COGILITY

2025

INSIDER RISK REPORT

The Shift to Predictive Whole-Person Insider Risk Management

Research by

Cybersecurity INSIDERS

Overview

Insider threats have evolved into sophisticated, persistent risks—and most organizations remain dangerously underprepared. With the rapid rise of remote work and widespread adoption of AI-driven tools, the challenge has shifted from detecting isolated suspicious actions to proactively understanding human intent, pressures, and context before damage occurs. Yet despite broad awareness of these growing risks, many insider threat programs remain fragmented, reactive, and narrowly focused on technical indicators. Without deeper behavioral insights, security teams continue to miss critical early-warning signs that could prevent breaches. To explore how cybersecurity leaders are addressing these escalating insider threats, Cybersecurity Insiders surveyed 635 CISOs and cybersecurity professionals in early 2025. The findings reveal a stark disconnect between recognizing insider threats and having the practical tools, processes, and maturity to manage them proactively. Critically, they highlight the urgent need to move beyond reactive monitoring toward integrated, predictive, whole-person intelligence.

Key findings include:

1. **Insider threats have outpaced defenses:** Ninety-three percent of respondents say insider threats are as difficult or more difficult to detect than external cyberattacks. Yet only 23% express strong confidence in their current ability to detect insider threats before significant damage occurs—a capability gap that leaves many organizations highly vulnerable.
2. **Behavioral signals remain underutilized:** Just 21% of organizations extensively integrate behavioral indicators such as HR signals, financial stress, and psychosocial context into their detection programs. Without these insights, insider threat management is limited to technical anomalies, causing teams to miss critical early-warning signs.
3. **Predictive analytics are lacking:** Only 12% have mature predictive risk assessment models capable of proactively identifying insider threats. Most organizations still rely on reactive alerts after incidents occur, missing crucial opportunities for early intervention.
4. **Key obstacles block progress:** Inadequate tools (71%), insufficient budgets (69%), and privacy concerns (58%) are cited as the top barriers preventing organizations from advancing their insider threat management programs.
5. **AI tools amplify insider risks:** Sixty percent of organizations express high concern about the misuse of AI tools by insiders. Leading worries include deepfake phishing and social engineering (69%), automated data exfiltration (61%), and AI-assisted credential abuse (53%).

These findings clearly underscore the urgent need to transform insider threat management programs from reactive, fragmented approaches into proactive, predictive models capable of anticipating and preventing incidents. The following chapters explore precisely where current efforts fall short, why behavioral and contextual insights are crucial, and how a whole-person intelligence approach can help organizations move decisively from awareness to effective, preventive action.

01

The Insider Threat Confidence Gap

While organizations widely acknowledge insider threats as critical, complex risks, there's a significant gap between awareness and preparedness. This chapter explores how a lack of confidence, driven by challenges in threat detection and the inherent complexity of insider behavior, leaves organizations vulnerable. Understanding these confidence gaps and vulnerabilities sets the stage to explore exactly why organizations struggle to build effective insider threat management programs.

Key Findings:

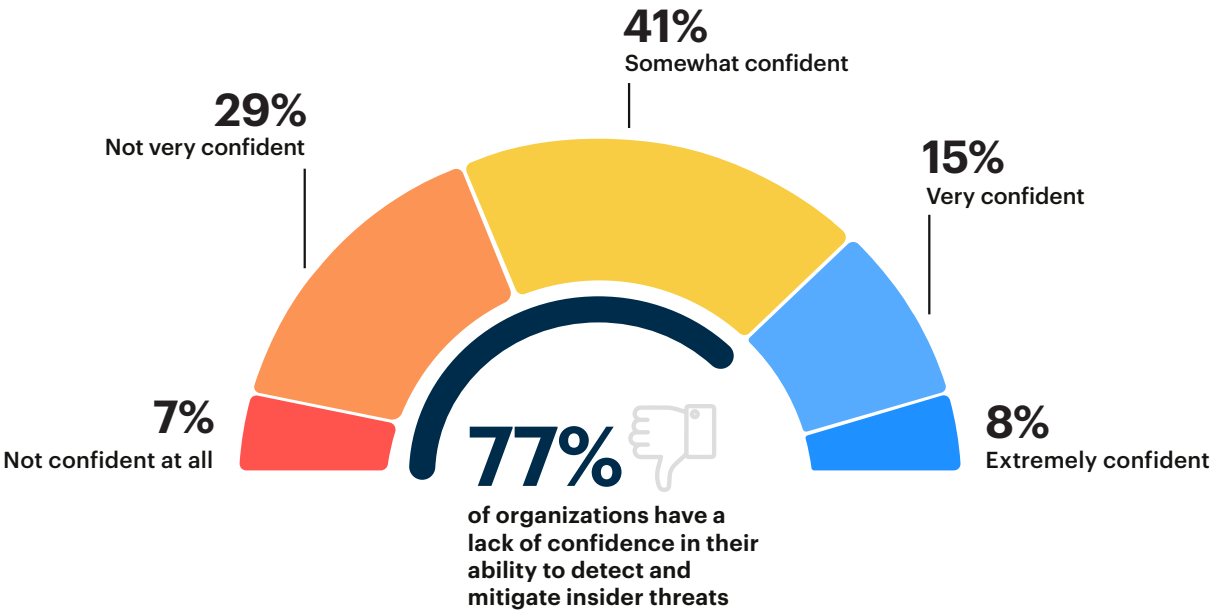
- **Confidence in detection remains critically low:** Only 23% of organizations strongly believe they can detect and prevent insider threats proactively, despite recognizing their severity.
- **Insider threats are increasingly complex:** 93% of respondents find insider threats as difficult or harder to detect than external cyberattacks, highlighting that traditional defenses fall short.
- **Employees perceived as vulnerable under pressure:** A majority (66%) believe a substantial portion of their workforce could be susceptible to insider threats if incentivized or under personal stress, amplifying organizational risk.
- **Privileged roles represent higher potential risk:** IT administrators (83%), third-party vendors (77%), and executives (64%) top the list due to elevated access—emphasizing that privileged access, in addition to malicious motivational factors, drives insider threat risk.
- **Internal failures have external consequences:** Nearly half (49%) report discovering insider-related data, credentials, or sensitive information exposed on the dark web, underscoring tangible impacts from internal detection gaps.

Most Organizations Doubt Insider Threat Readiness

Detecting insider threats before they cause harm is a benchmark of cybersecurity maturity—yet few organizations feel genuinely prepared. This finding sets a clear tone for the broader report: insider threat awareness is widespread, but capabilities are lagging.

Just 8% of respondents describe themselves as "extremely confident" in their insider threat defenses, and fewer than one in four (23%) express strong confidence overall. Meanwhile, a significant majority (77%) lack confidence to varying degrees, including 41% who are merely "somewhat confident" and 36% who openly report low or no confidence. This underscores that most programs remain stuck in a reactive state, limited by fragmented data, insufficient behavioral insight, and slow escalation paths.

How confident are you in your organization's ability to detect and mitigate insider threats before significant damage occurs?



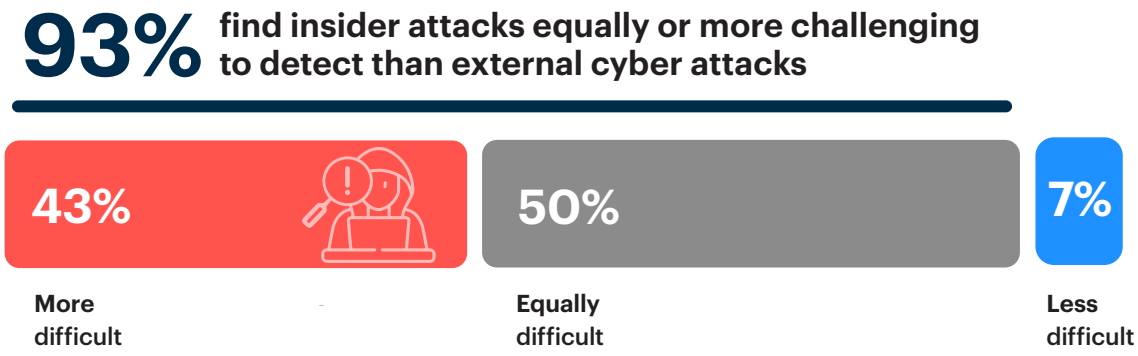
Consider a privileged user quietly downloading sensitive files over time. Without behavioral context—such as recent financial stress or HR-related concerns—their actions appear routine in security monitoring tools. By the time an anomaly is flagged, critical damage may already be done. The issue here isn't insufficient tooling; it's the absence of integrated behavioral visibility needed to proactively detect threats.

