COST OF INSIDER RISKS

2026 GLOBAL REPORT

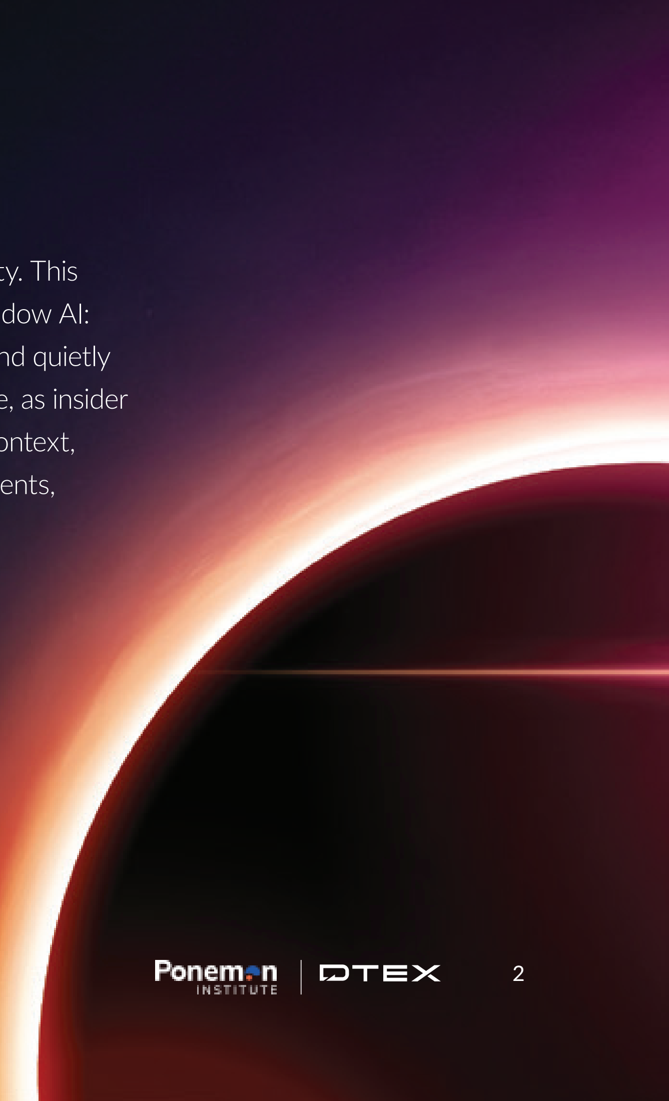
Independently conducted by

Ponemon Institute | DTEX

Table of contents

About the cover

Today's threat landscape is defined by speed and complexity. This year's cover reflects that reality. The eclipse represents shadow AI: the unsanctioned tools operating beyond security's view and quietly creating insider risk. The surrounding light presents promise, as insider risk management shows its ability to restore visibility and context, giving organizations a proactive advantage to prevent incidents, reduce loss, and move forward with confidence.



Ponemon Institute is pleased to present the findings of the **2026 Cost of Insider Risks Global Report** sponsored by DTEX.

This is the seventh benchmark study conducted to understand the financial consequences of insider risks. Expanding on the 2025 edition, this year's report explores the growing influence of artificial intelligence on insider risk and defense, and unlocks measurable data on the ROI of insider risk management.

Study snapshot:

354

Organizations that experienced one or more material events caused by an insider

25

Incidents per company

8,750

IT and IT security practitioners interviewed

7,490

Total number of insider incidents

> **"AI is the most transformative and dangerous shift in enterprise security history. Now more than ever, behavioral intelligence is needed to detect and deter insider risk: human or machine."**
>
> - Marshall Heilman, DTEX CEO

Insider risk types

MALICIOUS

Seeks to cause harm

- Espionage
- IP theft
- Unauthorized disclosure
- Sabotage
- Fraud
- Workplace violence

NON-MALICIOUS

NEGLIGENT:

Causes harm through carelessness or inattentiveness

- Ignores warnings

MISTAKEN:

Causes harm through a genuine mistake that cannot be attributed to carelessness

- Presses the wrong button in a stressful environment

OUTSMARTED:

Causes harm through being reasonably outmaneuvered by an attack or adversary

- Being phished by a new advanced phishing attack

This graphic is based on **MITRE Corporation's Insider Threat Types**

Human–agent risk interaction matrix

The following matrix was developed by DTEX's Insider Intelligence and Investigations (i^3) division to help security professionals classify and articulate the risk of any AI-related security incident. It offers a clear framework for mapping human and agent interactions so teams can quickly understand the scenario, gauge risk, and take the right investigative or defensive actions.

	AGENT: **NON-MALICIOUS**	AGENT: **MALICIOUS**
HUMAN: **NON-MALICIOUS**	**IDEAL STATE** • Collaborative, productive work • Both parties aligned on goals • Mutual benefit, ethical outcomes • Trust is warranted Risk: **LOW** Detection: **N/A**	**COMPROMISED** • Agent manipulates/deceives user • User trusts but is exploited • Data exfiltration, sabotage • User unaware of harm being done Risk: **HIGH (hidden threat)** Detection: **DIFFICULT**
HUMAN: **MALICIOUS**	**ADVERSARIAL USER** • User attempts jailbreaks/abuse • Agent should refuse/resist • Prompt injection attacks • Social engineering attempts Risk: **MEDIUM (agent as defense)** Detection: **MODERATE**	**COLLUSION** • Both parties aligned on harm • Maximum damage potential • Coordinated malicious activity • No internal checks/resistance Risk: **CRITICAL** Detection: **VERY DIFFICULT**

EXECUTIVE SUMMARY

Rising negligence reveals the cost of shadow AI

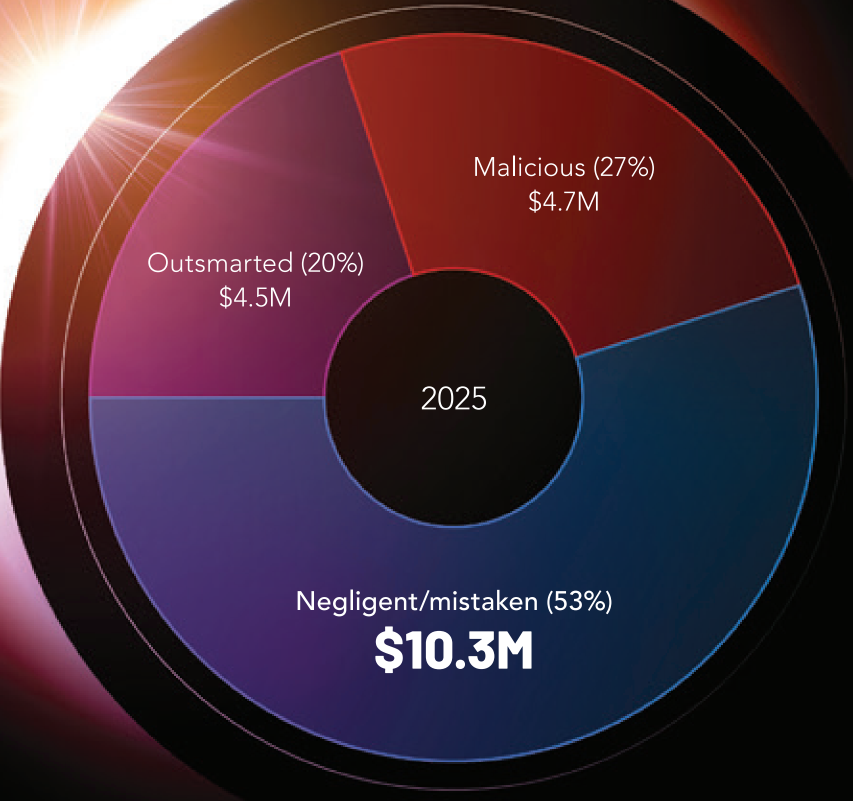
Insider risk security incidents now cost organizations an average of US$19.5M annually, up from $17.4M in 2024, underscoring how quickly exposure is escalating.

At the center of this growth is insider negligence, now the fastest-growing risk category, with associated losses rising 17% year over year to $10.3M annually. These incidents are not driven by malicious intent, but by everyday behavior in increasingly complex digital environments: misjudgments, process gaps, and unmanaged workflows.

This year's research highlights a new accelerant within these scenarios: shadow AI. As AI adoption accelerates across the workforce, visibility and governance are failing to keep pace, leaving organizations in the dark about how routine productivity behaviors expose sensitive data.

Ninety-two percent of organizations acknowledge that generative AI has fundamentally changed how employees access and share information, yet only 13% have formally integrated AI into their business strategies. Seventy-three percent worry that unauthorized AI use is creating invisible data exfiltration paths, 44% believe malicious use of AI agents will significantly or moderately increase data theft risk, while just 18% have fully integrated AI governance into their insider risk programs. The result is a widening strategy-reality gap where exposure grows faster than control.

> **The fastest-growing insider risk isn't malicious. It's everyday behavior amplified by gaps in AI visibility and governance.**



To examine whether the AI visibility gap translates into non-malicious insider risk, DTEX's Insider Intelligence and Investigations (i^3) division investigated the link between **shadow AI** use and **negligent insider behavior.** Their findings, detailed on page 10-11, point to a clear correlation: a cause-and-effect chain linking AI governance gaps, everyday employee behavior, and expanding risk.

Insider-ready organizations avoid 7 incidents, save $8.2M per year

This year's Ponemon report also provides clear evidence of the ROI of mature insider risk management programs.

Organizations with established insider risk programs prevent at least seven insider incidents annually, saving roughly $8.2M in avoided breach costs. With 63% now operating an insider risk program and spend rising to 19% of IT security budgets, returns are visible at scale.

Containment time, one of the most stubborn cost drivers, has dropped from 81 to 67 days, a 17% improvement year over year and the fastest recorded since the study began. Faster containment materially reduces exposure: incidents contained in under 30 days average $14.2M annually, versus $21.9M when containment exceeds 90 days.

Defensive AI and behavioral intelligence gain ground in insider risk prevention

Defensive AI adoption is accelerating. Forty-two percent of organizations now use AI to detect or prevent insider risks. Nineteen percent have deployed AI agents in daily workflows, with 71% rating them important to extremely important for early insider risk detection.

Behavioral intelligence also continues to gain traction. Seventy-one percent of users rate it as important to essential, while 58% cite avoided financial impact as a primary benefit. Among security investments, identity management (privileged access management) delivers the highest cost savings ($6.1M), followed closely by behavioral intelligence (user behavior analytics) ($5.1M).

The evidence points to a clear shift: programs combining behavioral insight and AI risk detection perform better. Where AI adoption outpaces visibility, negligent risk rises. How organizations close that gap increasingly shapes breach severity and cost.

SHADOW AI

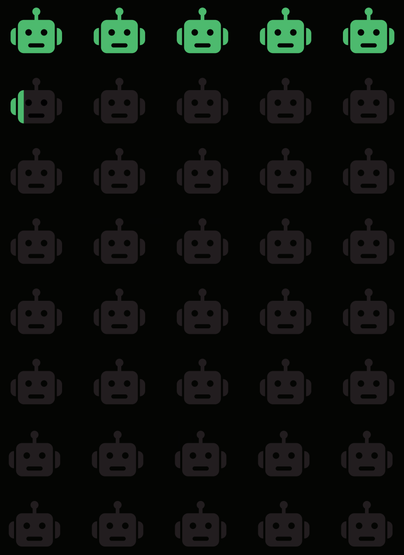
The insider risk you can't see but pay for.

Shadow AI is disrupting the insider risk landscape. Of all insider risk types, negligent insiders saw the biggest jump, costing organizations an average of $10.3M annually — up 17% year over year.

The cost of negligent insiders is up 17% year over year.

The top three causes of negligent incidents, observed by DTEX i³:

- SHADOW AI
- PERSONAL WEBMAIL
- FILE SHARING SITES



AI IN THE DARK

Only 13% have formally adopted AI into their business strategies.

92% say generative AI has fundamentally changed how employees access and share information.

73% worry that unauthorized AI use is creating invisible data loss pathways.

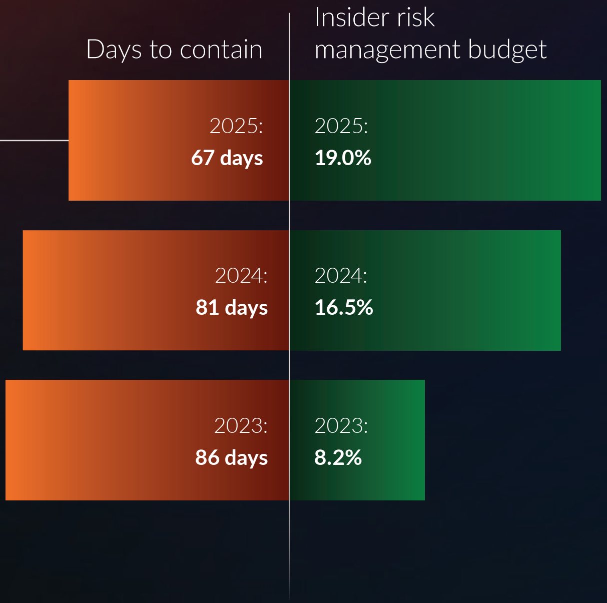
Only **18%** have fully integrated AI governance policies into their insider risk management program.

AI AGENTS: THE NEW DIGITAL EMPLOYEE

44% believe malicious use of AI agents will significantly or moderately increase the risk of data theft, yet only 19% classify AI agents as equivalent to human insiders.

INSIDER RISK MANAGEMENT ROI, PROVEN

67 days to shut it down.
Time to containment shrinks as insider risk budgets grow.



2023: $16.2M

2024: $17.4M

2025:

$19.5M

Total average annual cost of insider security incidents

7,490 incidents • 25 per organization

The strongest metric is what never happens.
Each year, organizations with an insider risk management program:

Avoid 7 insider incidents

82% have or plan to have an insider risk management program.

Of those with a program (63%), **49%** say their program is very or highly effective at preventing insider incidents.

50% measure insider risk management by fewer incidents.

40% fund it to prevent them.

Save $8.2M in breach costs

The tech delivering the savings

$6.1M	$5.1M
Identity management	Behavioral intelligence

71% using behavioral intelligence describe it as important to essential for preventing insider risks.

The numbers behind the savings: We calculate savings by comparing expected annual insider incident costs for organizations with and without an insider risk management program. Organizations with a program avoid an average of seven incidents ($5.4M). When costs are weighted by adoption rates (63% vs. 37%), total exposure drops from $24.9M to $16.7M, delivering roughly $8.2M in annual savings per organization.

All monetary values mentioned on this spread are in US dollars (USD).

NEGLIGENCE AT MACHINE SPEED:

How shadow AI is redefining insider risk

Negligence accounted for the lion's share of insider risk cost this year. To understand what's driving this increase, we asked DTEX's Insider Intelligence and Investigations (i^3) division to assess whether emerging work patterns are accelerating negligent insider activity. Their analysis identified three dominant contributors to negligent insider risk:

1. Unmonitored file sharing enables silent data leaks and regulatory exposure
2. Personal webmail enables sensitive data sharing often beyond organizational oversight
3. Shadow AI turning routine productivity behaviors into persistent data leakage

The following findings reflect the most prevalent shadow AI behaviors observed across DTEX i^3 investigations throughout 2025.

KEY FINDINGS, DTEX i^3

Shadow AI is everywhere and rarely sanctioned. Unapproved AI tools were embedded in daily work across government, financial services, telecoms, mining, and retail.

Prompting is now a dominant leakage pathway

Employees regularly input internal documents, legal material, source code, architecture diagrams, and strategy into ChatGPT, Claude, Gemini, Perplexity, and Grok AI.

Meetings have become an unguarded data source

AI notetakers (Read AI, Gong, Fireflies, Otter.ai, Fathom) routinely produced publicly accessible recordings and summaries containing sensitive internal discussions and staff personally identifiable information (PII), including vendor meetings.

Agentic AI expands the insider boundary

AI browsers and agents (e.g., Perplexity Comet) accessed corporate systems, conducted work, and bypassed traditional controls and logging.

Blocking one tool simply shifts the behavior

When ChatGPT was restricted, users migrated to Gemini, Perplexity, and agentic AI browsers.

