident has now reached $17.5 million, and the total number of incidents has surged by nearly 50% in the last three years.[2] This makes insider risk a significant and pervasive challenge that requires a dedicated strategy beyond traditional perimeter defenses.

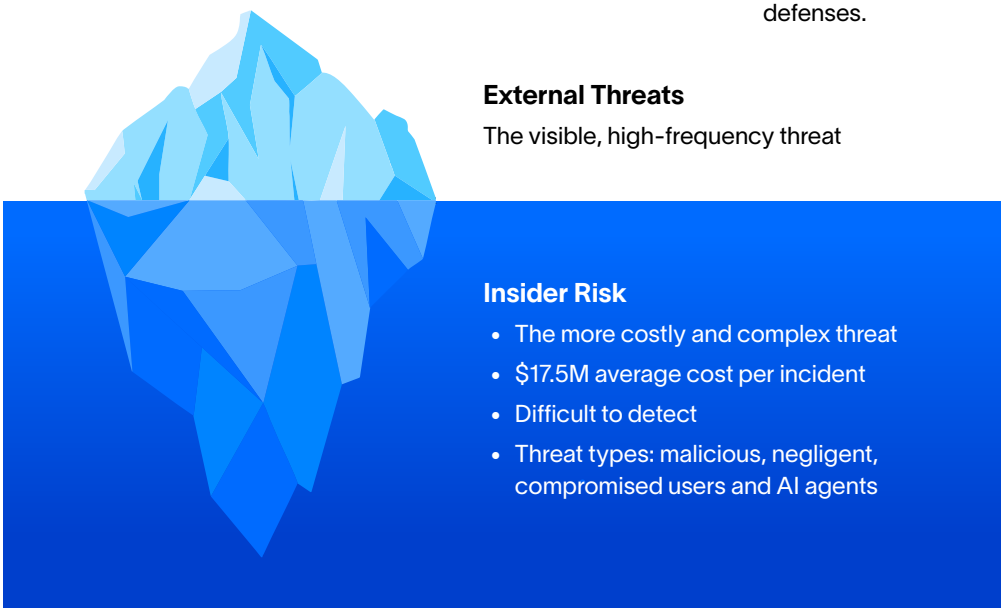

Figure 1. While external threats are more visible, insider risk represents the larger, more costly, and more complex threat to your organization.

[1] Verizon (2025). 2025 Data Breach Investigations Report.

[2] Ponemon Institute (2025). 2025 Cost of Insider Threats Global Report.

Understanding the Modern Insider

Humans are complex, and their circumstances and motivations are prone to constant change. This is the central challenge you must address when building a program to manage insider risk. Most insider incidents are not driven by malice. Rather, they are the result of simple human error, negligence, or credential theft. Understanding the different categories of insiders is the first step toward building an effective detection and response strategy.

The motivations driving intentional insider incidents are more varied than ever. While financial gain remains a significant factor, the 2025 DBIR indicates it is no longer the sole primary driver. Today, insiders are just as likely to be motivated by a personal grudge against the organization. Other critical motivators include espionage (stealing secrets for a competitor or nation-state) and simple convenience or curiosity. Understanding this diverse range of motivations is key to developing a robust detection strategy.

Negligent Insiders

Negligent insiders are individuals with authorized access who unintentionally expose the organization to risk. They may fail to follow security policies, misconfigure a cloud server, or fall victim to a phishing attack. Despite their lack of malicious intent, they are the most common source of insider incidents, responsible for 54% of them.[2]

Compromised Insiders

Compromised insiders are users whose credentials have been stolen by an external attacker. The attacker then masquerades as the legitimate user to gain access to systems and data. This category has seen a steady increase, now accounting for 21% of insider incidents as phishing and other credential theft tactics grow more sophisticated.[2]

Malicious Insiders

Malicious insiders are individuals with trusted access who knowingly and intentionally steal data or cause harm. Accounting for 25% of insider incidents, these individuals often abuse their legitimate access privileges for personal gain.[2]

A Framework for Tracking Insider Behavior

1. Adopt a Formal Framework

Your organization can lean on established frameworks from institutions like the National Institute of Standards and Technology (NIST) and the CERT Division of the Software Engineering Institute (SEI) at Carnegie Mellon University.