Organizations need more than surface-level monitoring. They require behavioral and contextual intelligence to recognize, not just observe, early warning signs. This is precisely where traditional approaches fall short and where the whole-person model becomes essential.

Insider Attacks Are Harder to Stop

The low confidence in insider threat defenses we've just seen is partly explained by the complexity that security teams face when detecting these threats. Nearly half of respondents (43%) say insider attacks are more challenging to detect and prevent than external cyberattacks, while another 50% see them as equally difficult. Only a small minority (7%) view insider threats as less difficult. Clearly, insider threats now rival—and often surpass—external threats in complexity, posing unique challenges for defenders.

How does your organization perceive the difficulty of detecting and preventing insider attacks compared to external cyber attacks?



Why is insider threat detection so challenging? Because insiders typically operate within their authorized access, their actions—malicious or accidental—often appear normal in standard security logs. Technical monitoring alone struggles to distinguish routine behavior from genuine threats without clear signals of intent, stress, or changing circumstances.

Imagine an employee accessing sensitive files at odd hours shortly after a negative performance review or missed promotion. Technically, they haven't broken explicit security policies. Without additional context—such as recent HR concerns or noticeable shifts in behavior—security systems tuned purely to detect technical anomalies would likely miss this as a potential threat. By the time traditional tools raise an alarm, critical damage might already be done.

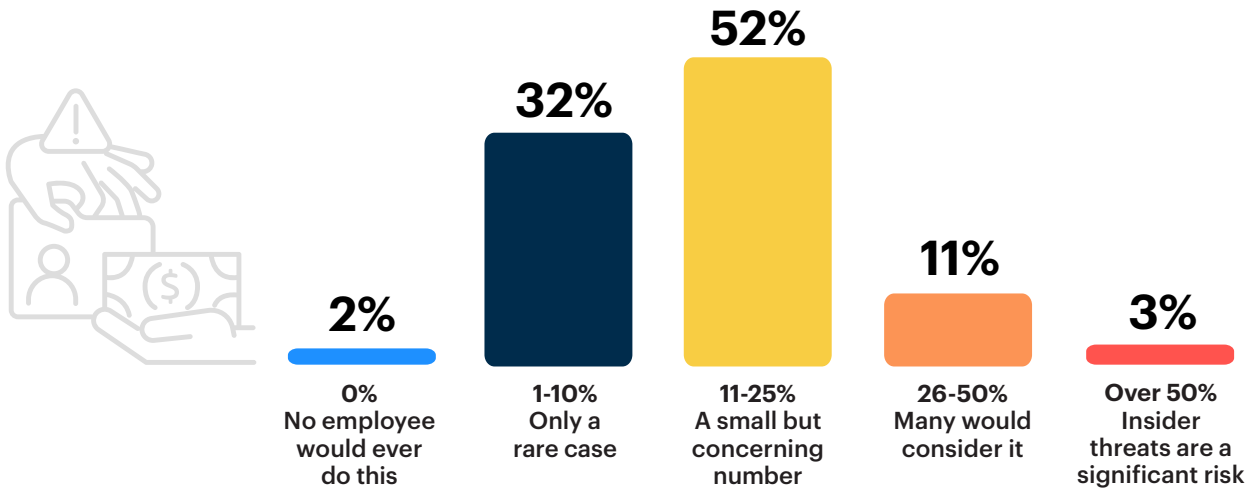
This scenario highlights a fundamental limitation: insider threat detection isn't just about better tools or more alerts. It's about gaining clear visibility into context, intent, and human factors behind user actions. To effectively address this challenge, organizations must integrate behavioral insights with technical monitoring, creating a proactive defense capable of identifying potential insider threats before damage occurs.

Insider Risk Potential: A Window of Opportunity

While insider threats are challenging to detect, understanding why employees might act is equally critical—and delicate. This question explores cybersecurity leaders' perceptions about employee susceptibility under hypothetical circumstances, such as significant financial incentives and guaranteed anonymity. Importantly, this data reflects perceived vulnerability, not predictions of actual malicious actions.

Only 2% of respondents feel their workforce is entirely resistant to such incentives. A majority (52%) estimate that 11%-25% of employees could potentially be influenced, with another 14% suggesting an even higher level of vulnerability. Altogether, 68% of respondents believe more than one in ten employees could theoretically succumb under intense pressures or incentives. This underscores a nuanced understanding of insider risk: that even trusted insiders might become vulnerable when experiencing significant personal stressors or unusual pressures.

If given a large financial incentive and guaranteed not to get caught, how likely would employees in your organization be to sell sensitive information to an outsider?



The challenge for insider threat programs, then, is moving beyond surface-level detection to proactively understand these pressures and vulnerabilities before they escalate into actual risk behaviors. While HR outreach and employee-assistance programs have their place, effective insider threat management fundamentally depends on integrating a broader set of indicators. By combining HR data, financial stress signals, legal concerns, behavioral anomalies, and technical indicators into a unified real-time view, organizations can proactively identify employees at risk before intent becomes action. For example, subtle signals such as sudden financial difficulty, escalating workplace conflicts, or suspicious changes in work habits can be surfaced through an integrated, real-time behavioral analytics model. Such a comprehensive approach provides security teams with critical early warnings and actionable context—enabling intervention strategies precisely targeted at emerging risk, without relying solely on reactive alerts.

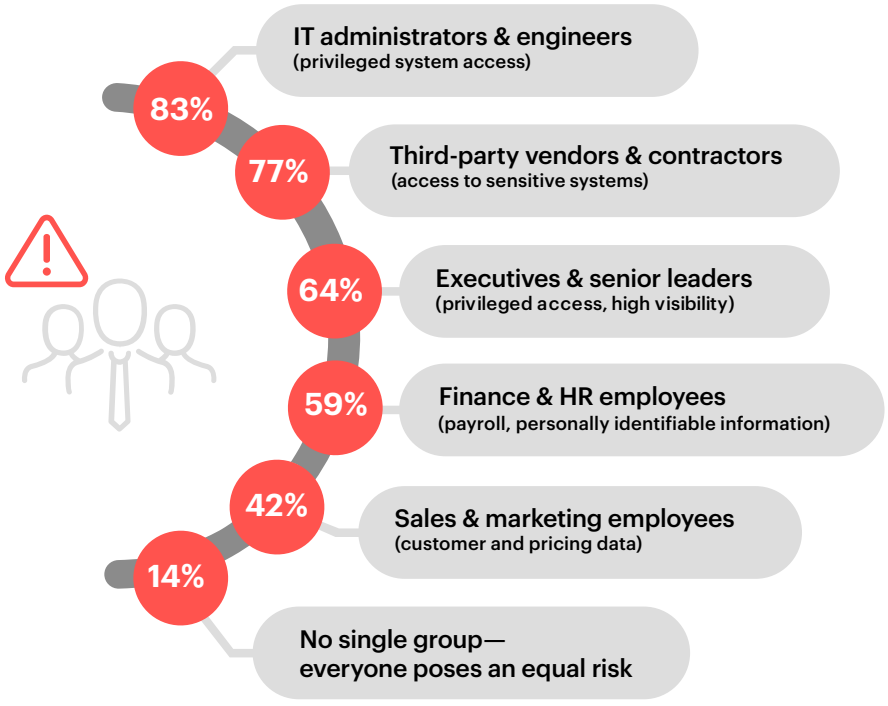
This holistic approach, integrating multiple dimensions of human context with traditional security data, moves insider threat management from reaction toward prevention, addressing potential vulnerabilities before they evolve into actual incidents.