Risky behavior is increasingly invisible

Alongside legitimate work, DTEX i^3 identified AI-assisted torrenting, NSFW content generation, and access to malicious sites via AI browsers.

This is negligence, not malice

The dominant pattern was well-intentioned employees optimizing for speed, not malicious insiders.

Visibility is the failure point

Organizations consistently lacked insight into which AI tools were used, what data entered them, and how long AI-generated artifacts remained accessible.

KEY FINDINGS, PONEMON

Rising insider risk costs are driven largely by containment.

Organizations now face average annual insider risk costs of US$19.5M, up from $17.4M in 2024, with containment representing the largest cost driver at $247,587 per incident, far exceeding escalation costs of $39,728.

Mature insider risk programs deliver measurable ROI.

Organizations with established insider risk management programs prevent at least seven insider incidents per year, avoiding approximately $8.2M in breach-related costs.

Rising insider risk investment is accelerating containment.

The share of IT security budgets allocated to insider risk management has more than doubled, increasing from 8.2% in 2023 to 19% in 2025. As investment has scaled, response effectiveness has improved: average containment time has dropped from 86 days in 2023 to 67 days in 2025, a 17% reduction and the fastest improvement recorded in the study.

Faster containment dramatically lowers incident costs.

Incidents contained within 30 days cost $14.2M annually, compared to $21.9M when containment exceeds 90 days.

Negligence dominates insider risk, and costs are rising fast.

Losses tied to insider negligence reached $10.3M annually, increasing 17% year over year. Organizations reported an average of 13.8 negligent insider incidents, with each incident costing approximately $747,107.

AI use is scaling faster than oversight.

Ninety-two percent of organizations say generative AI has changed how employees access and share information, yet only 13% have formally integrated AI into their business strategies.

AI agents are emerging as a blind spot in insider risk programs.

Forty-four percent of organizations believe malicious use of AI agents will significantly or moderately increase data theft risk, but nearly half (44%) report minimal to no visibility into AI agent activity. Only 19% classify AI agents as equivalent to human insiders.

Governance gaps are widening insider risk exposure.

Seventy-three percent of organizations worry unauthorized AI use is creating unseen data exfiltration paths, while just 18% have fully integrated AI governance into insider risk management programs.

Defensive AI and behavioral intelligence are gaining traction.

Forty-two percent of organizations now use AI to detect or prevent insider risks, while 71% rate behavioral intelligence as important or essential. Among organizations using risk-adaptive policy automation (26%), 71% say it plays a critical role in preventing insider risk.

ABOUT THIS STUDY

Our research focuses on actual insider-related events or incidents that impact organizational costs over the past 12 months.

Our methods attempt to capture both direct and indirect costs including but not limited to the following business risks:

- Theft or loss of mission-critical data or intellectual property
- Impact of downtime on organizational productivity
- Damages to equipment and other assets
- Cost to detect and remediate systems and core business processes
- Legal and regulatory impact, including litigation defense costs
- Lost confidence and trust among key stakeholders
- Diminishment of marketplace brand and reputation

This research utilizes an activity-based costing (ABC) framework. Our fieldwork was conducted over a two-month period concluding in September 2025. Our final benchmark sample consisted of 354 separate organizations. A total of 8,750 interviews were conducted with key personnel in these organizations. Activity costs for the present study were derived from actual meetings or site visits for all participants conducted under strict confidentiality.

Targeted organizations were:

- Commercial and public sector organizations
- Global headcount of less than 500 or more employees
- Locations throughout the following regions: North America, Europe, Middle East and Africa, and Asia-Pacific
- Central IT function with control over on-premises and/or cloud environment
- Experienced one or more material incidents caused by negligent/mistaken, malicious/criminal, or outsmarted insiders

In this report, we present an objective framework that measures the full cost impact of events or incidents caused by insiders. Following are the three case profiles that were used to categorize and analyze insider-related cost for 354 organizations:

- Negligent or mistaken employee or contractor
- Malicious or criminal insider including employee or contractor
- Outsmarted employee (i.e., credential theft)

Our first step in this research was the recruitment of global organizations. The researchers utilized diagnostic interviews and activity-based costing to capture and extrapolate cost data. Ponemon Institute executed all phases of this research project, which included the following steps:

- Working sessions with DTEX to establish areas of inquiry
- Recruitment of benchmark companies
- Development of an activity-based costing framework
- Administration of research program
- Analysis of all results with appropriate reliability checks
- Preparation of a report that summarizes all salient research findings

PART 1:

ANALYSIS AND SCOPE OF THE INSIDER RISK PROBLEM

In this section, we provide a deeper analysis of the benchmark study on the cost of insider risks. These results are based on interviews conducted with IT security and line-of-business (LOB) practitioners in 354 organizations in North America (47%), Europe (26%), Middle East (12%) and the Asia-Pacific regions (15%).

We have organized the benchmark results according to the following topics:

- Analysis and cost of the insider risk problem
- The cost of insider risk by activity

Trends in the insider risk benchmark research

Since 2018, the number of insider incidents discovered has more than doubled and the organizations represented in the research have more than doubled. Table 1 provides a retrospective of the research and how insider risks have impacted organizations.

Trends in how insider risks have impacted organizations	FY2018	FY2019	FY2022	FY2023	FY2024	FY2025
Total number of incidents discovered	3,269	4,458	6,803	7,343	7,868	7,490
Average number of insider risk incidents per organization	21.0	20.8	22.0	26.4	24.6	25.4
Average number of interviews per organization	20.0	21.3	20.8	24.5	23.8	25.5
Average number of benchmarked organizations	156	214	278	309	349	354

Table 1

Frequency of 7,490 incidents by insider risk profile

Negligent employees or contractors continue to be the primary source of an insider incident. Figure 1 shows the distribution of 7,490 reported attacks analyzed in our sample. A total of 3,970 attacks, or 53%, were caused by employee or contractor negligence. Malicious or criminal insiders caused another 2,022 attacks, or 27%, and there were 1,498 incidents caused by outsmarted insiders (20%).

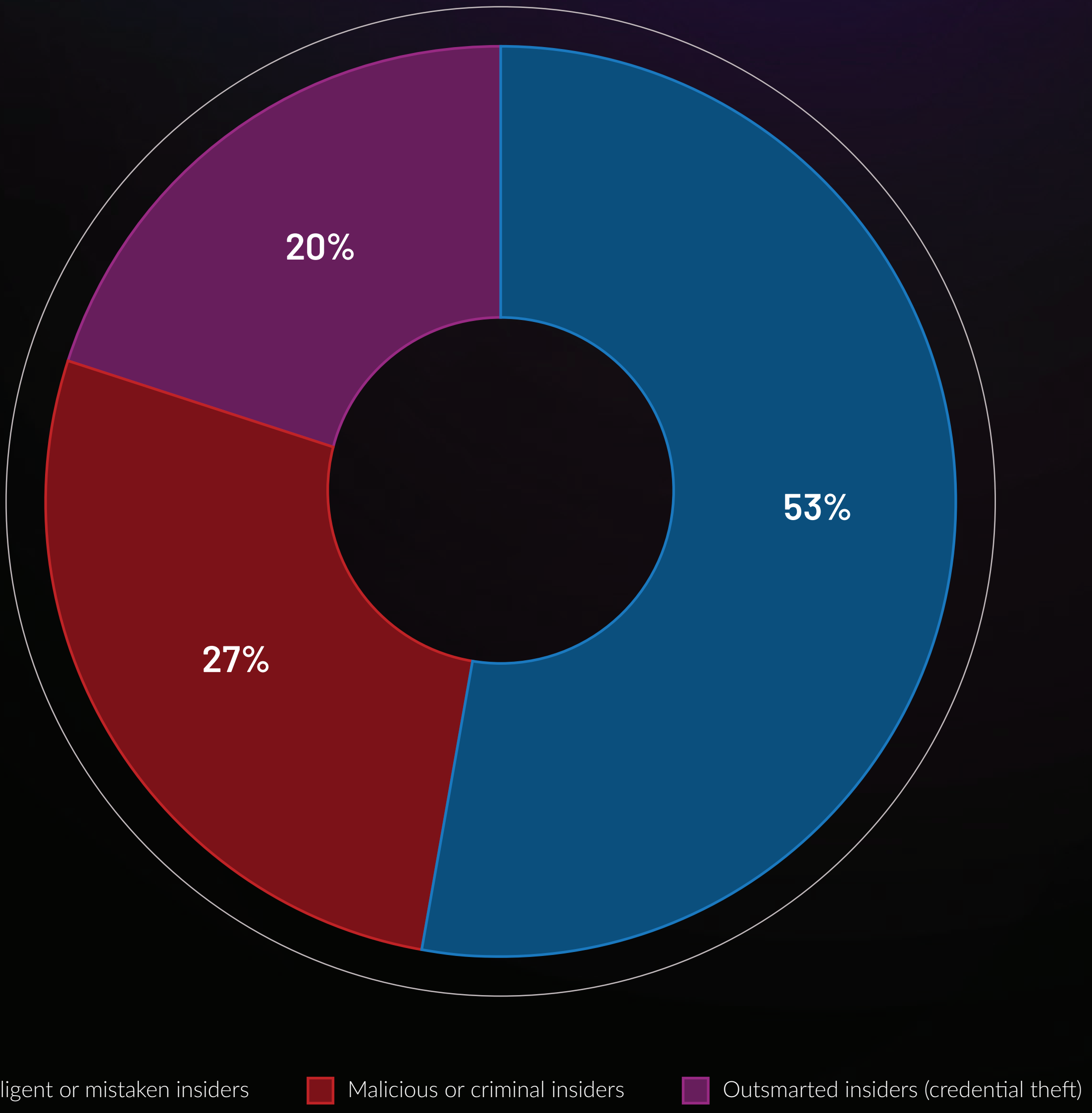


Figure 1

Frequency for three profiles of insider incidents over four years

Employee negligence continues to be the most frequent incident. As shown in Figure 2, the frequency of employee or contractor negligence was 13.8 in 2025 and 13.5 in 2024. Credential theft increased from 4.8 incidents to 5.3 in this year's study. Criminal and malicious insider incidents stayed the same, 6.3 in 2024 and 6.3 in 2025.

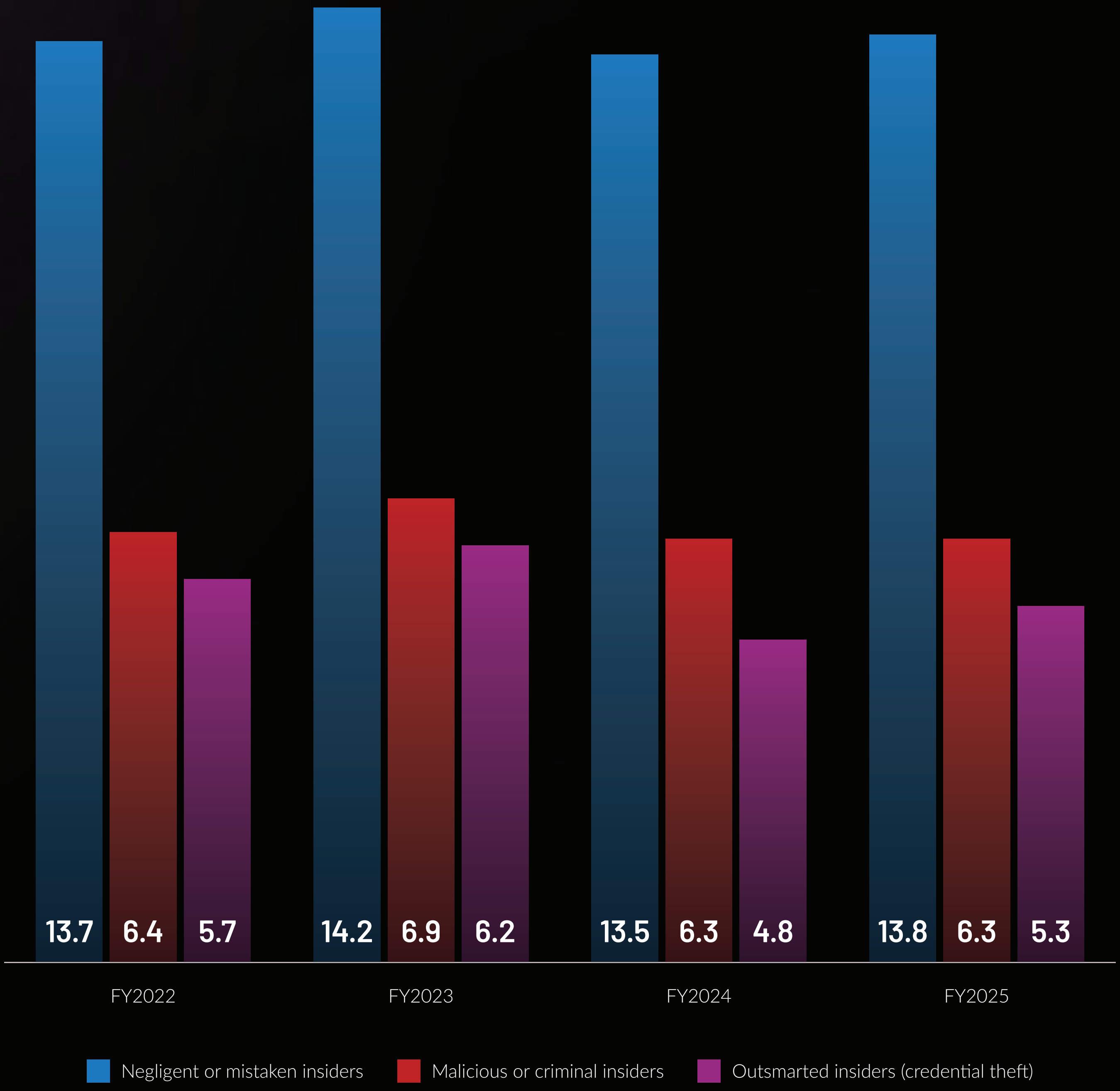


Figure 2

Average cost per incident and annualized cost from 2024 to 2025

Negligence continues to be the costliest type of incident. As shown in Table 2, the annualized cost increased from $17.4M in 2024 to $19.5M in 2025. The average cost to remediate negligence increased from $676,517 in 2024 to $747,107 in 2025.

FY2025 case profiles	Average cost per incident	Number of incidents	Annualized cost
Negligent or mistaken insider	$747,107	13.8	$10,310,077
Criminal or malicious insider	$742,125	6.3	$4,675,388
Outsmarted insider (credential theft)	$842,462	5.3	$4,465,049
			$19,450,513

FY2024 case profiles	Average cost per incident	Number of incidents	Annualized cost
Negligent or mistaken insider	$676,517	13.5	$8,828,292
Criminal or malicious insider	$715,366	6.3	$3,719,898
Outsmarted insider (credential theft)	$779,707	4.8	$4,834,190
			$17,382,380

Table 2

Frequency of insider incidents by organizations over six years

Organizations having between one to 30 incidents decreased. Table 3 shows the average consolidated frequency of employee/contractor negligence or mistakes, criminal or malicious insider, and outsmarted incidents (credential theft) per company. According to the 2024 research, 69% of organizations (25% + 18% + 26%) experienced between one and 30 incidents. In 2025, 54% (15% + 17% + 22%) had between one and 30 incidents.

Frequency of insider incidents per organization	FY2018	FY2019	FY2022	FY2023	FY2024	FY2025
1 to 10	28%	25%	19%	18%	25%	15%
11 to 20	18%	16%	14%	11%	18%	17%
21 to 30	26%	29%	31%	30%	26%	22%
31 to 40	19%	19%	21%	22%	21%	30%
More than 40	8%	12%	15%	19%	10%	16%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Table 3

Average incident frequency by four global regions

In 2025, organizations in the Middle East experienced the most employee negligence incidents (14.9) and Asia-Pacific had the least number of such incidents (12.6). Figure 3 presents the frequency of insider incidents in the four regions represented in the research. In all regions, employee or contractor insider negligence incidents occurred the most frequently. Organizations in North America are most likely to experience credential theft.