2. Implementing Preventative Controls

Preventative controls are a foundational element of any security program. These include identity and access management (IAM), privileged access management (PAM), data loss prevention (DLP), and robust security awareness training. While these controls are essential for reducing risk, they cannot stop every threat, particularly those originating from trusted users abusing their legitimate access.

3. Automate Behavioral Detection

To spot threats that bypass your preventative controls, you need to embrace automated detection. User and entity behavior analytics (UEBA) provides the necessary visibility by ingesting data from across the IT environment to establish a baseline of normal behavior for every user and entity. When an account's activity deviates from its unique baseline, the system generates a risk score and a timeline of the anomalous activity, allowing analysts to quickly determine if it is a credible threat.

This distinction between human and non-human accounts is more critical than ever. The AI agents being embedded in your business represent a new vector for insider risk. Exabeam extends behavioral analytics to this digital workforce by ingesting data from platforms like Google Cloud Agentspace and custom AI applications. We baseline an AI agent's normal behavior just as we would for a human user. When an agent's activity deviates from that baseline, security teams get a clear, contextualized alert to investigate and respond quickly. This closes a critical visibility gap and allows you to secure your entire workforce—both human and digital.

AI Agents: The Emerging Insider Threat

As organizations embed AI agents into business operations, a new class of insider risk emerges. These agents can access systems, handle sensitive data, and take autonomous actions, all while operating with valid credentials and trusted access. If an agent is misconfigured, hijacked, or jailbroken, it can create risks identical to a malicious human insider, including data leakage, privilege misuse, or unauthorized changes. These actions often bypass security tools that depend on static rules and cannot baseline the agent's normal behavior.

Insider Risk is a Shared Responsibility

While you and your security team will own the insider risk program, its success depends on deep, cross-functional collaboration. If leaders and departments operate in silos, it only adds to the complexity and cost when an incident occurs. A transparent charter that delineates roles is essential. Key partners include:

Human Resources

HR must monitor employee behavior and its context. This includes technical indicators, like poor performance reviews, but also non-technical ones, such as attitude changes. HR can communicate these potential risk indicators to the security team to help create watchlists and establish appropriate courses of action. Impending layoffs or contractors nearing the end of their engagements represent other real risk scenarios that require monitoring.

Legal

The legal department is critical when an incident has regulatory or compliance implications. Legal must help the security team understand the circumstances under which an incident must be escalated. For example, at what point does an event become a breach that requires external reporting? Legal also advises on employee privacy protections relative to security policy.

Business Leadership

Standalone insider threat programs may report to a Chief Risk Officer or a fraud team. For larger organizations, an incident may also necessitate action from the physical security team.