Privileged Access Fuels Insider Risk

While any employee could theoretically pose an insider threat, certain roles inherently have greater potential due to their elevated privileges and access—not necessarily because they're more likely to act maliciously. Respondents identify IT administrators and engineers (83%) as having the greatest potential, followed closely by third-party vendors (77%), executives (64%), and finance/HR personnel (59%). Even sales and marketing employees (42%) appear prominently, reflecting broad recognition that insider risk follows privilege, not job titles alone.

Interestingly, 14% of respondents indicate no single group stands out, reinforcing that insider threats can emerge from anywhere. Effective insider risk management therefore requires dynamic monitoring based on actual behaviors and access patterns rather than static assumptions tied to organizational roles. By integrating behavioral context with technical monitoring, organizations can proactively identify insider risks—regardless of position—and intervene before damage occurs.

Who within your organization poses the greatest insider risk?



Insider Exposure Surfaces on the Dark Web

Insider threats may begin internally, but their impact often becomes public—sometimes surfacing on hidden corners of the internet. This question examines how frequently organizations detect insider-related information exposed on the dark web.

Nearly half of respondents (49%) confirm finding sensitive company credentials, intellectual property, or internal communications exposed online—with 10% experiencing this frequently. Another 28% haven't yet discovered such breaches but actively monitor the dark web for signs. Meanwhile, 18% aren't monitoring at all and 5% remain unsure. Clearly, insider-driven exposures aren't just theoretical; they're a real and ongoing concern.

Has your security team ever found your company's credentials, intellectual property, or insider discussions on the dark web?

Not sure 5%

Discovering compromised data externally signals more than just data leakage—it indicates failures in earlier detection. Often these breaches result from overlooked behavioral signals like escalating personal stress, changes in employee access patterns, or misuse of emerging technologies such as AI tools. Traditional security monitoring alone rarely catches these subtle early indicators.

Organizations should shift from relying on dark web discoveries as their reactive detection method to adopting proactive measures that integrate behavioral, technical, and contextual signals. By tracking and interpreting early warning signs internally, security teams can identify potential insider threats sooner—before sensitive information ever reaches external platforms.

02

Breaking Through Barriers to Proactive Insider Risk Management

As Chapter 1 showed, organizations widely recognize insider threats as significant yet struggle with confidence and preparedness. This chapter reveals precisely why those readiness gaps persist—highlighting common barriers like insufficient tools, constrained budgets, privacy concerns, and a reactive mindset. Recognizing these systemic barriers makes it clear why traditional monitoring alone has proven insufficient—highlighting the need to integrate deeper behavioral insights.

Key Findings:

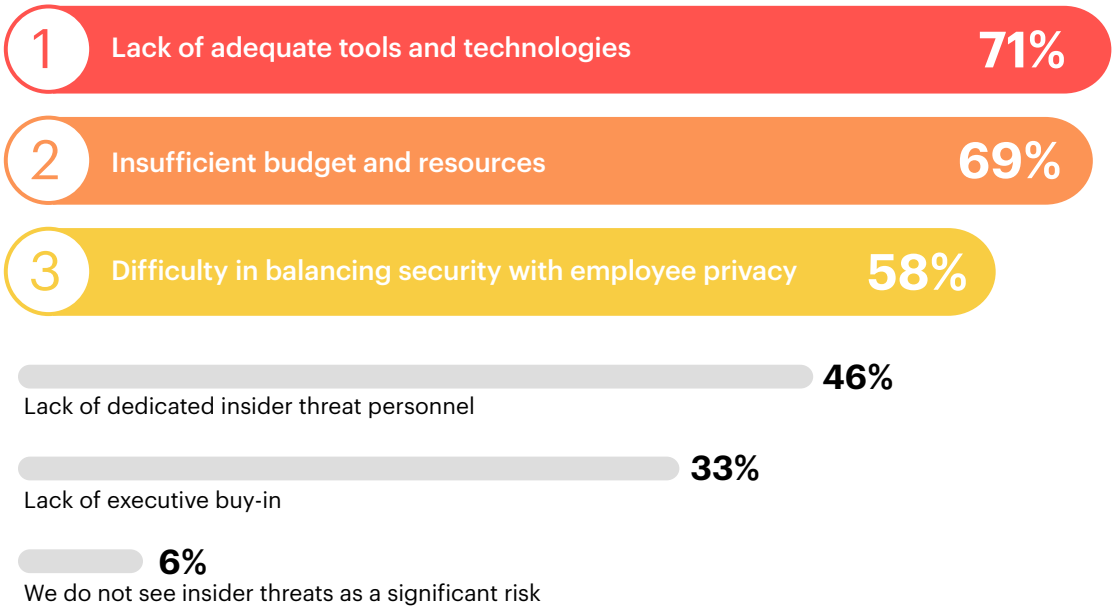
- **Tools, budgets, and privacy concerns block progress:** Organizations identify inadequate tools (71%), budget constraints (69%), and privacy or legal challenges (58%) as the primary obstacles to advancing insider threat management.
- **Incident response planning is limited and reactive:** Only 27% of organizations have a detailed insider threat response plan, while 69% rely on informal approaches or have no plan at all, leaving most organizations unprepared for insider threats.
- **A proactive mindset is missing:** Effective insider threat management must shift focus from responding to attacks after harm occurs toward proactive detection and intervention at the earliest signs of emerging risk.
- **Behavioral and contextual integration is key:** Organizations need integrated workflows combining technical, HR, behavioral, and contextual insights, moving insider risk management from incident reaction to risk mitigation.

Key Obstacles to Better Insider Risk Management

If organizations clearly see insider threats as high-impact risks, why is improvement slow? The survey data clarifies what holds them back: insufficient tools (71%), limited budgets (69%), and privacy concerns (58%) top the list, reflecting a combination of technical and organizational hurdles.

Legacy systems often can't effectively correlate technical and behavioral indicators in real time, leaving security teams without critical context. Budget limitations frequently push insider threat initiatives behind more visible external security projects, even as internal risks grow. Privacy and legal concerns complicate efforts further, making many organizations hesitant to integrate sensitive behavioral, HR, or legal data into their detection processes.

What are the 3 biggest obstacles preventing your organization from improving its insider threat management program?

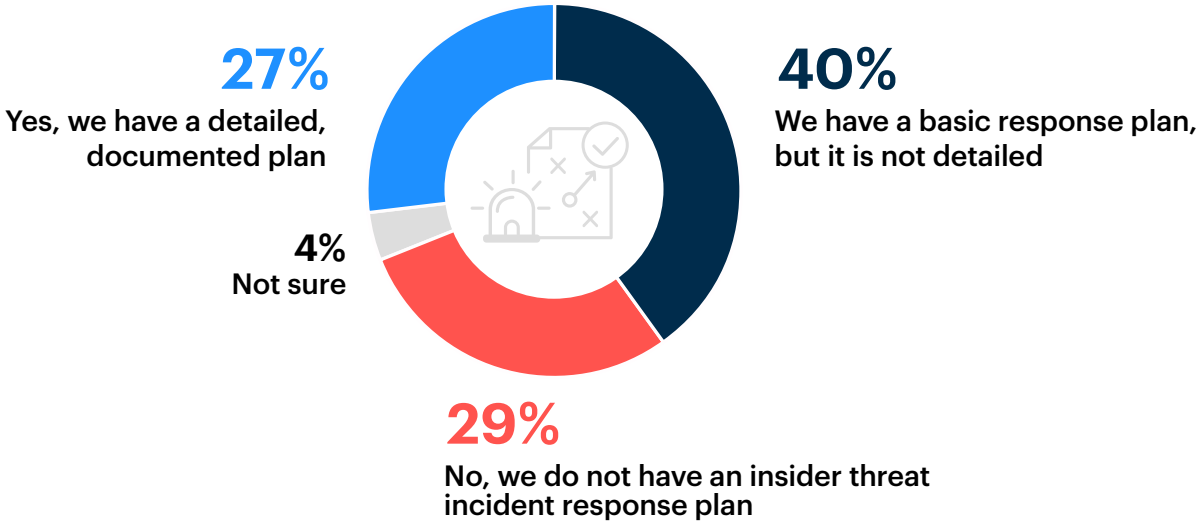


These barriers illustrate why insider threat management remains mostly reactive and surface level in many organizations. To progress, security teams need solutions designed specifically to overcome these integration, resource, and privacy hurdles—enabling them to interpret early risk signals without disrupting operations or violating internal policies.