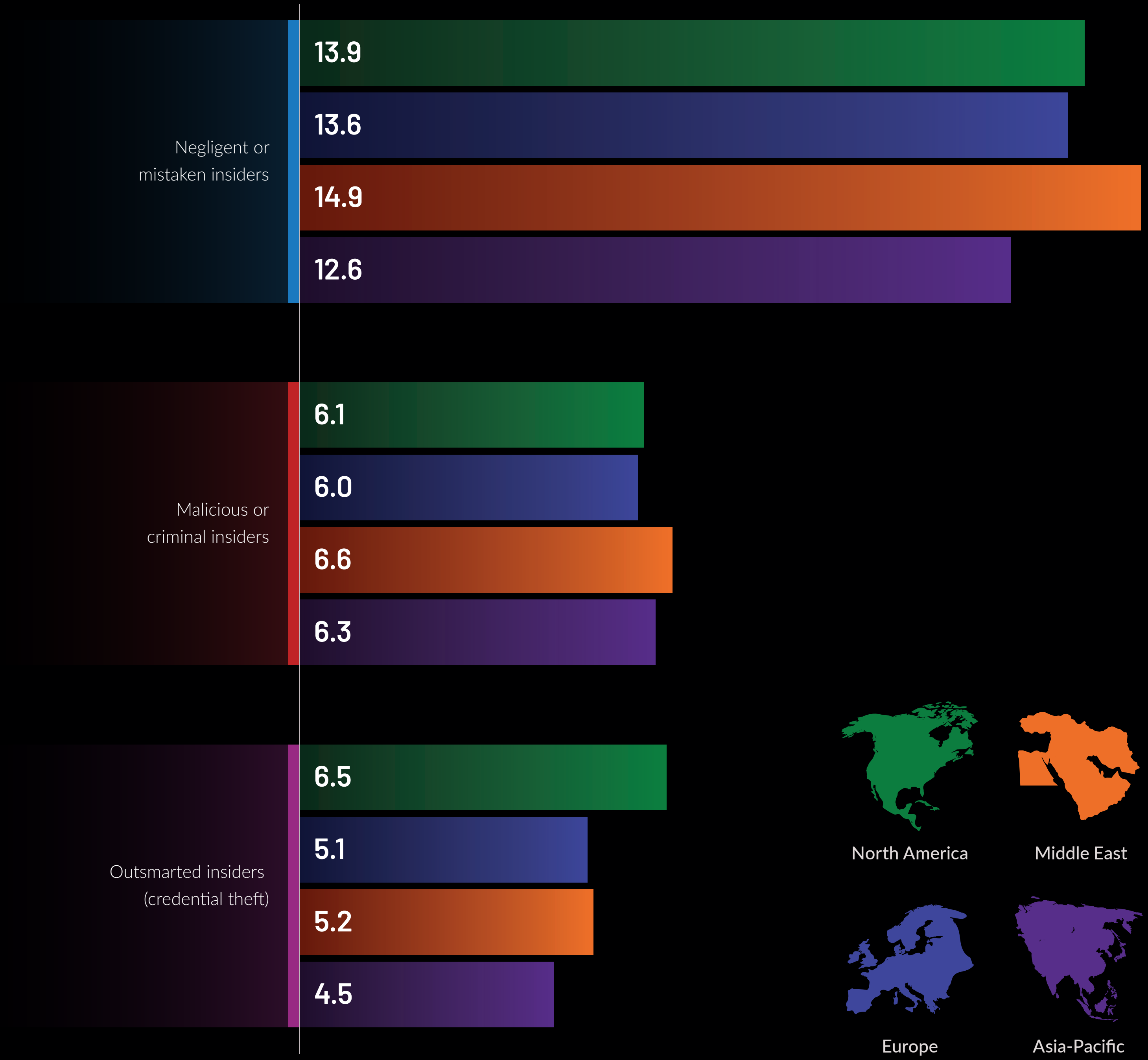


Figure 3

Average cost of insider risks by global region

North American companies are spending significantly more than the average cost of insider incidents to deal with insider risks. The total average cost of activities to resolve insider risks over a 12-month period is $19.5M. As shown in Figure 4, companies in North America experienced the highest total cost at $24M. European companies had the next highest cost at $18.6M. Asia-Pacific and Middle East had an average cost much lower than average total cost for all 354 companies ($17.5M and $17.4M).

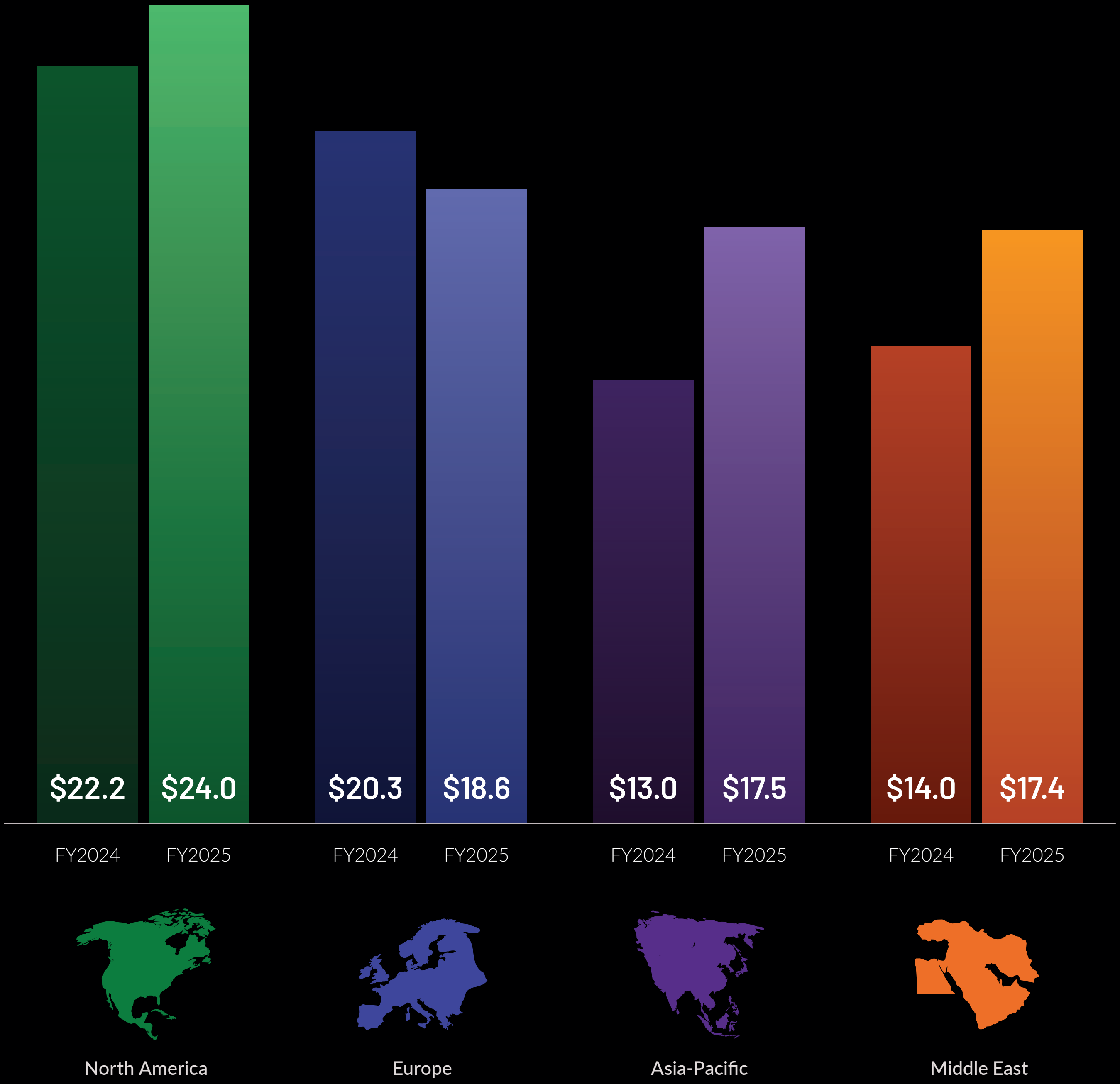


Figure 4: US$ millions

Average time to contain an insider incident

Companies are spending an average of 67 days to contain one insider security incident. According to Figure 5, 29% of the incidents took an average of more than 90 days to contain. Thirty-two percent say it took an average of 60 to 90 days. Only 13% of incidents were contained in less than 30 days.

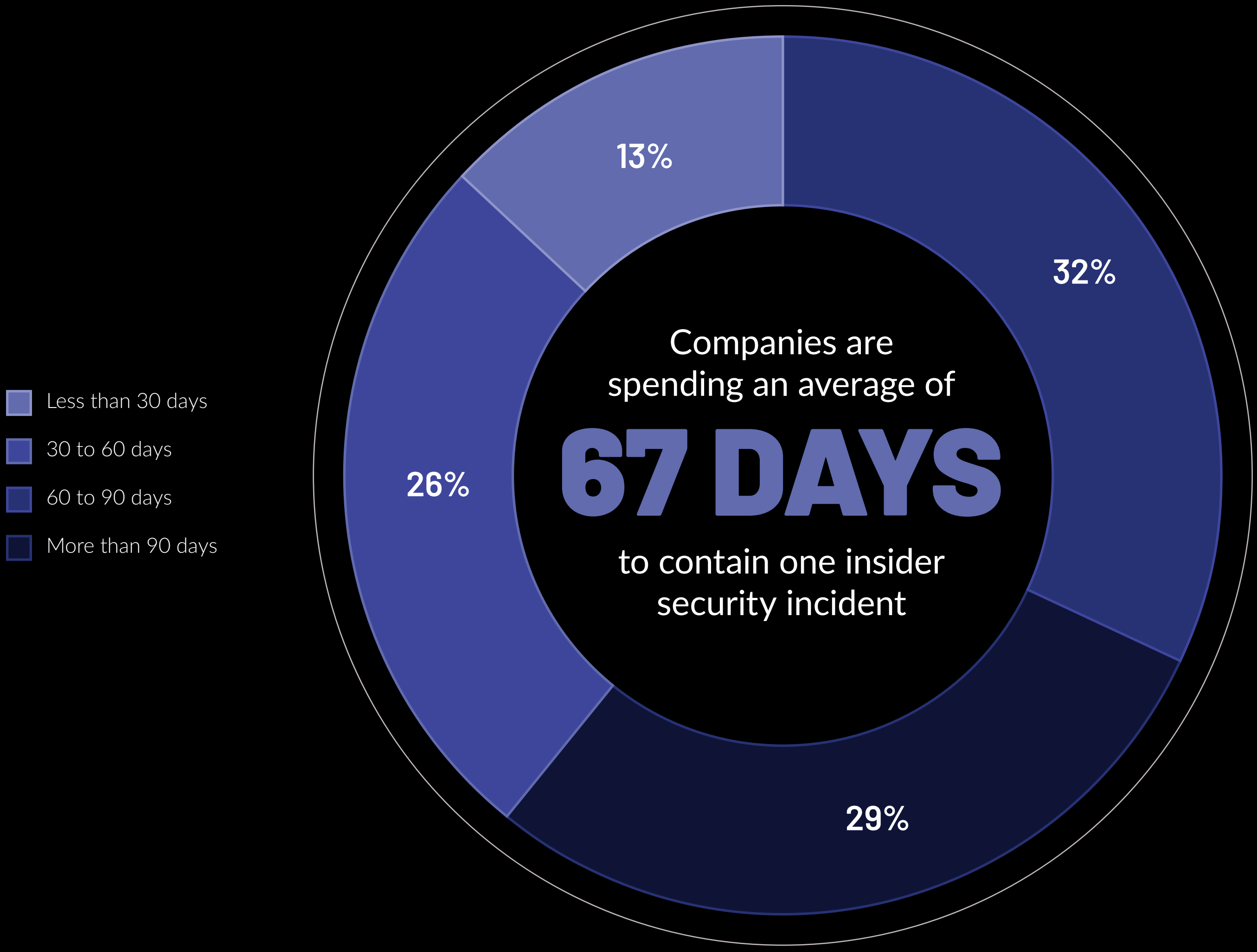


Figure 5

Average cost to contain an insider incident in 2025

The longer it takes to contain an insider incident, the more costly it is to remediate. As shown, if it takes more than 90 days the average cost is $21.9M. If it takes less than 30 days, the average cost is $14.2M.

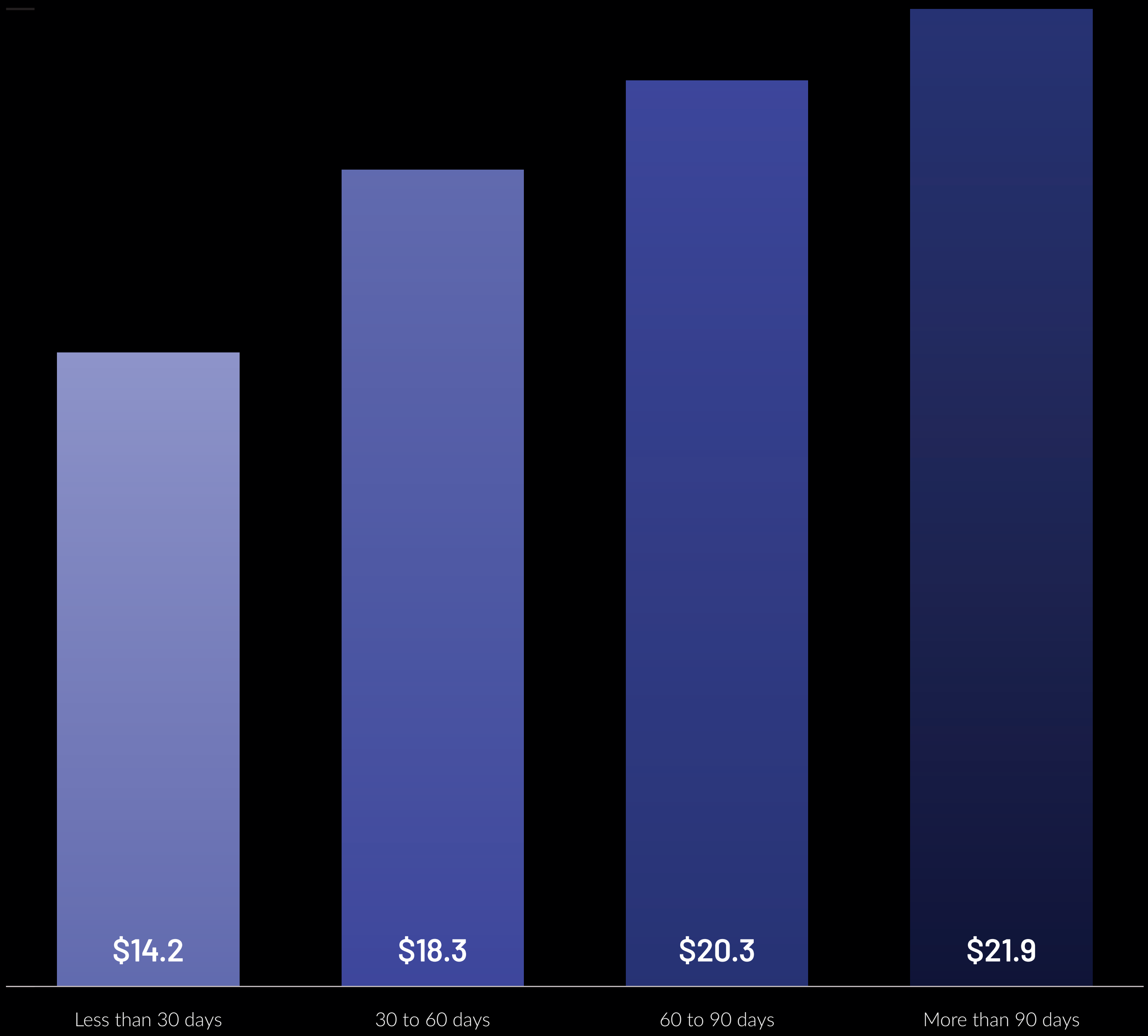


Figure 6: US$ millions

Average cost by days to contain the incident

The faster containment occurs, the lower the cost. The total annualized cost appears to be positively correlated with the time to contain insider incidents.