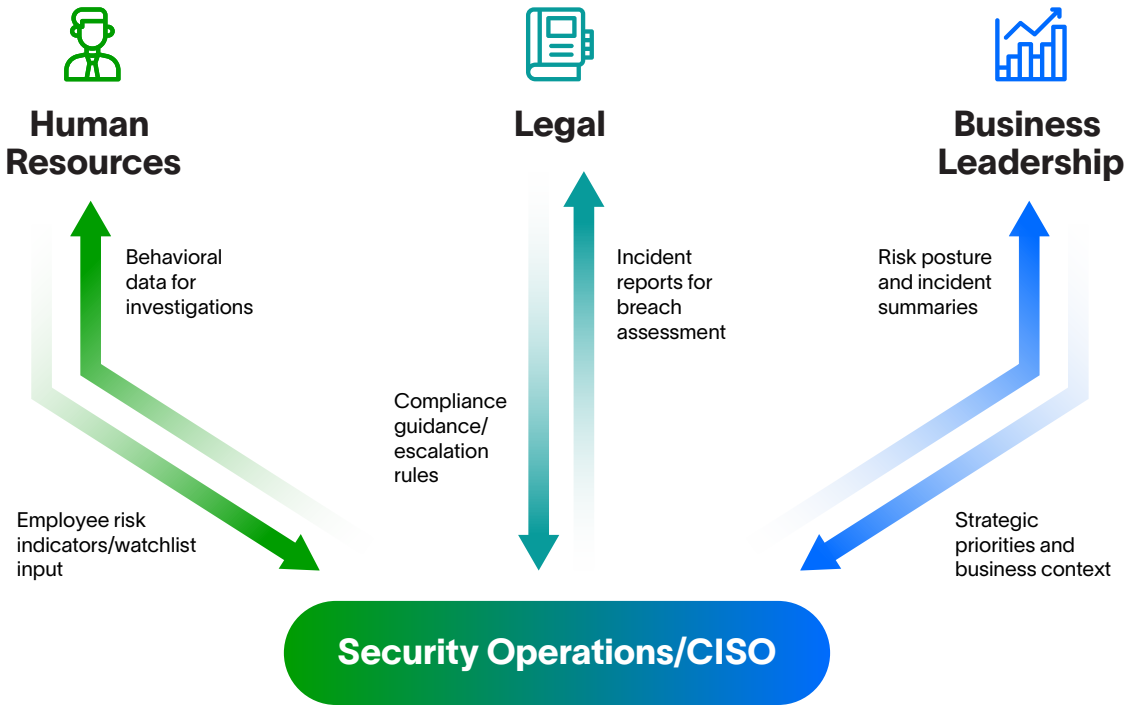

Figure 2. An effective insider threat risk program requires a collaborative framework built on a constant flow of communication between Security, HR, Legal, and Leadership.

Benefits of a Collaborative Framework

A formal, collaborative charter serves several significant goals that strengthen an organization's security posture.

Empower the CISO

The perception of the CISO as the sole arbiter of cybersecurity can be a vulnerability. When the responsibilities of cybersecurity are shared by an executive steering committee and communicated effectively, it enhances employee confidence and reinforces a culture of shared ownership.

Enhance Prevention

When HR identifies employees associated with known insider threat indicators—such as disputes, negative performance feedback, or financial distress—they can be added to an internal watchlist. This process, governed by clear policies, allows for heightened monitoring of potential high-risk individuals. Clear lines of communication between the CISO, HR, Legal, and senior leadership are essential for this to be effective and fair.

Augment Detection

The CISO can share aggregated data that defines normal and abnormal insider behavior. This can aid other departments in their own investigations without violating the confidentiality of the employees in question.

Building a Multi-Year Plan

The best insider threat programs are defined by key characteristics:

- Collaborative and interdisciplinary
- Coordinated by well-defined playbooks and charters
- Co-funded amongst participants
- Guided by a cohesive multi-year plan to continuously improve performance

A successful plan should include:

Touchpoints

At the executive level, senior leaders included in this charter should meet quarterly or biannually. At the team lead level, more frequent engagements will allow participants to share intelligence and best practices related to recent incidents.

Tangible Assets

An intelligence brief or similar asset should result from these touchpoints and be presented to an executive chairperson annually. Year-end summaries should include data visualization to demonstrate investigation triggers and how incidents are resolved, proving the program's value.

From Fear to Focus

Managing insider risk requires a programmatic approach guided by a cohesive multi-year plan to continuously improve performance. By augmenting your preventative controls with automated behavioral detection, you can move from a state of fear and uncertainty to one of focus and control. Modern, collaborative security operations are central to this cultural shift, helping to reinstate trust across the organization by providing the context and visibility needed to separate real threats from normal business activity.

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 →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.

2025 Exabeam, LLC. All rights reserved.