From Attack Response to Risk Prevention

Given the complexity and likelihood of insider threats, structured response planning should be a baseline—but most organizations remain significantly behind. Only 27% of respondents have a detailed insider threat response plan. Another 40% rely on a basic or informal plan, while 29% have no plan at all. Clearly, many organizations lack clear guidance on insider threat management.

Does your organization maintain an insider threat incident response plan?



Yet the real issue isn't just the absence of an incident response plan focused on handling attacks after they occur. It's that many organizations lack proactive planning aimed at responding to insider risk signals before an incident ever takes place. A truly effective insider risk program is preventive—designed to identify and address potential threats early, guided by subtle behavioral indicators and context, rather than merely responding after harm is done.

This proactive approach requires integrated workflows that combine technical alerts with HR, behavioral, and contextual intelligence, enabling organizations to recognize emerging risks and intervene decisively before they escalate. Whole-person intelligence supports this shift from reactive attack response to proactive risk prevention, providing teams with critical early warnings to act on vulnerabilities and behavioral shifts before damage occurs.

03

From Monitoring Activity to Understanding User Behavior

Chapter 2 outlined critical barriers preventing organizations from proactively managing insider threats. Now we dive deeper into the specific monitoring and intelligence gaps behind these barriers. This chapter examines how organizations currently monitor and analyze insider threats—and highlights the urgent need to evolve insider threat programs from reactive monitoring towards proactive behavioral prediction.

Key Findings:

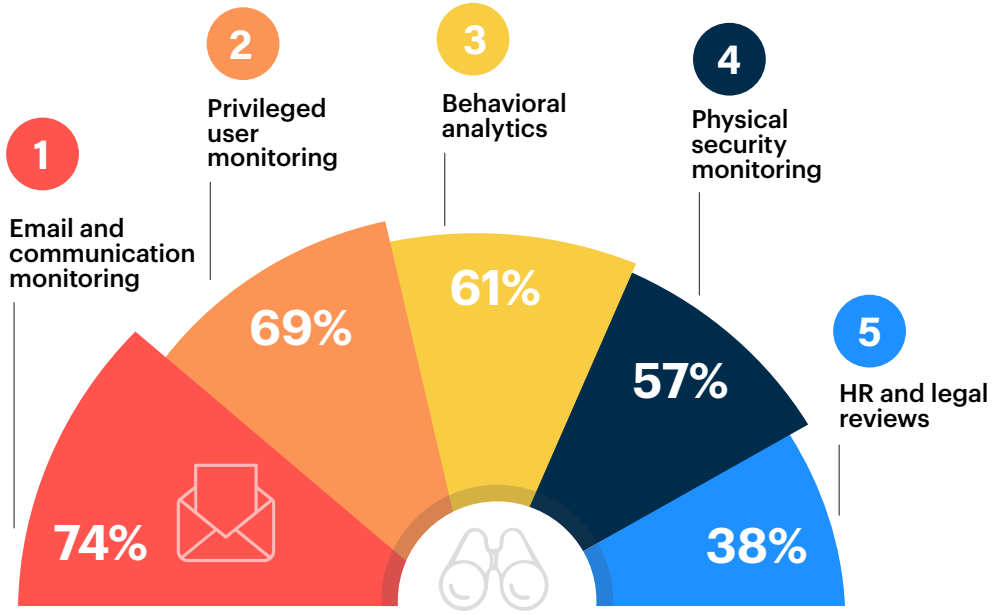
- **Technical signals dominate insider monitoring:** Organizations mainly rely on email monitoring (74%), privileged user oversight (69%), and basic behavioral analytics (61%), but few meaningfully integrate deeper behavioral context.
- **Behavioral intelligence remains underutilized:** Only 21% of organizations extensively incorporate behavioral indicators, such as HR data or financial stress, into their detection programs, leaving many insider risks undetected or misunderstood.
- **Critical human signals often go unnoticed:** While common behavioral signals like erratic behavior (65%) and HR-related issues (58%) are monitored, deeper predictive signals—including financial pressures (32%) and legal issues (19%)—remain significantly overlooked.
- **A need for integrated, actionable intelligence:** Organizations should shift from reactive, technical monitoring to proactive, behaviorally informed analysis, enabling earlier, clearer insights into insider risk.

Monitoring Without Behavioral Context Falls Short

While many organizations have insider threat monitoring in place, most still rely heavily on technical and transactional signals. This survey question, asking about the type of insider risk monitoring that organizations conduct, highlights a significant gap: the limited inclusion of deeper, contextual behavioral data.

Respondents primarily monitor email and communications (74%), privileged-user activity (69%), and basic behavioral analytics (61%). Physical access controls (57%) also rank highly. However, fewer than four in ten (38%) integrate HR or legal data into their monitoring. Even when organizations use behavioral analytics, these typically focus on technical anomalies—not human factors like workplace grievances or financial pressures.

What type of insider risk monitoring does your organization conduct?



We do not conduct insider risk monitoring 8% | Other/not sure 3%

This limited integration means many insider threat programs detect suspicious activities but fail to understand why they're occurring. Technical alerts alone—such as email spikes or unusual logins—rarely indicate whether someone poses a genuine threat or simply triggered a false positive.

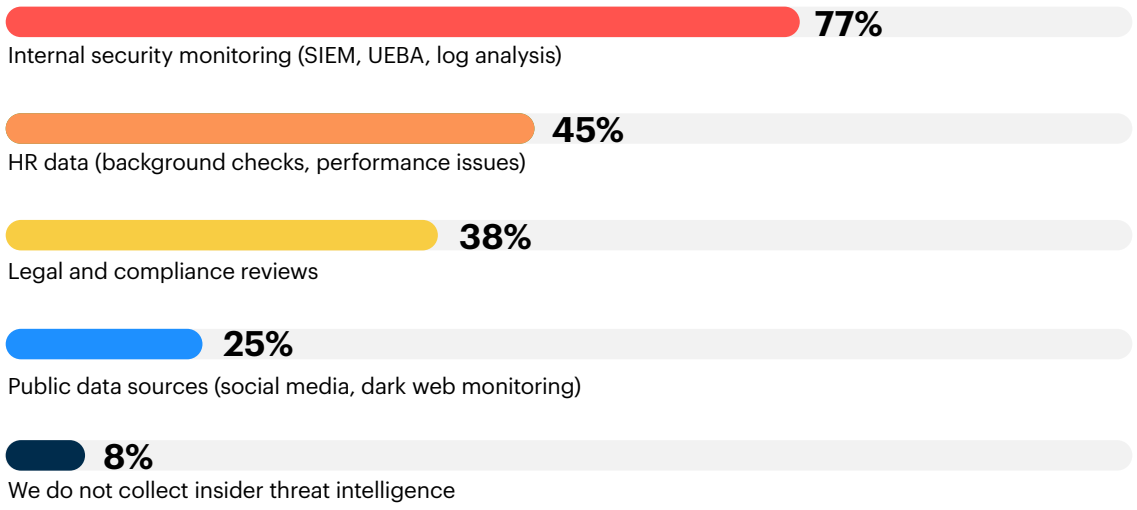
Organizations should expand their monitoring beyond purely technical indicators to incorporate relevant human factors and early warning signals. Integrating richer, contextual data streams—such as HR indicators, workplace stressors, and related behaviors—enables security teams to differentiate minor anomalies from genuine insider threats and to intervene before actual harm occurs.

Intelligence Feeds Lack Behavioral Depth

Beyond deciding what to monitor, how organizations collect and analyze insider threat intelligence critically impacts their ability to manage risk effectively. While technical data remains dominant, many organizations still overlook behavioral and contextual signals crucial for detecting insider threats early.