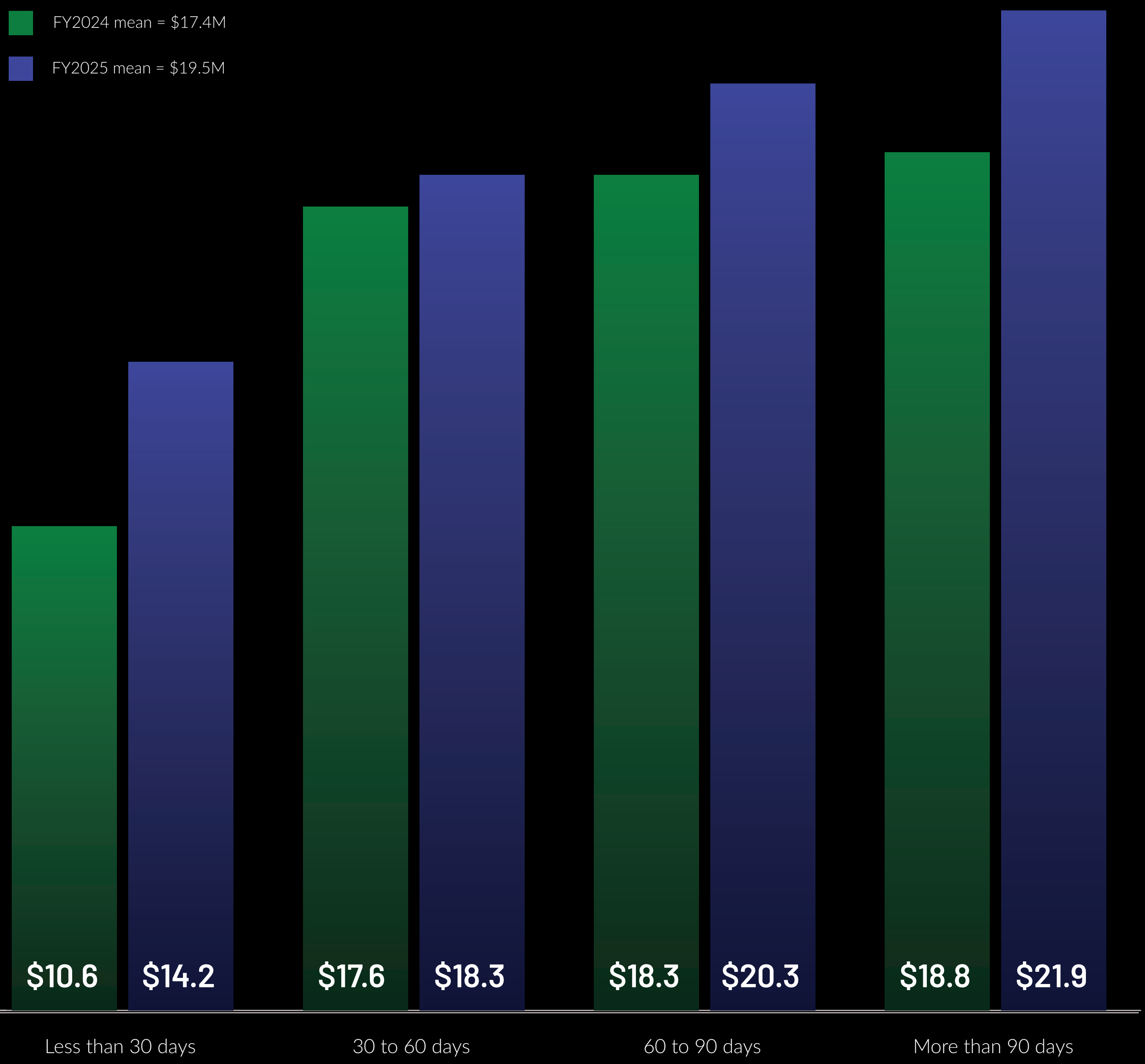


Figure 7: US$ millions

Average cost by industry

In 2025, insider risk costs are highest for health and pharmaceutical. According to Figure 8, the average annualized cost for health and pharmaceutical is $28.8M. The second highest is technology and software at $24.2M. Both industries are much higher than the average annualized cost of $19.5M.

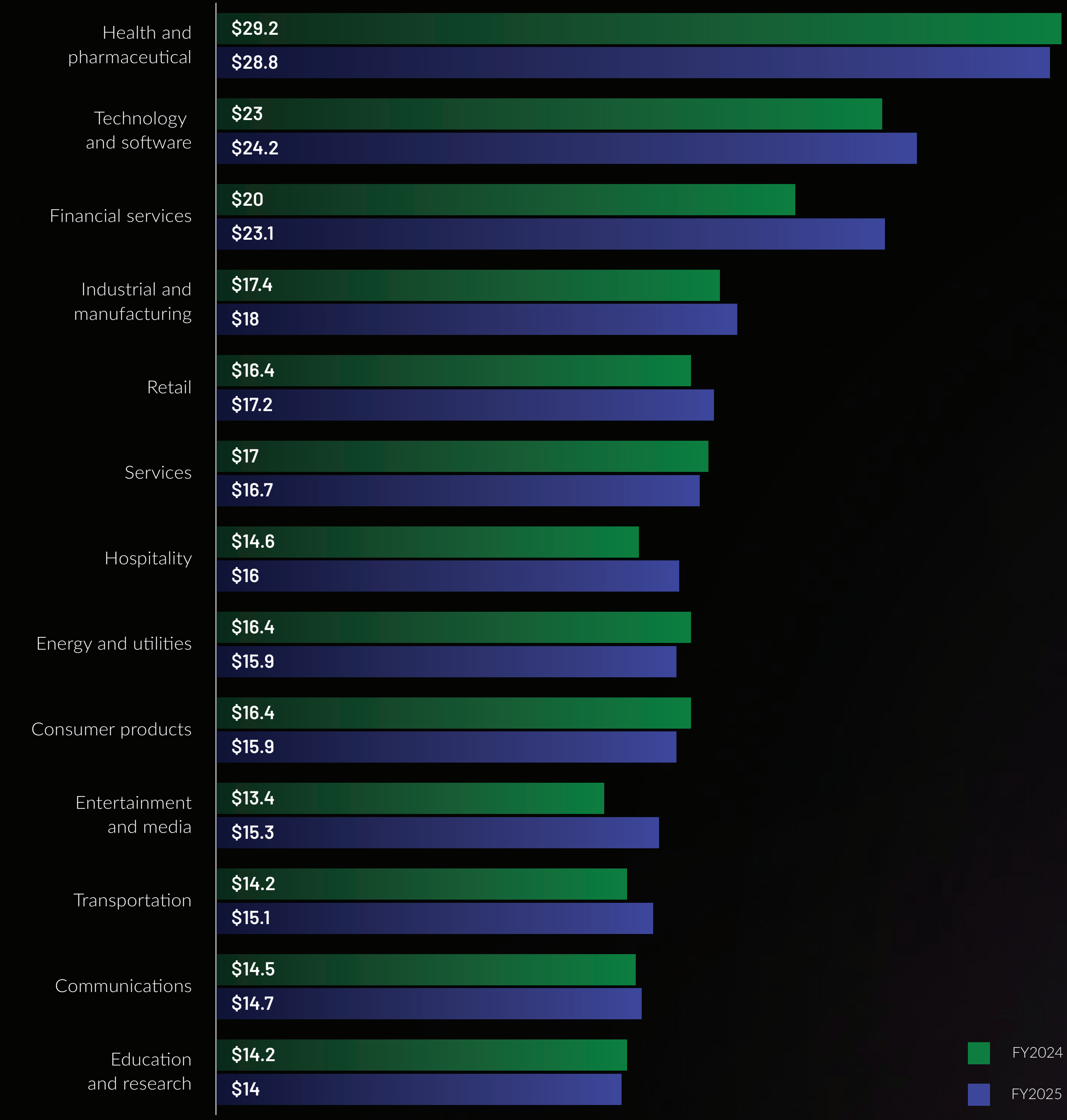


Figure 8: US$ millions

Percentage frequency in the use of tools and activities

Most participating organizations (83%) are conducting training and awareness programs to reduce insider risks. Table 4 shows 76% of organizations deploy privileged access management (identity management) solutions and 74% have data loss prevention. Least used are strict third-party vetting procedures (44%), incident response management and threat intelligence sharing tools (both 43%).

FY2025 tools and activities that reduce insider risks	Percentage of companies
User training and awareness	83%
Privileged access management (identity management)	76%
Data loss prevention	74%
Security incident and event management (SIEM)	70%
Employee monitoring and surveillance	65%
User behavior analytics (behavioral intelligence)	51%
Network traffic intelligence	47%
Strict third-party vetting procedures	44%
Incident response management	43%
Threat intelligence sharing tools	43%

Table 4

Cost savings resulting from the deployment of security technologies and activities

Privileged access management (identity management) solutions are used by 76% of companies and are shown to reduce insider costs significantly. Table 5 presents the tools and activities companies deploy to reduce the occurrence of insider risks and the cost savings for each given item.

The technology that reduces costs the most is privileged access management ($6.1M) followed by user behavior analytics (behavioral intelligence) ($5.1M).

Tools and activities that reduce insider risks	**FY2025 cost savings** (US$ millions)
Privileged access management (identity management)	$6.1
User behavior analytics (behavioral intelligence)	$5.1
User training and awareness	$4.8
Security incident and event management (SIEM)	$4.6
Incident response management	$4.1
Strict third-party vetting procedures	$3.0
Network traffic intelligence	$2.7
Threat intelligence sharing	$2.4
Employee monitoring and surveillance	$2.3
Data loss prevention	$2.0

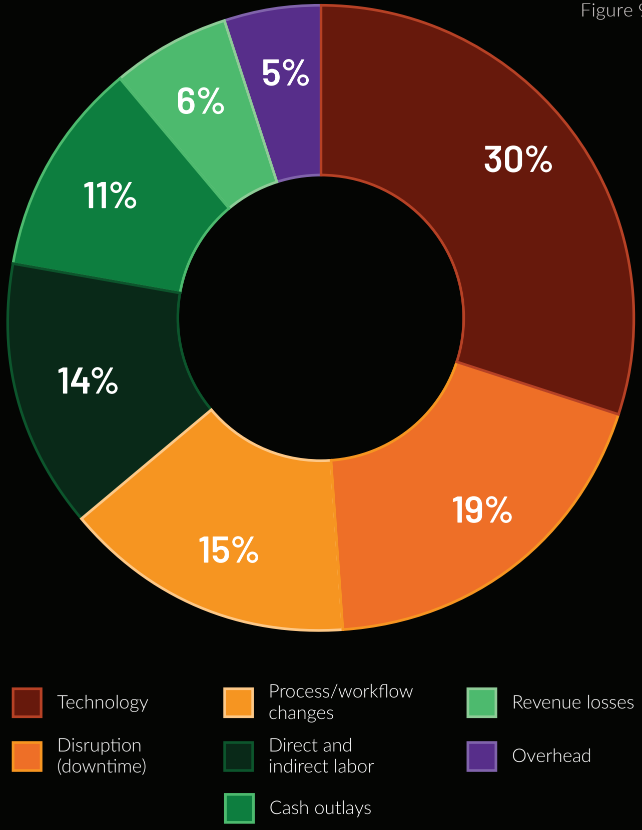
Table 5

Cost breakdown of insider incidents

Technology and disruption or downtime have the most significant financial consequences when dealing with insider incidents. Figure 9 shows the cost breakdown of insider incidents across the following seven categories: disruption (downtime), direct and indirect labor, technology, cash outlays, process/workflow changes, revenue losses and overhead.

The most common financial consequence is the cost incurred by technologies (30%) that are used to respond to the insider incident. It includes the amortized value and the licensing for software and hardware that are deployed. Business disruption is the next significant cost and includes diminished employee/user productivity (19%). Revenue losses (6%) and overhead (5%) have the lowest financial consequences.

Figure 9



Trends in the percentage of insider costs by the seven consequences

The most significant changes in cost by consequence are technology, followed by downtime, as shown in Figure 10.

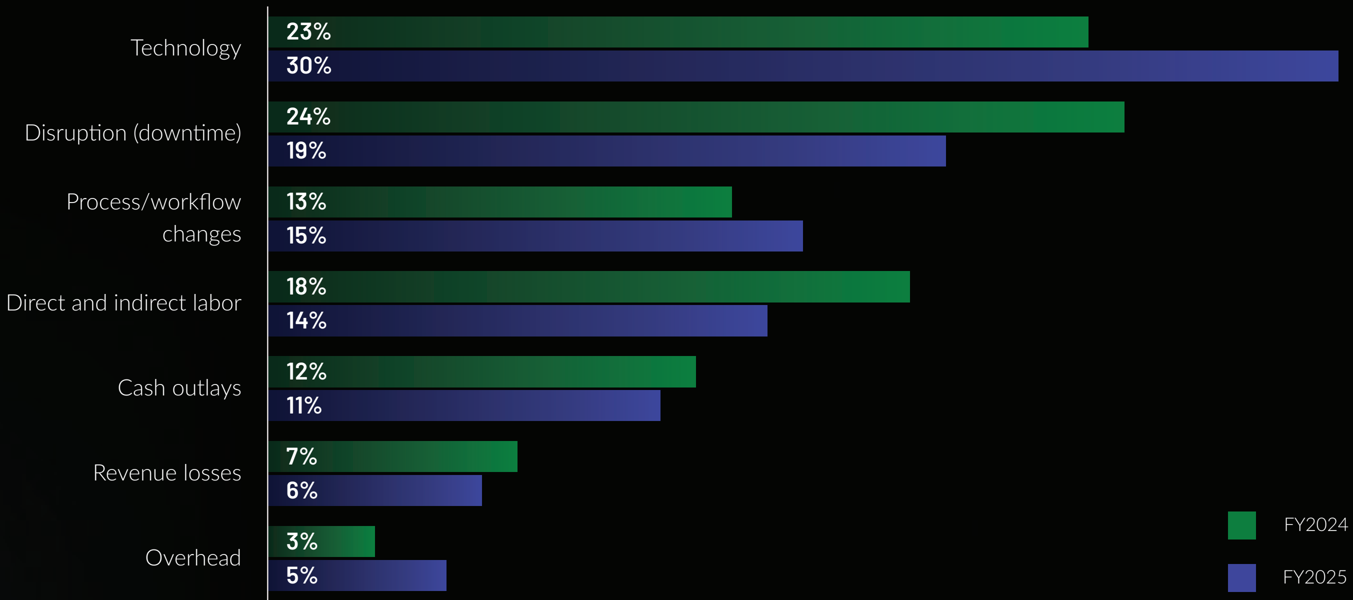


Figure 10

The cost of insider risk by activity

This study addresses the core process-related activities that drive a range of expenditures or costs associated with a company's response to insider-related incidents. The seven cost activity centers in our framework are defined as follows:[1]

Monitoring and surveillance: Activities that enable an organization to reasonably detect and possibly deter insider incidents or attacks. This includes allocated (overhead) costs of certain enabling technologies that enhance mitigation or early detection.

Investigation: Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents.

Escalation: Activities taken to raise awareness about actual incidents among key stakeholders within the company. The escalation activity also includes the steps taken to organize an initial management response.

Incident response: Activities relating to the formation and engagement of the incident response team including the steps taken to formulate a final management response.

Containment: Activities that focus on stopping or lessening the severity of insider incidents or attacks. These include shutting down vulnerable applications and endpoints.

Ex-post response: Activities to help the organization minimize potential future insider-related incidents and attacks. It also includes steps taken to communicate with key stakeholders both within and outside the company, including the preparation of recommendations to minimize potential harm.

Remediation: Activities associated with repairing and remediating the organization's systems and core business processes. These include the restoration of damaged information assets and IT infrastructure.

[1] Internal costs are extrapolated using labor (time) as a surrogate for direct and indirect costs. This is also used to allocate an overhead component for fixed costs such as multiyear investments in technologies.

Average cost of seven activities in 2024 and 2025

The average activity cost to contain an insider security incident increased 17% from 2024. Table 6 summarizes the average cost of insider-related incidents for seven activities. While the average time to contain an insider incident has declined to 67 days, the average cost increased from $211,021 to $247,587.

The second most costly activity is incident response which increased from $154,819 to $158,233. Included in these costs are the activities related to the formation and engagement of the incident response team including the steps taken to formulate a final management response.

Activity cost center categories	FY2024	FY2025
Containment	$211,021	$247,587
Incident response	$154,819	$158,233
Remediation	$131,761	$129,402
Investigation	$121,974	$117,526
Monitoring and surveillance	$37,756	$44,699
Ex-post response	$34,290	$40,057
Escalation	$32,242	$39,728
Total	**$723,863**	**$777,231**

Table 6

Percentage net increase in average cost for seven activity centers from FY2024 to FY2025

Since 2024, costs for five of the seven activities have increased. As shown in Figure 11, the cost of escalation activities has increased the most (23%) followed by monitoring and surveillance (18%), containment and ex-post response (both 17%).

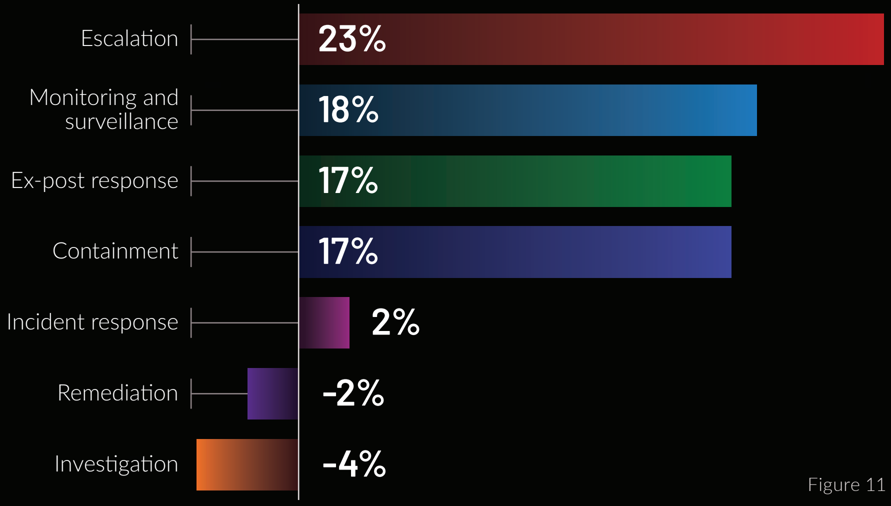


Figure 11

Average cost for seven activities by incident type in 2025

FY2025 activity cost center categories	Negligence	Malicious	Outsmarted (credential theft)	Average
Containment	$230,104	$229,138	$283,518	$247,587
Incident response	$144,491	$163,538	$166,670	$158,233
Remediation	$123,725	$122,197	$142,284	$129,402
Investigation	$123,523	$112,907	$116,147	$117,526
Monitoring and surveillance	$47,600	$42,905	$43,592	$44,699
Ex-post response	$38,829	$34,305	$47,037	$40,057
Escalation	$38,835	$37,137	$43,214	$39,728
Total	**$747,107**	**$742,125**	**$842,462**	**$777,231**

Table 7

The average activity cost per incident for the three types of incidents in 2025

The average activity cost is highest for credential theft. Figure 12 demonstrates the significant difference in activity costs between credential theft, criminal or malicious insider and employee negligence.

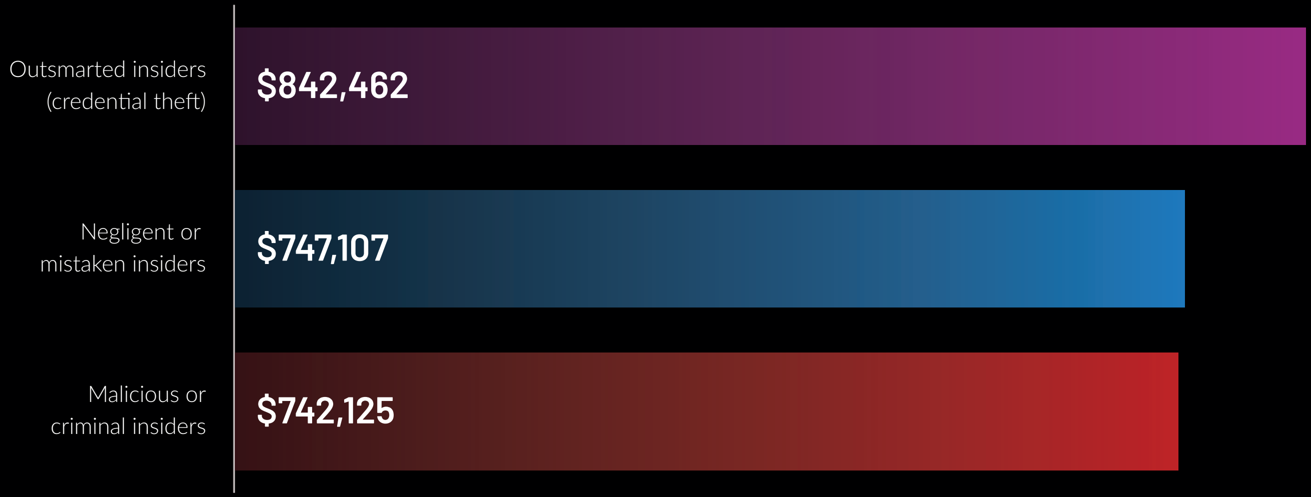


Figure 12

Percentage cost of insider incidents by activity center in 2025

Containment accounts for 32% of all costs. The following pie chart shows the percentage cost for seven activity centers. According to Figure 13, containment represents 32% of total annualized insider-related activity costs. Activities relating to incident response represent 20% of the cost.

Percentage of direct vs. indirect costs for activity centers

Companies were asked to estimate the direct and indirect costs[2] spent to accomplish a given activity. Direct costs are the direct expense outlay to accomplish a given activity, and indirect costs are the amount of time, effort and other organizational resources spent, but not as a direct cash outlay.

Figure 13

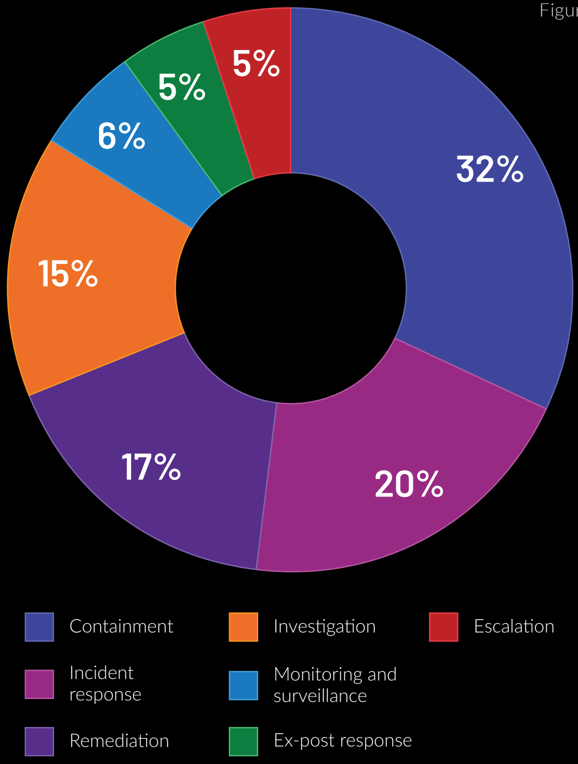
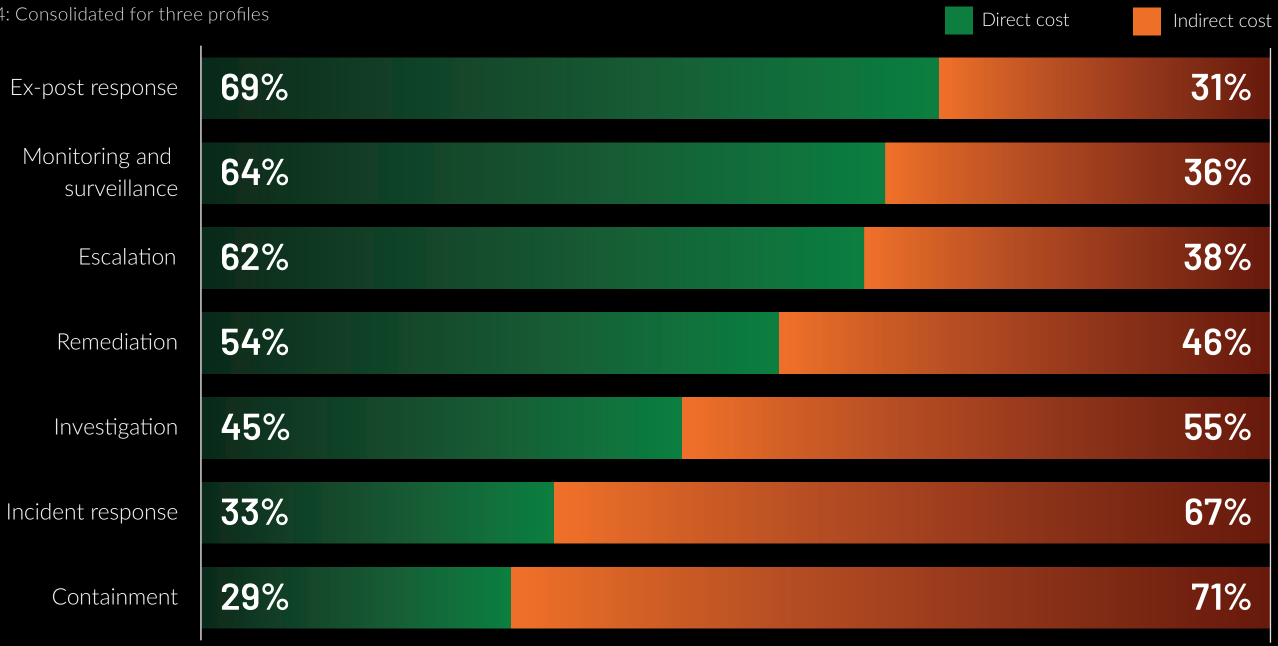


Figure 14 shows the proportion of direct and indirect costs for seven internal activity cost centers. The cost for ex-post response and monitoring and surveillance have the highest percentages of direct cost (69% and 64%, respectively). The highest percentages of indirect costs for activities are for incident containment and incident response (71% and 67%, respectively).

Figure 14: Consolidated for three profiles



[2] The direct cost is what is spent to accomplish a given activity, and indirect costs are the amount of time, effort and other organizational resources spent to resolve the incident.

PART 2:

MANAGING THE INSIDER RISK

Independent from determining the cost of insider risks for companies in this research (presented in part 1 of this report, page 15), we surveyed 1,323 participants about their experiences with insider risk and what they are doing to reduce the threat. This section presents the highlights of the research.

Agent or insider? The AI classification gap

Companies are increasingly concerned about AI agents. Forty-four percent believe malicious use of AI agents will significantly or moderately increase the risk of data theft, yet only 19% classify AI agents as equivalent to human insiders.

Perceived data theft risk from malicious use of AI agents

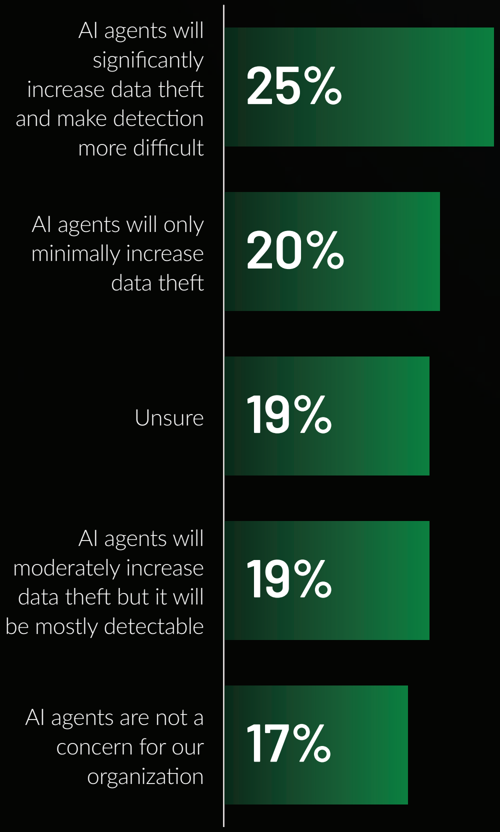


Figure 15

How organizations are classifying AI agents

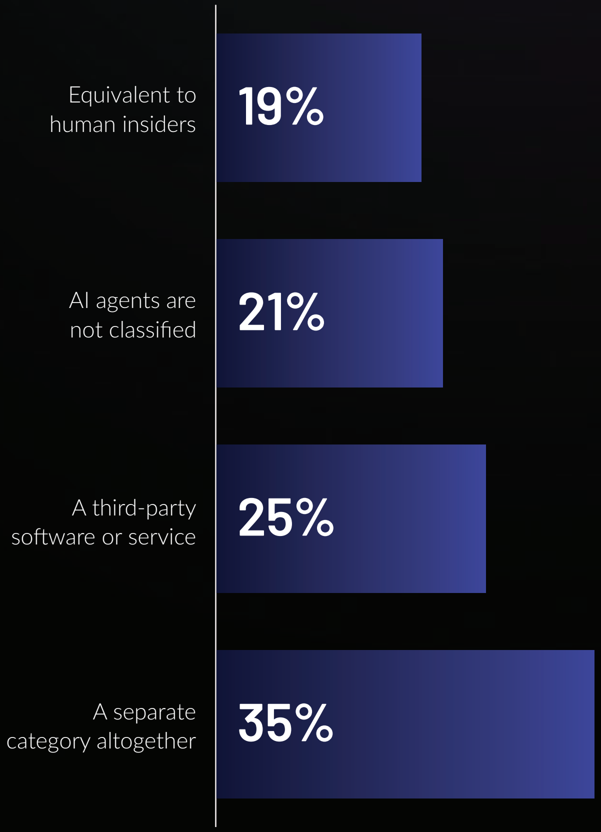


Figure 16

Risk without oversight. The AI control gap

Almost half of all surveyed organizations (44%) report minimal or no visibility at all into AI agents. Few (18%) organizations have fully integrated AI governance into their insider risk management programs, leaving most governance efforts outside insider risk oversight.

AI agent visibility

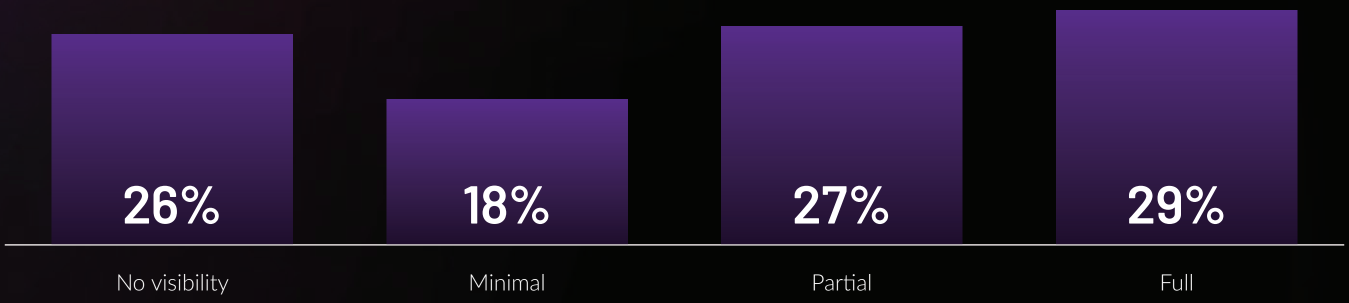


Figure 17

AI governance maturity

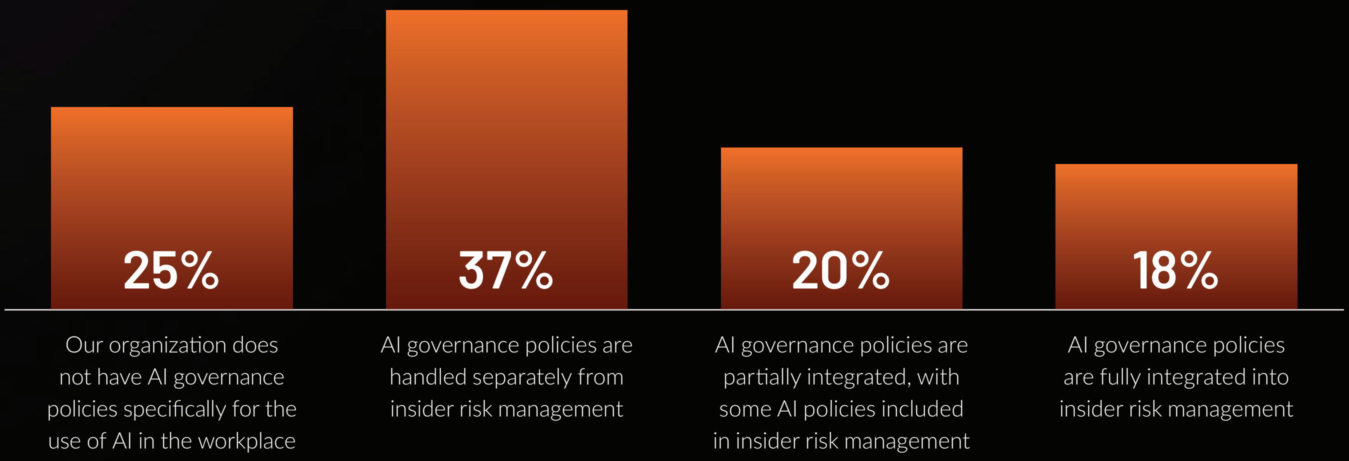


Figure 18

> **AI governance** policies are the rules, regulations, and ethical guidelines that control the development, deployment, and use of artificial intelligence technologies. They aim to ensure AI systems are safe, fair, transparent, and accountable, aligning with human values and legal requirements to mitigate risks like bias, privacy violations, and misuse.