Most organizations (77%) rely heavily on internal technical telemetry—such as SIEMs, UEBA, and system logs—as their primary source of threat intelligence. However, fewer than half incorporate HR data (45%) or conduct legal and compliance reviews (38%), and only 25% leverage public sources like social media or dark web monitoring. This imbalance underscores a common shortcoming: organizations focus primarily on technical indicators, rarely capturing the human factors and stressors that precede insider incidents.

How does your organization collect and analyze insider threat intelligence?



Technical data effectively answers "what" happened, but rarely provides insight into "why" it occurred. Without structured analysis of HR records, legal actions, or publicly available information, organizations miss critical opportunities to detect early-stage risk behaviors.

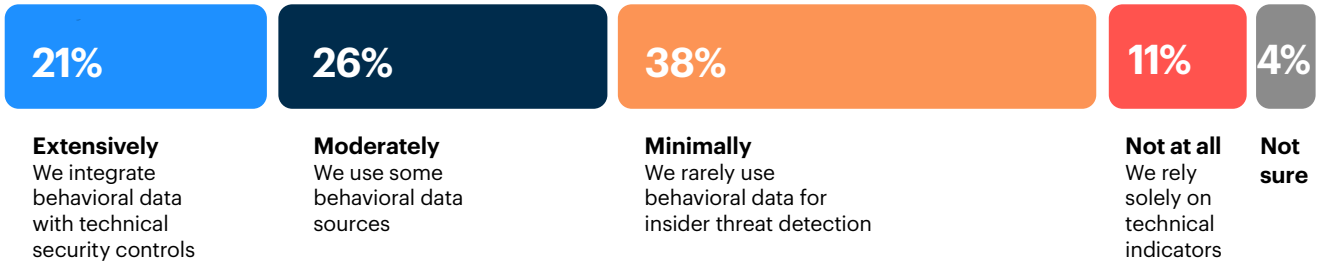
By integrating these broader behavioral and contextual sources with traditional technical logs, organizations can shift from reactive investigation to proactive anticipation—identifying emerging insider threats earlier, understanding their root causes, and intervening before damage occurs.

The Missing Link: Behavioral Insights

Building on the limitations of purely technical indicators, behavioral data is essential to understand not just what happened, but why it occurred. Despite recognizing the importance of human factors, most organizations still rely heavily on technical indicators—leaving critical behavioral data largely underutilized.

Only 21% of respondents say their organizations extensively integrate behavioral data (such as HR issues, financial stress, or social media signals) into their insider threat detection programs. Another 26% report moderate integration, but nearly half (49%) acknowledge minimal or no behavioral data use at all. This illustrates a significant gap: insider threats are widely recognized as driven by human factors, yet detection practices remain reactive and technical.

To what extent does your organization incorporate behavioral date (e.g., HR data, legal records, financial stress indicators, social media activity) into insider threat detection?



Without behavioral context, security teams often see only isolated events like unusual data downloads or off-hours system access. But lacking deeper insights—such as an employee's recent HR issues or escalating personal stress—teams struggle to interpret these events accurately or promptly.

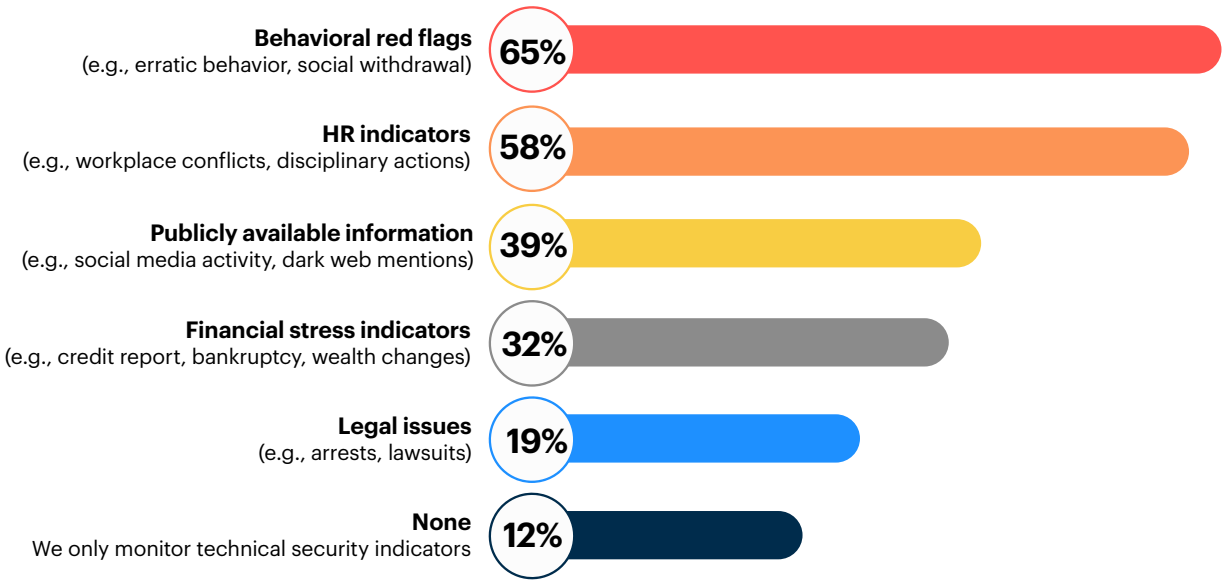
Closing this gap requires organizations to elevate behavioral data from supplemental to central in their detection strategy. By systematically integrating human-centered signals alongside technical alerts, security teams gain critical predictive capabilities—enabling earlier identification, clearer understanding, and more effective prevention of insider threats.

Critical Human Risk Signals Remain Overlooked

While behavioral data integration remains limited, even when organizations do monitor non-technical indicators, they frequently overlook some of the most predictive and actionable signals—particularly those related to financial, legal, and external factors.

Sixty-five percent of organizations monitor basic behavioral indicators like erratic behavior or social withdrawal, while 58% track HR-related issues such as workplace conflicts or disciplinary actions. Yet fewer organizations incorporate deeper and often more predictive indicators: only 39% monitor publicly available data (such as dark web or social media activity), just 32% track financial stress signals, and a mere 19% include legal concerns like lawsuits or arrests in their monitoring efforts.

What types of non-technical indicators does your organization monitor to assess insider threats?



The limited attention given to these powerful indicators leaves security teams without early warnings of potential threats. Issues like sudden financial changes, mounting debts, or legal troubles frequently precede insider incidents, yet often remain hidden without deliberate monitoring.

To address this gap, insider threat programs should extend their monitoring beyond basic internal observations and technical telemetry. By systematically capturing and analyzing deeper financial, legal, and external behavioral signals, organizations gain critical early visibility into emerging insider threats—enabling timely, precise interventions.

04

From Detection to Proactive Mitigation – The Case for Whole-Person Intelligence

Having identified significant monitoring gaps in Chapter 3, we now explore how adopting a whole-person intelligence model can close those gaps, shifting insider threat management from reactive detection to proactive anticipation. This chapter identifies the core obstacles preventing organizations from shifting insider threat programs from reactive detection to proactive risk prediction—highlighting structural, privacy, integration, and maturity challenges that continue to stall progress. Adopting whole-person intelligence is no longer optional; it's essential, especially given how emerging threats like AI misuse are reshaping insider risk.