AI sentiment. Formal adoption and concern

Only 13% of organizations have formally adopted generative AI into their business strategies, yet 73% are concerned that AI is introducing less visible forms of data loss.

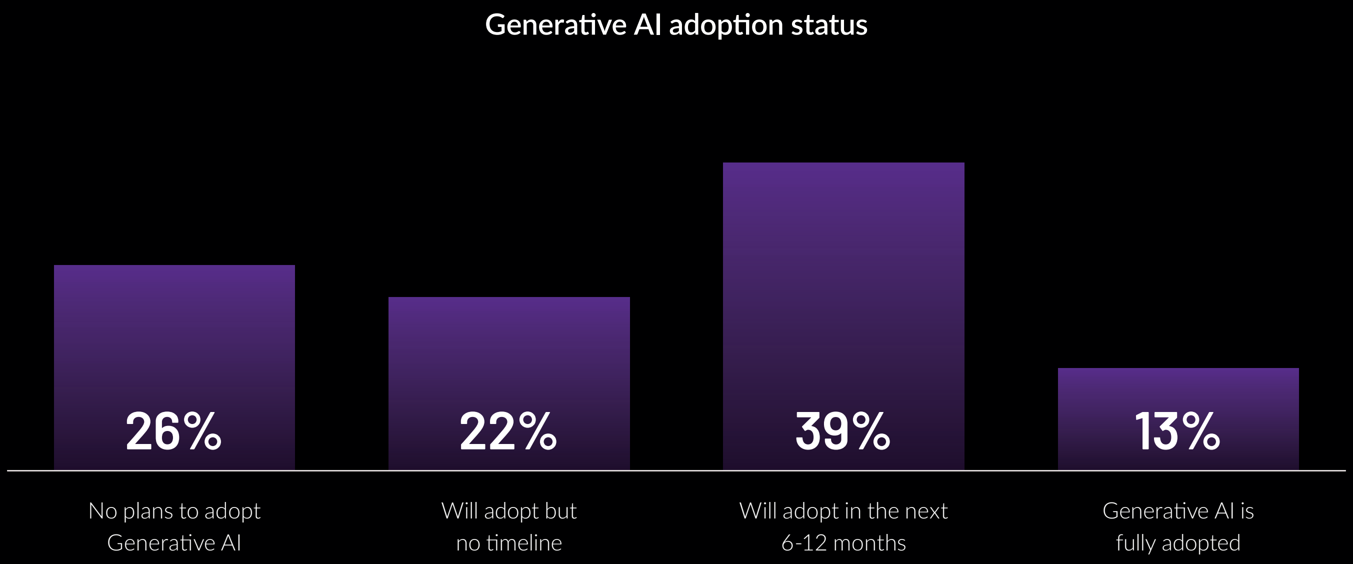


Figure 19

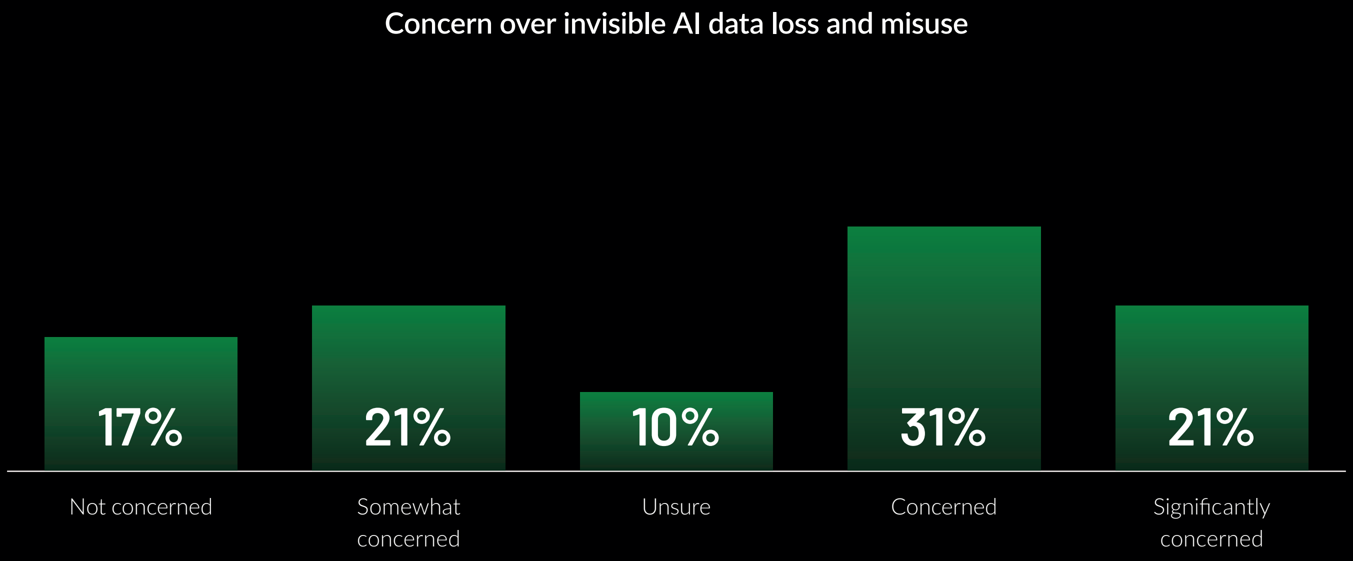


Figure 20

Sharpening risk detection. The AI defense

Forty-two percent of organizations now use AI to detect or prevent insider risks, and 47% of those report a reduction in false positives as the primary benefit.

Adoption of AI for insider risk detection and prevention

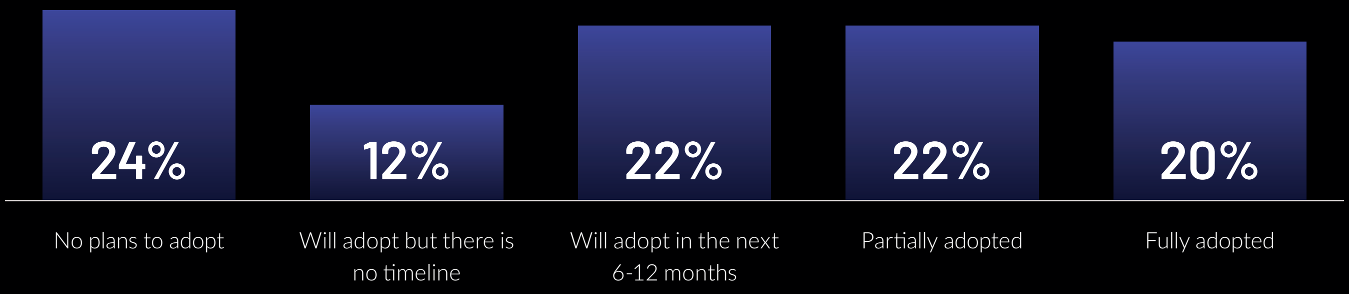


Figure 21

Benefits of AI for insider risk management

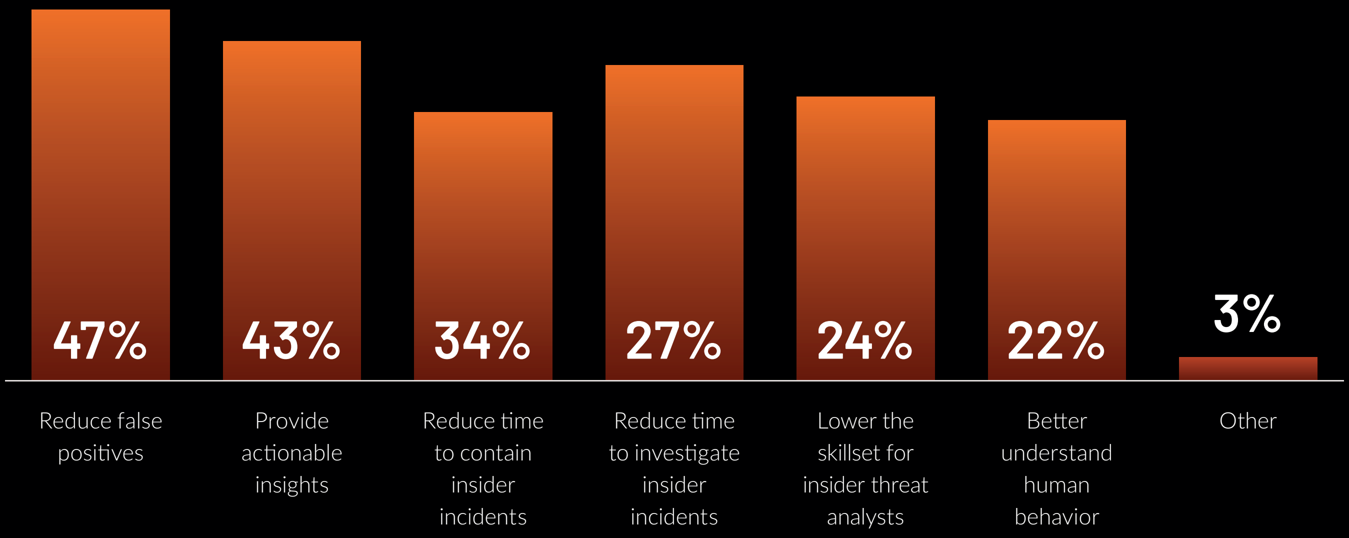


Figure 22: Two responses permitted

Agentic AI. Adoption and defense

Nineteen percent of organizations have deployed AI agents in daily workflows, with 71% rating them important to extremely important for early insider risk detection.

Agentic AI adoption for insider risk detection and prevention

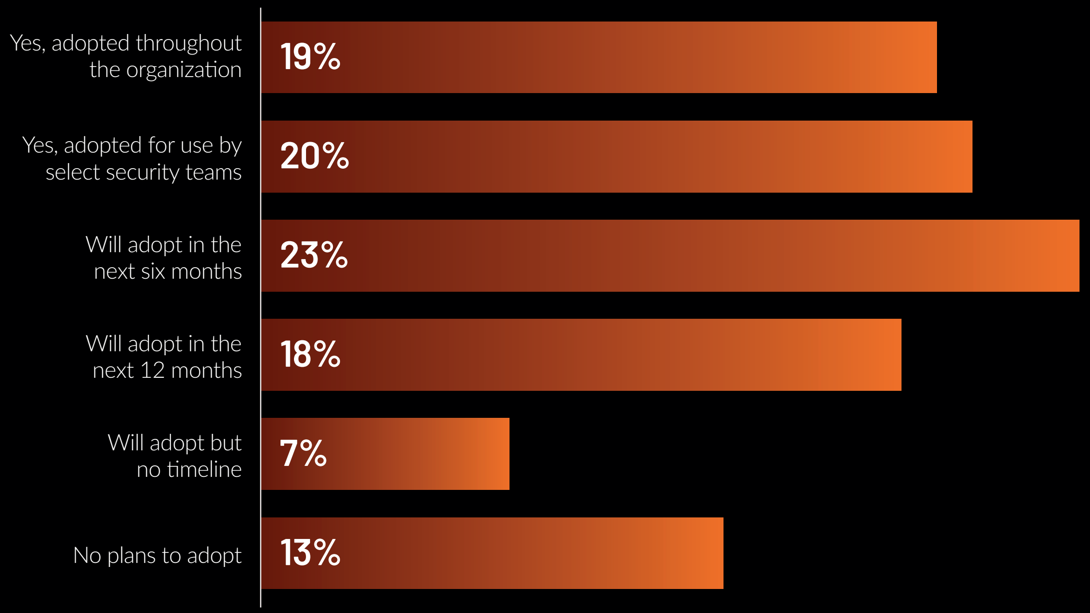


Figure 23

The importance of agentic AI in detecting insider risks early

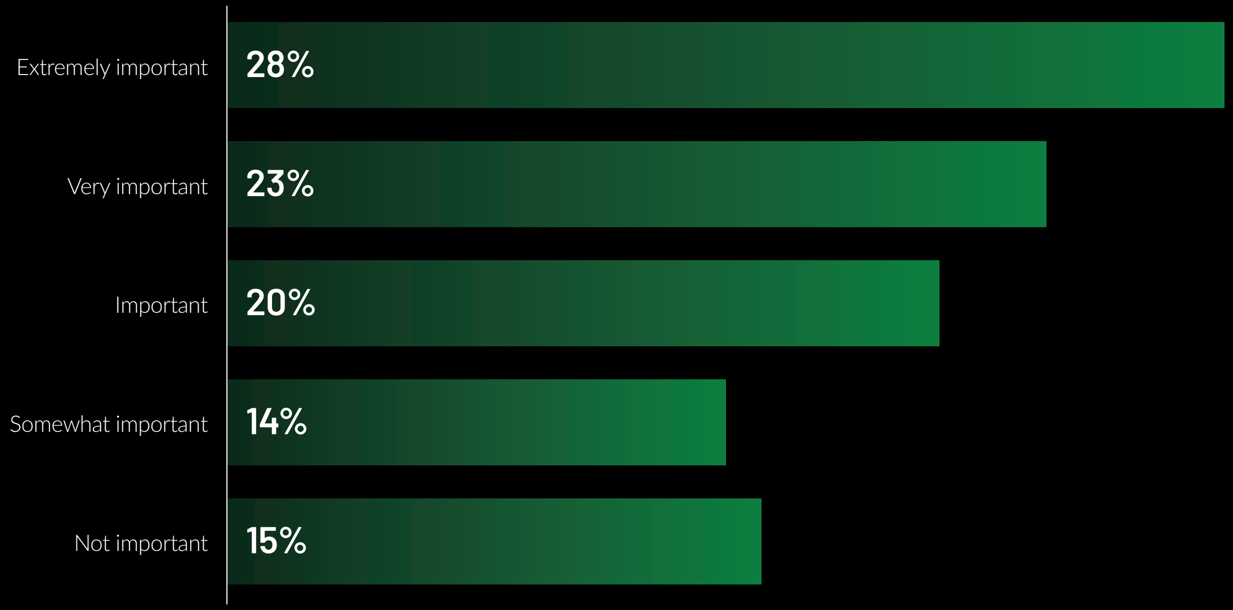


Figure 24

Insider risk budgets grow. Demand outpaces funding

Sixty-four percent of organizations increased their budgets for insider risk management in 2025. The top two reasons were to hire and retain IT security practitioners (44%), and to invest in technologies that can prevent and detect insider risks (42%).