Key Findings:

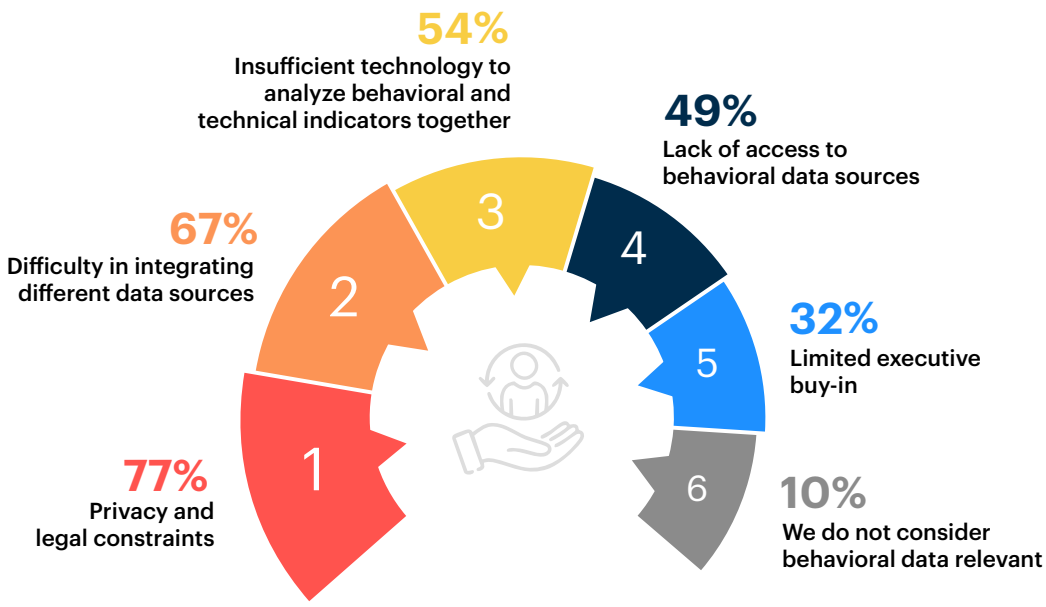
- **Privacy, integration, and technical barriers dominate:** Organizations cite privacy concerns (77%), integration difficulties (67%), and technology limitations (54%) as major roadblocks to incorporating comprehensive behavioral context.
- **Access to behavioral data remains constrained:** Nearly half (49%) struggle simply to access behavioral data, limiting their ability to meaningfully integrate human factors into insider threat detection.
- **Predictive risk models remain rare:** Only 12% of organizations have a mature predictive risk assessment capability, while 84% remain largely reactive—unable to effectively anticipate insider threats before incidents occur.
- **A critical maturity gap exists:** Organizations must move beyond reactive monitoring toward predictive, expert-informed modeling that combines technical signals, behavioral indicators, and contextual data—enabling security teams to proactively identify insider threats at their earliest stages.

Barriers to Whole-Person Intelligence

Even as organizations increasingly recognize the value of integrating behavioral insights into insider threat management, significant structural, technical, and policy barriers persist.

Privacy and legal concerns top the list (77%), reflecting uncertainty about responsibly collecting, analyzing, and acting on sensitive behavioral data. Integration challenges closely follow (67%), highlighting the difficulty of merging disparate HR, IT, and security systems not originally designed to interact. Over half (54%) indicate their technology can't effectively correlate behavioral and technical signals, while nearly half (49%) struggle simply to access relevant behavioral data.

What challenges does your organization face in adopting a whole-person approach to insider threat management?



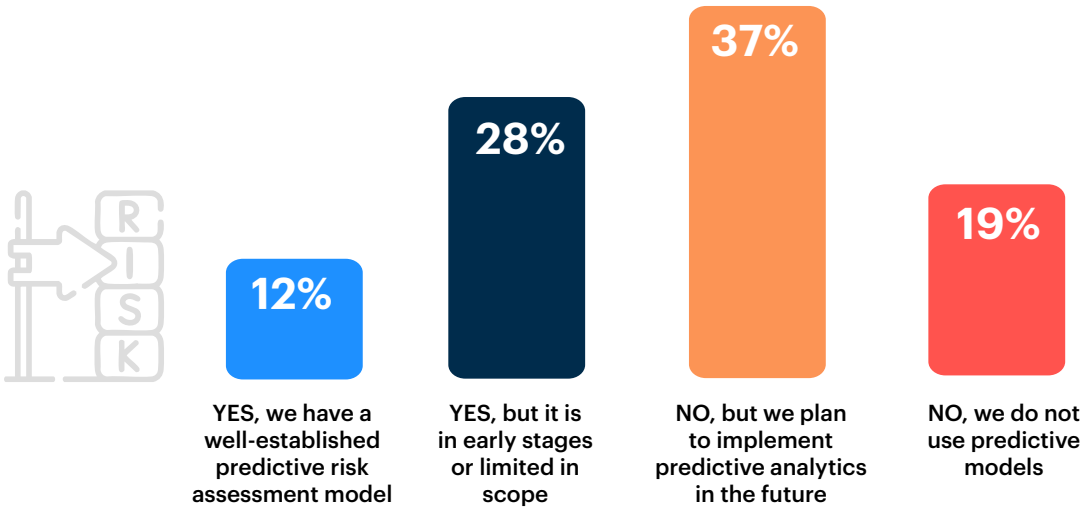
These obstacles trap organizations in reactive modes—relying on technical data alone without deeper understanding. Overcoming these challenges requires models designed explicitly for privacy-preserving, expert-informed analysis, enabling practical integration of sensitive behavioral and technical data. Such an approach embeds expert-informed modeling—leveraging consensus-driven calibration and explainable analytics—directly into insider threat detection workflows. This structural shift moves insider threat management beyond fragmented visibility toward proactive risk anticipation, empowering security teams to detect, understand, and respond to threats long before harm occurs.

Predictive Models Remain Rare

The ability to proactively predict—not merely react—is critical as insider threats become increasingly subtle. Yet this survey reveals a substantial gap between recognizing the need for predictive capability and actually implementing it.

Only 12% of respondents currently have a mature, fully operational predictive risk assessment model in place. Another 28% indicate their programs are still in early or limited stages. Notably, a majority (56%) either do not utilize predictive analytics at all or have only begun preliminary planning. This maturity gap underscores a critical finding: despite widespread awareness of insider threats and investments in various security tools, most organizations have yet to meaningfully combine technical and behavioral signals into predictive, proactive assessments.

Does your organization use risk scoring or predictive analytics to assess potential insider threats before an incident occurs?



Not sure 4%

The result is a persistent reliance on after-the-fact detection. Organizations continue to react to alerts and incidents rather than proactively identifying emerging patterns of risk, behavioral escalation, or subtle early-warning signs.

To bridge this critical maturity gap, organizations need predictive, expert-informed models that systematically integrate multiple behavioral and technical data sources. Leveraging structured risk scoring and multi-source analytics enables security teams to move from reactive detection toward proactive anticipation—significantly enhancing their ability to identify and mitigate insider threats before incidents ever occur.

05

How AI and Emerging Trends Transform Insider Risk

As Chapter 4 highlighted, proactive behavioral intelligence is critical to managing insider threats effectively. As AI adoption accelerates and the workplace continues to decentralize, organizations face new and amplified insider risks. This final chapter explores how the rapid expansion of AI capabilities, combined with trends in remote work and cloud collaboration, significantly broadens the insider threat landscape—requiring more sophisticated, context-driven approaches. These emerging trends make clear that predictive, adaptive behavioral modeling and comprehensive contextual analytics are no longer optional—they're imperative for effective insider risk management.