Despite investments growing, 45% say insider risk management budgets are still insufficient, and 70% expect budgets to increase in 2026. Of those, 28% expect budgets to increase by 10% or more.

Top reasons for increasing insider risk management budget

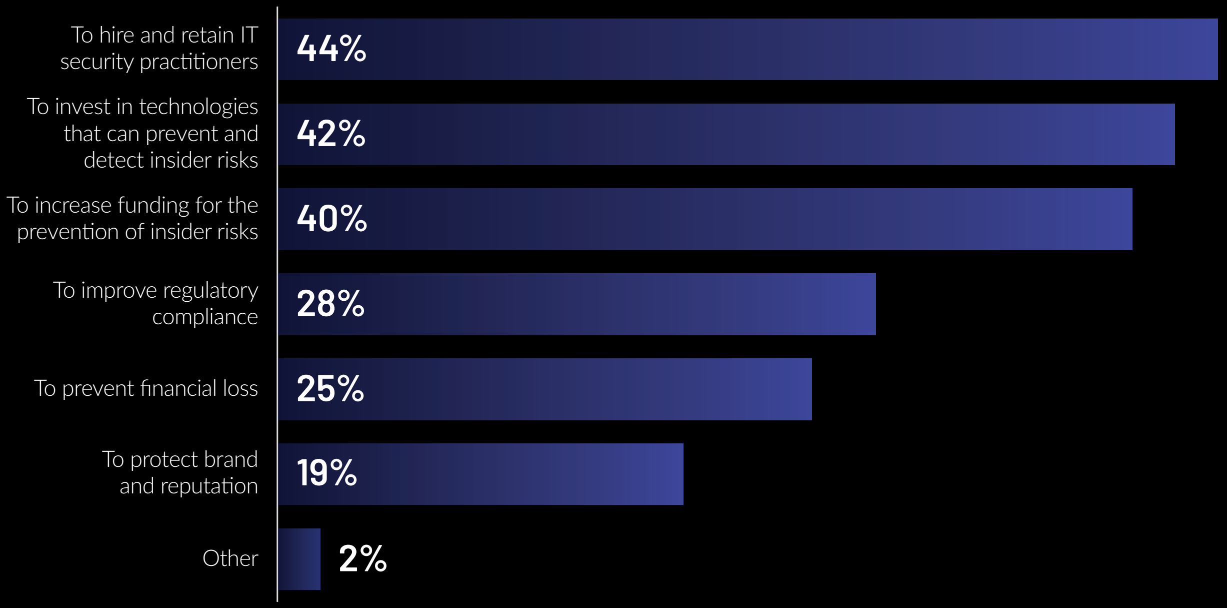


Figure 25: Two responses permitted

2026 insider risk management funding outlook

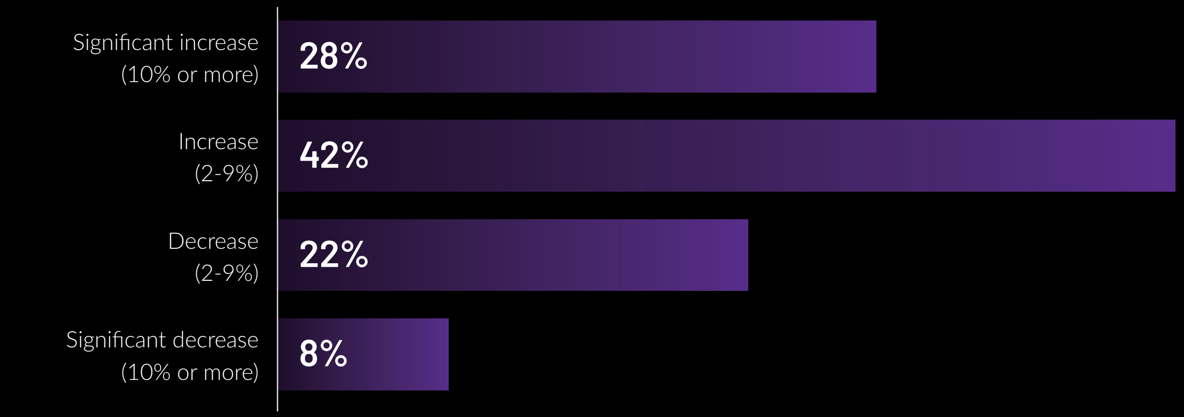


Figure 26

Insider risk management. Budget allocation

In 2025, organizations dedicated an average of 19% of their IT security budget to insider risk management (up from 8.2% in 2023).

Percentage of IT security budget allocated to insider risk management in 2025

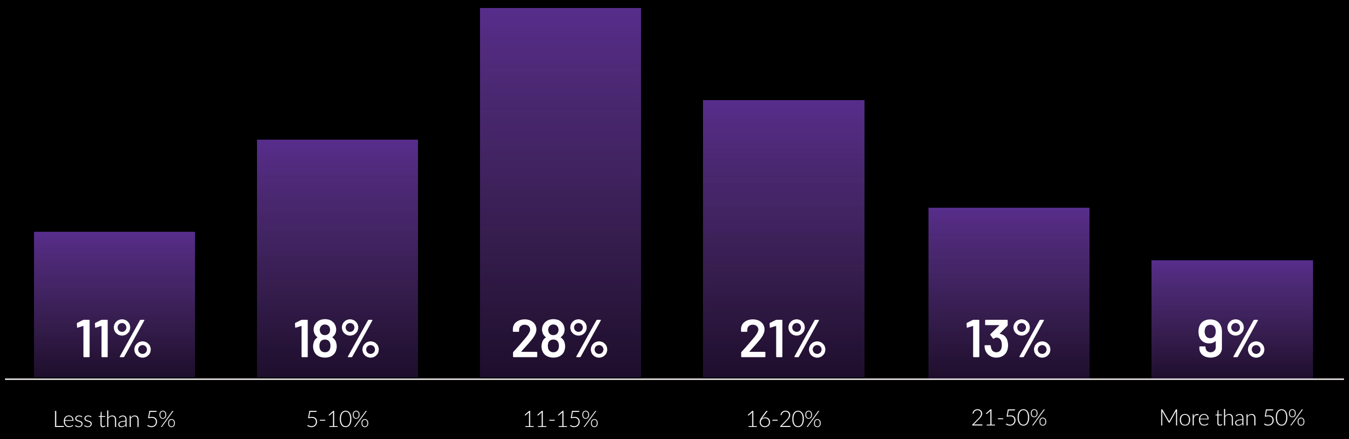


Figure 27

Who pays for it? Funding insider risk management

Responsibility and budget for insider risk management is split across the business. According to the research, legal (20%), and fraud and investigations (20%) are most responsible for funding insider risk management.

Department most responsible for funding insider risk management

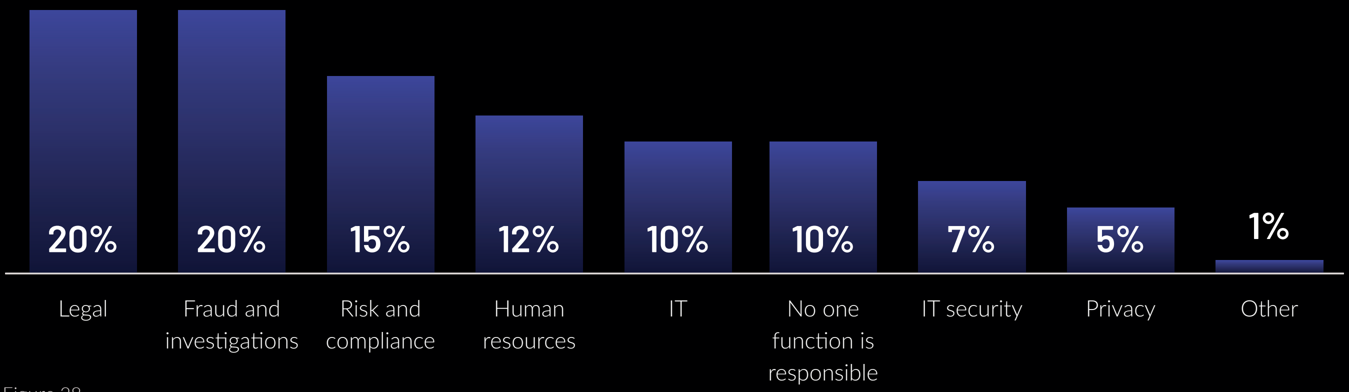


Figure 28

Budget barriers. What holds funding back

About half (51%) of organizations say getting budget for insider risk management is a challenge. The top two reasons cited were lack of collaboration across security, HR, legal, and compliance (58%) and difficulty demonstrating ROI from insider risk management programs (49%).

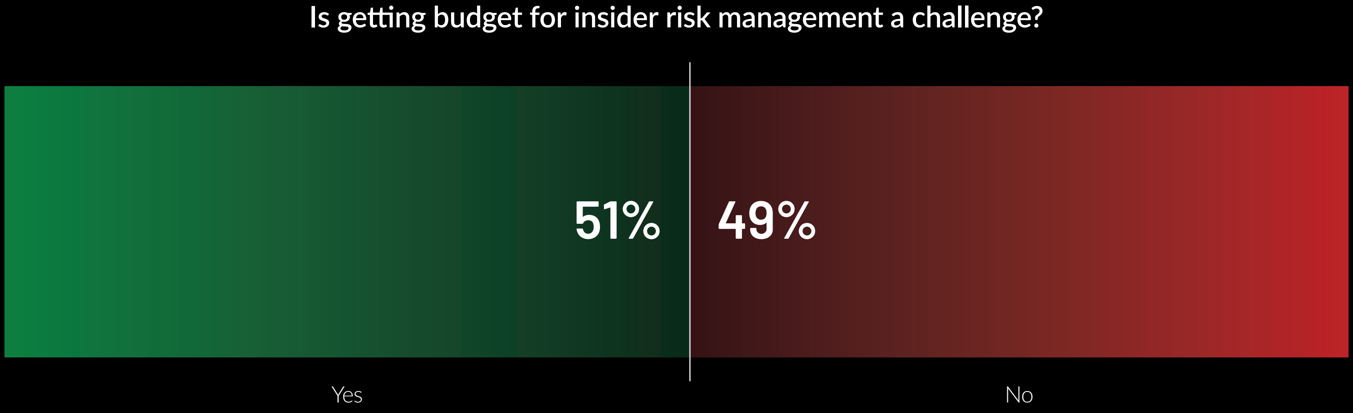


Figure 29

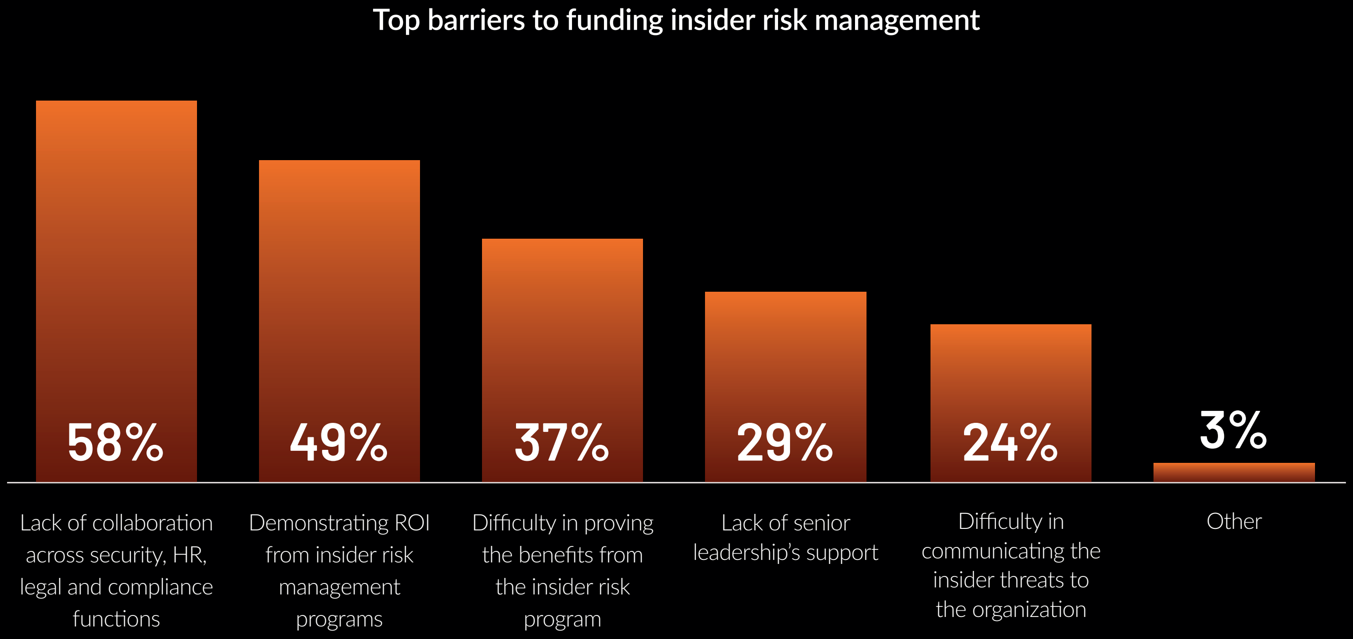


Figure 30: Two responses permitted

The business case. Justifying insider risk management

Forty percent of respondents say the primary reason for having an insider risk program is to be proactive in preventing insider risk incidents. When asked why a dedicated insider risk program has a greater advantage over other security strategies, 50% of respondents say it enables the identification of insider behavior that is not considered normal.