Key Findings:

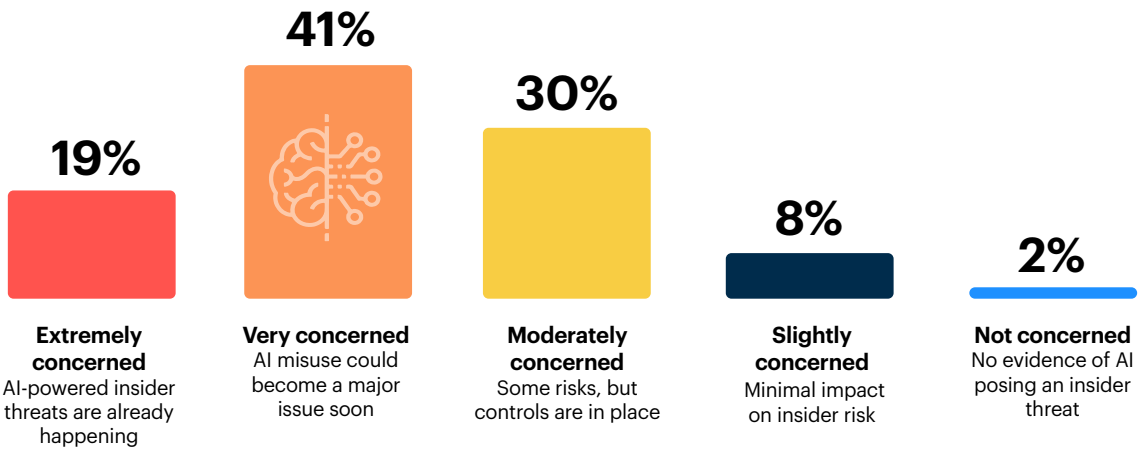
- **AI misuse significantly raises insider threat concerns:** Sixty percent of organizations are highly concerned about employees misusing AI tools, intentionally or unintentionally, to enable or amplify insider threats.
- **AI enables diverse insider attack vectors:** Organizations specifically highlight threats such as AI-driven phishing and social engineering (69%), automated data exfiltration (61%), credential abuse (53%), and AI-generated malware (46%), demonstrating the breadth and complexity of AI-facilitated insider risks.
- **Remote work, AI, and cloud collaboration will dominate future insider risks:** Security leaders expect remote and hybrid work (75%), AI and automation (69%), and cloud-based collaboration (66%) to be the primary drivers reshaping insider threats over the next 3–5 years.
- **Proactive behavioral modeling becomes essential:** Effectively managing this evolving risk landscape demands predictive, adaptive models that integrate behavioral and contextual signals, enabling organizations to anticipate insider threats early and intervene effectively.

AI Misuse Widens Insider Threat Surface

As organizations increasingly adopt AI tools such as ChatGPT and Copilot for daily tasks, security leaders recognize the growing potential for these powerful tools to facilitate insider threats—whether intentionally or inadvertently.

Sixty percent of respondents are either extremely or very concerned about employees misusing AI tools in ways that could lead to insider-related incidents. An additional 30% acknowledge some risk but believe existing controls are adequate—a perspective that could quickly become outdated as AI capabilities and usage rapidly expand. Only 2% express no concern at all.

How concerned are you about employees misusing AI tools (e.g., ChatGPT, Copilot, or deepfake technology) to facilitate insider threats?



Crucially, this risk isn't limited to deliberate misuse. Unintentional mishandling of AI—such as employees uploading sensitive company data into publicly accessible AI models—can lead to significant security incidents. For instance, in April 2023, Samsung engineers inadvertently exposed proprietary source code by entering sensitive information into ChatGPT, prompting swift corporate restrictions.

To effectively address these evolving insider threats, organizations must expand their risk models beyond traditional indicators of intent to proactively monitor and manage behavioral patterns linked to AI usage. By incorporating behavioral and contextual insights, security teams can detect and respond early to risky behaviors involving AI tools—preventing incidents before sensitive data is compromised.

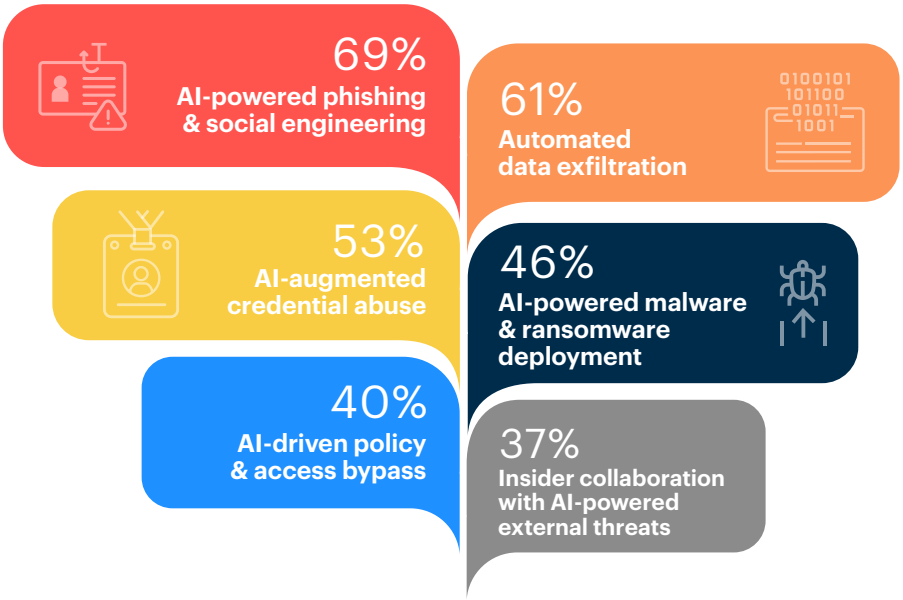
How AI Amplifies Insider Risk

Building on rising concerns about AI misuse, security leaders are pinpointing exactly how AI tools expand insider risk—both in obvious and less visible ways.

Respondents identify AI-powered phishing and deepfake social engineering (69%), automated data exfiltration (61%), and AI-assisted credential abuse (53%) as top threats. Nearly half (46%) also highlight AI-generated malware and ransomware, underscoring the risk of insiders leveraging generative AI to escalate attacks rapidly and covertly.

Equally noteworthy are emerging AI threats that often go overlooked: insider collaboration with AI-enabled external attackers (37%), AI-manipulated audit logs (32%), algorithmic manipulation (27%), and data poisoning (22%). These represent subtle yet powerful risks where insiders exploit AI not just to steal data, but to corrupt it or conceal their activities entirely.

Which of the following AI-enabled or AI-supported attack vectors do you perceive as the most significant risks for insider threats within your organization?



Addressing these amplified insider threats requires more than traditional detection. Security teams must evolve their approach to proactively identify early behavioral signals linked to AI misuse, enabling early intervention before threats escalate. By integrating behavioral insights with technical monitoring, organizations can better anticipate and respond to the widening landscape of AI-facilitated insider threats.

Additional responses: AI-manipulated audit logs (32%) | Algorithmic manipulation (27%) | Data poisoning (22%)

Key Trends Accelerate Insider Risk

Looking ahead, security leaders anticipate significant shifts in how insider risks will evolve—driven largely by distributed work, AI adoption, and cloud-enabled collaboration. These emerging factors will fundamentally reshape insider threats, demanding greater behavioral insight and contextual awareness.

Remote and hybrid workforce models top respondents' concerns at 75%, highlighting the persistent challenge of maintaining visibility and control as work environments decentralize. AI and automation follow closely at 69%, reinforcing earlier worries around the potential misuse of generative tools and sophisticated algorithms by insiders. Cloud-based collaboration and data-sharing platforms (66%) add another critical dimension, increasing both the speed and scale at which sensitive data can be compromised.

Other notable risks include advanced social engineering techniques (53%) and insider collusion with external threat actors (48%)—both highlighting increasingly complex, coordinated threats blending human factors with technological vulnerabilities. Interestingly, quantum computing remains less immediate (27%), reflecting current prioritization around more tangible, near-term risks tied directly to user behavior and access control.

Which of the following emerging risks do you think will have the biggest impact on insider threats in the next 3-5 years?

75% Remote and hybrid workforces

69% AI and automation in cybersecurity

66% Cloud-based collaboration and data sharing

53% Advanced social engineering techniques

48% Insider collusion with external threat actors

27% Quantum computing and encryption risks

These future trends underscore a clear imperative: effective insider threat management must move beyond traditional boundaries, integrating adaptive behavioral modeling and comprehensive contextual analytics. As insider threats become increasingly multifaceted and distributed, only approaches capable of interpreting nuanced human signals alongside technical events will be effective—validating that behavioral context is not merely helpful, but indispensable.

Best Practices for Insider Risk Management

Transforming Insider Threat Programs with Behavioral and Predictive Intelligence

Insider threats have evolved beyond isolated incidents to become pervasive, sophisticated risks requiring proactive prevention rather than reactive response. With only 23% of organizations strongly confident in detecting insider threats proactively, it's clear that current programs urgently need a strategic shift toward integrated behavioral analytics and predictive modeling. To effectively manage this escalating risk landscape, security and risk leaders should prioritize the following best practices:

1. **Adopt a Whole-Person Approach:** Insider threats are rooted in human behavior and context—not just technical anomalies. Only 21% of organizations extensively integrate behavioral signals (such as HR data, financial stress, or legal concerns) into their insider risk programs. Effective management requires systematically incorporating these signals into your detection models, providing critical insights into employee stressors, intent, and emerging risks long before threats materialize.

2. **Integrate Behavioral Intelligence with Technical Data:** Technical signals alone fail to provide the context needed for accurate insider threat detection. With 77% of organizations relying primarily on internal technical telemetry, most remain reactive. By integrating behavioral indicators (like employee engagement changes, HR disputes, or unusual work-hour activities) directly into technical monitoring workflows, teams gain real-time visibility into both human and system risks—enabling proactive, precise interventions.

3. **Implement Predictive, Privacy-Preserving Analytics:** Only 12% of organizations currently leverage mature predictive models for insider threats, leaving most in reactive mode. Mature insider risk programs should employ predictive analytics grounded in calibrated, expert-informed models. These privacy-preserving frameworks ensure responsible use of sensitive behavioral data, offering early warning signals without compromising employee privacy or compliance requirements.

4. **Prioritize Cross-Functional Collaboration:** Barriers such as inadequate tools (71%), limited budgets (69%), and privacy concerns (58%) significantly stall insider risk program advancement. Overcoming these challenges requires strong alignment among security, HR, legal, and compliance teams. Establish clearly defined escalation and off-ramping pathways, supported by collaborative policy frameworks, to rapidly address emerging insider risks with coordinated cross-functional interventions.

5. **Address Emerging AI and Remote-Work Risks:** With 60% highly concerned about AI misuse by insiders, organizations must extend insider threat monitoring beyond traditional boundaries. Proactively monitor how employees interact with powerful AI tools (like ChatGPT and Copilot), educate your workforce about potential inadvertent misuse, and establish governance and compliance policies that track subtle behavioral changes linked to AI adoption and remote or hybrid work dynamics.

Conclusion

The future of insider risk management can't rely on technical alerts and reactive measures alone. It will depend entirely on the organization's ability to understand people—their behaviors, intentions, access patterns, and stressors—in real time. This survey confirms that although organizations are increasingly aware of insider threats, crucial integration of behavioral insights and predictive modeling is often lacking.

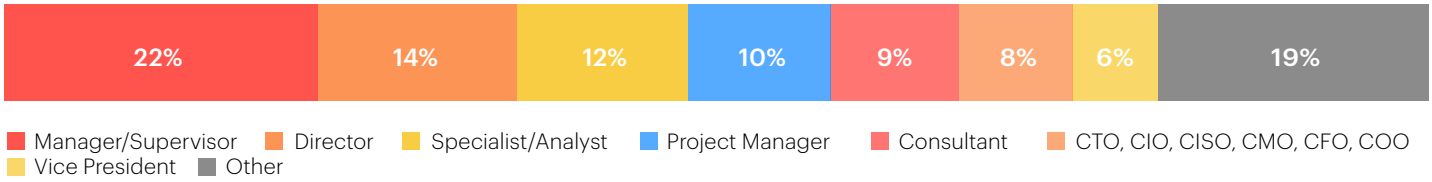
Embracing a comprehensive, whole-person approach is no longer simply beneficial—it's now an imperative step forward to proactively safeguard organizations from threats originating within. The time to transition from reactive detection to proactive behavioral intelligence is now.

Methodology and Demographics

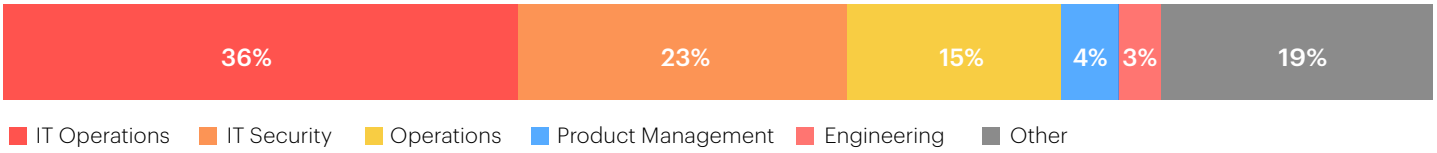
The 2025 Insider Risk Report is based on an online survey conducted in early 2025, gathering responses from 635 professionals responsible for insider risk management. Participants included CISOs, security directors, HR leaders, compliance officers, and IT executives from diverse industries, such as financial services, healthcare, technology, manufacturing, retail, government, and telecommunications.

A stratified sampling approach ensured balanced representation, achieving a 95% confidence level with a ±3.8% margin of error. Some questions allowed respondents to "select all that apply," resulting in percentages exceeding 100%. This methodology provides a comprehensive snapshot of current insider risk practices, challenges, and emerging trends.

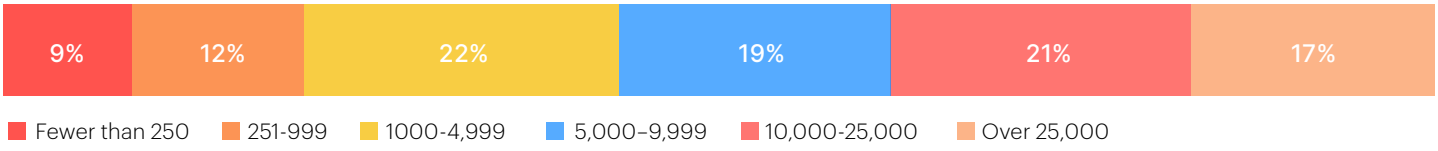
CAREER LEVEL



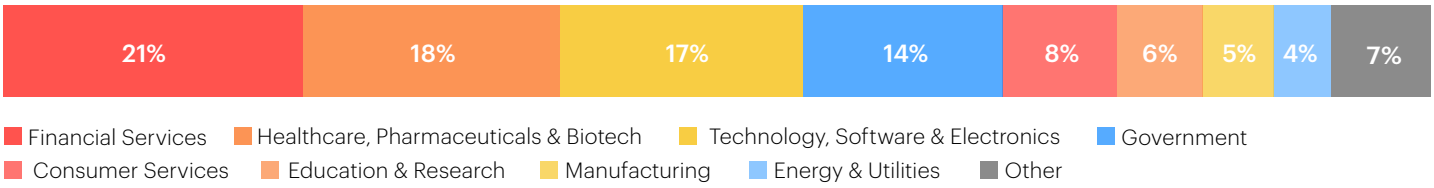
DEPARTMENT



COMPANY SIZE



INDUSTRY



COGILITY

Cogility's continuous Decision Intelligence Platform, Cogynt.ai, provides an advanced decision intelligence and decision support streaming analytic solution for government and commercial organizations — allowing our customers to get left of harm or ahead of opportunity. A cloud-scalable, proven solution, Cogynt.ai enables organizations to efficiently and effectively manage complex intelligence challenges with high-confidence, predictive and explainable insights required to become proactive versus reactive in highly complex and high consequence environments.

To learn more, visit **www.cogility.com**.

Cybersecurity
INSIDERS

STRATEGIC INSIGHT FOR CYBERSECURITY LEADERS

Cybersecurity Insiders delivers evidence-backed insights that empower security leaders to make informed, strategic decisions. Backed by over a decade of research and a global network of 600,000+ cybersecurity professionals, we provide actionable intelligence to help leaders navigate emerging threats, evaluate new technologies, and shape forward-looking strategies with confidence.

For cybersecurity vendors, we turn research into results — delivering credibility, visibility, and demand through high-impact formats such as:

- Data-powered market reports that establish thought leadership,
- Webinars that build trust with buyers through credible, expert-led narratives,
- CISO guides that showcase best practices,
- Product reviews that independently validate solutions,
- Thought leadership articles that educate buyers, and
- Award programs that elevate brand reputation.

By combining this content with built-in distribution, we help brands earn trust, amplify awareness, and drive demand in a crowded cybersecurity market.

For more information visit

cybersecurity-insiders.com