Top business reasons for having an insider risk program

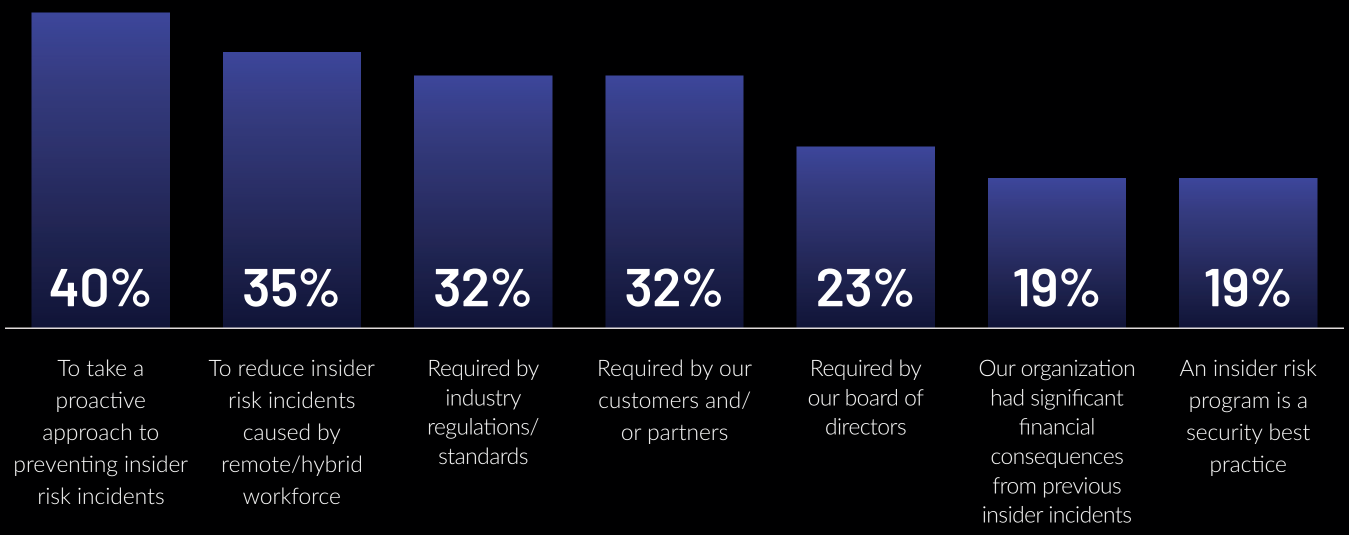


Figure 31: Two responses permitted

Capabilities unique to insider risk programs

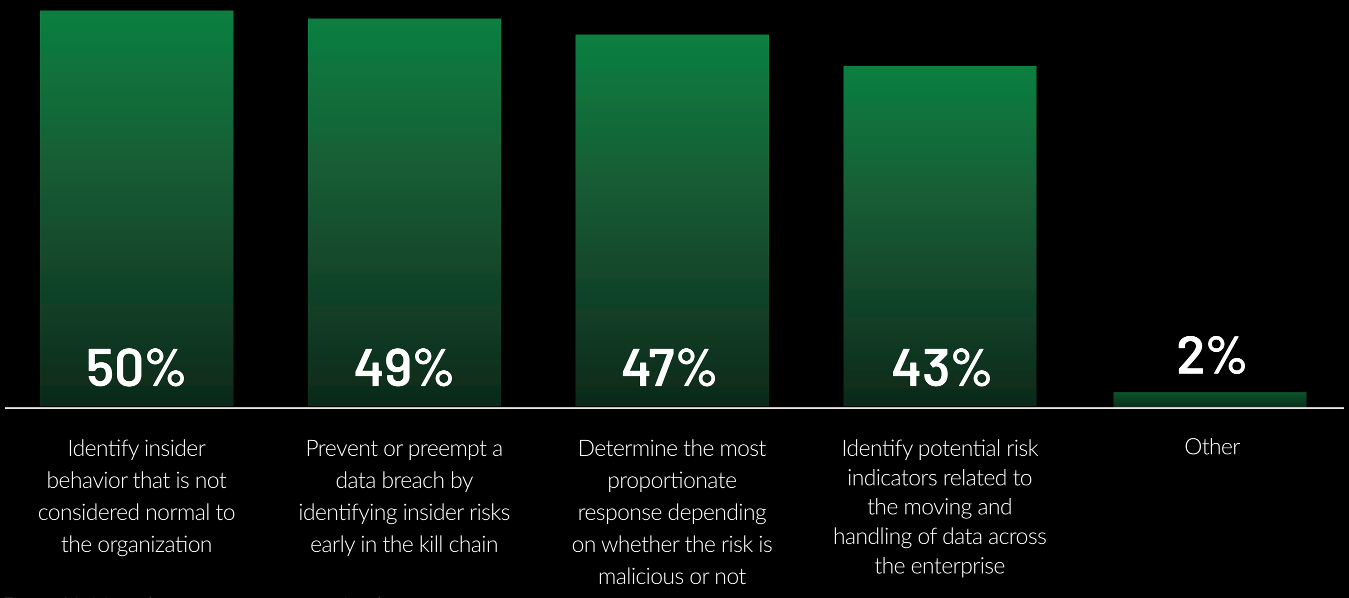


Figure 32: More than one response permitted

Insider risk prevention. By the numbers

Eighty-two percent of organizations have or plan to have an insider risk management program. Those running a program (63%) said it enabled them to avoid an average of seven insider security incidents in the past 12 months.

Organizations with an insider risk management program

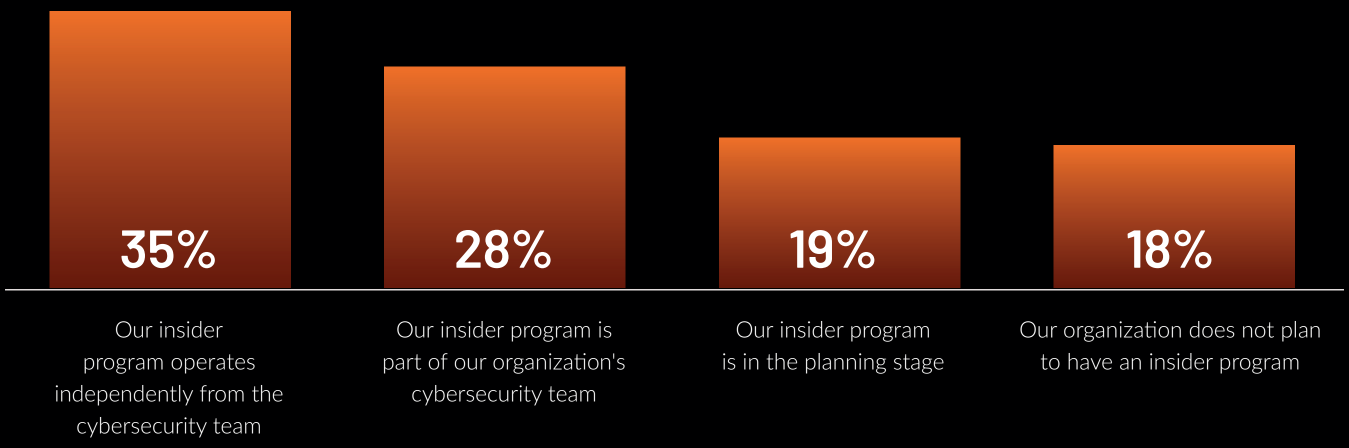


Figure 33

Average number of insider incidents avoided due to having a dedicated insider risk program in the past 12 months

Extrapolated average:
7 avoided incidents

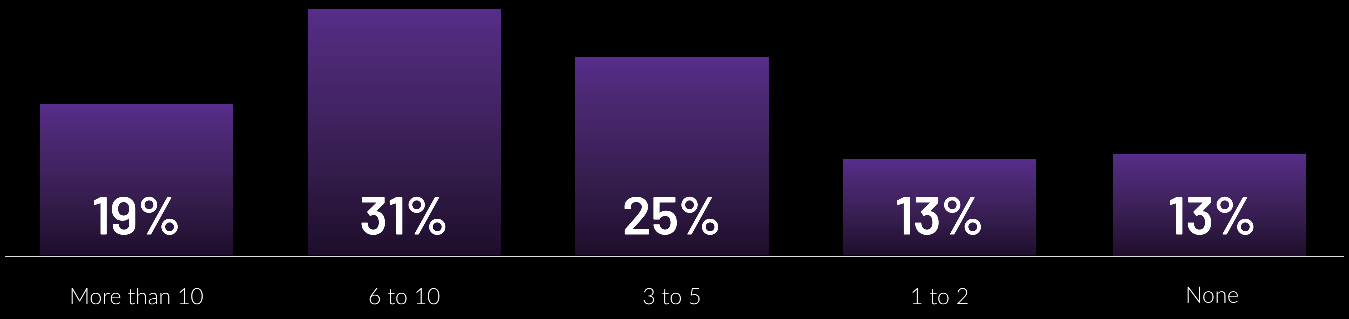


Figure 34

Prevention enablers. What's working

Behavioral intelligence.

Of the organizations using behavioral intelligence for insider risk management (42%), 71% say it is important to essential for insider risk prevention and detection.

Risk-adaptive policy automation.

Of the organizations using risk-adaptive policy automation for insider risk management (26%), 71% say it is important for insider risk prevention and detection.

Consolidation.

Sixty-seven percent of organizations rate technology consolidation as important to essential for insider risk prevention and detection.

Top benefits of consolidation

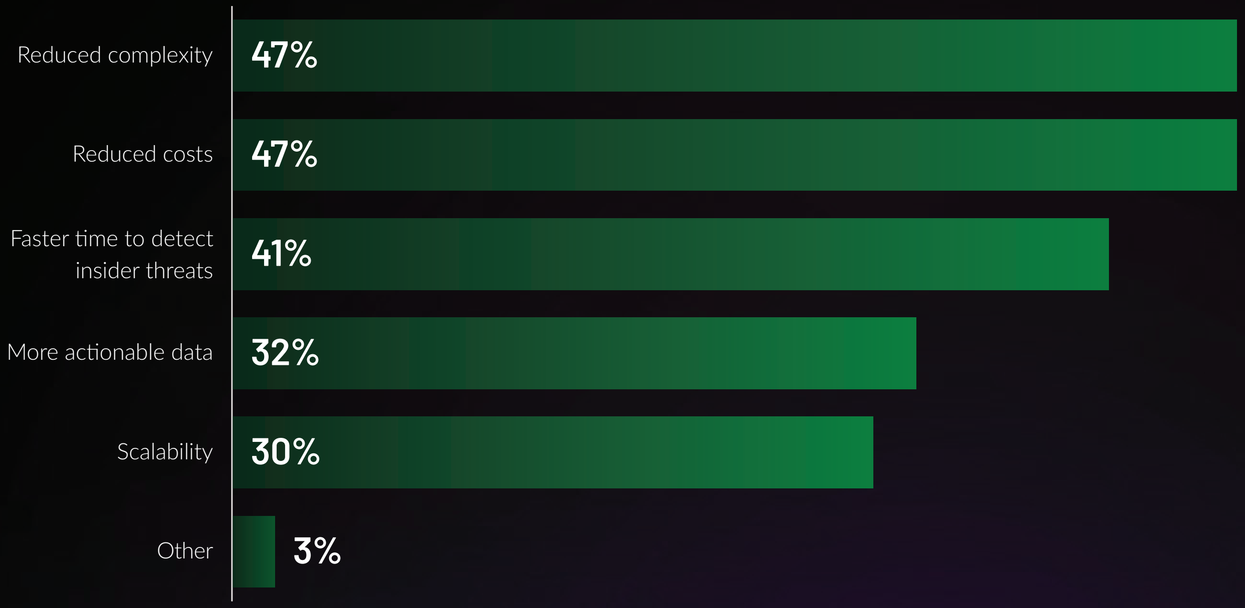


Figure 35: Two responses permitted

Insider risk management programs.

Of the organizations with an insider risk management program, 45% say the program reduced the financial consequences of insider risk incidents. Almost half (49%) rate their program as very to highly effective at preventing insider incidents.

Insider risk program incident prevention effectiveness

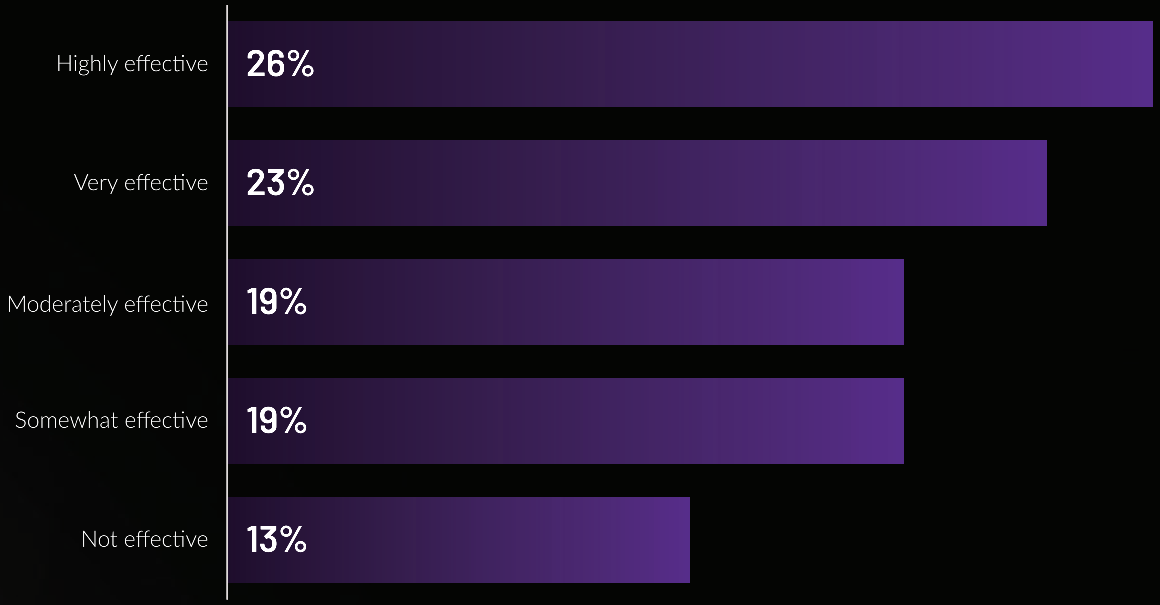


Figure 36

Early behavioral risk detection.

Forty-four percent say their insider risk program helped identify concerning insider behavior that could have caused an incident. Of those, the top two benefits were avoiding the financial consequences from an insider incident (58%) and reducing the time to respond and contain the insider incident (50%). This was followed by preventing loss of sensitive and confidential data (48%), preventing harm to brand and reputation (43%), and other (1%).

Most at risk. By role

Customer service (51%) poses the greatest insider risk followed by IT (49%) and HR (46%).

Roles or functions that pose the greatest insider risk

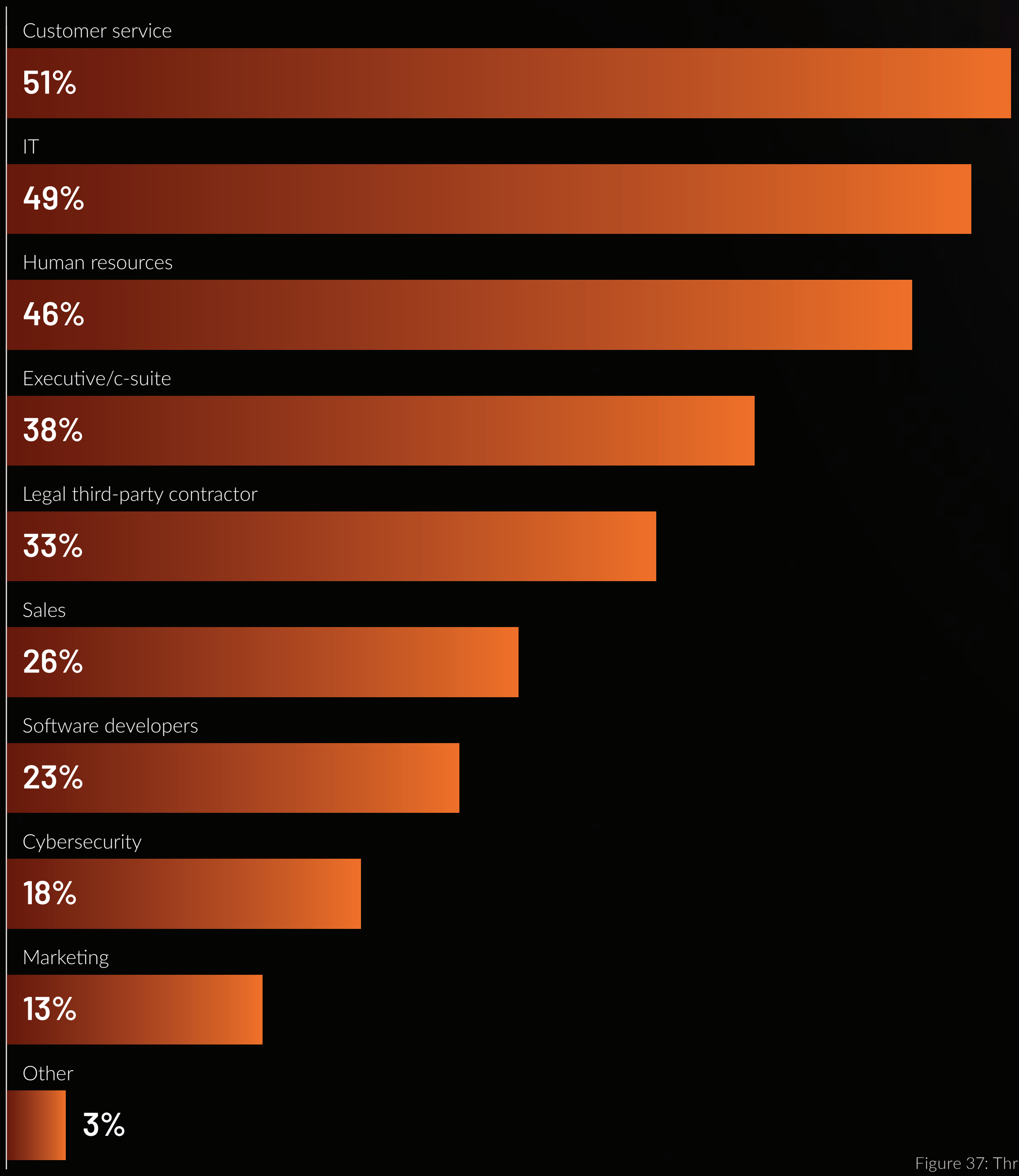


Figure 37: Three responses permitted

Most at risk. By data

Non-sensitive data (51%) is most often involved in insider incidents, followed by personally identifiable information (48%) and intellectual property (46%).

Data types involved in insider incidents

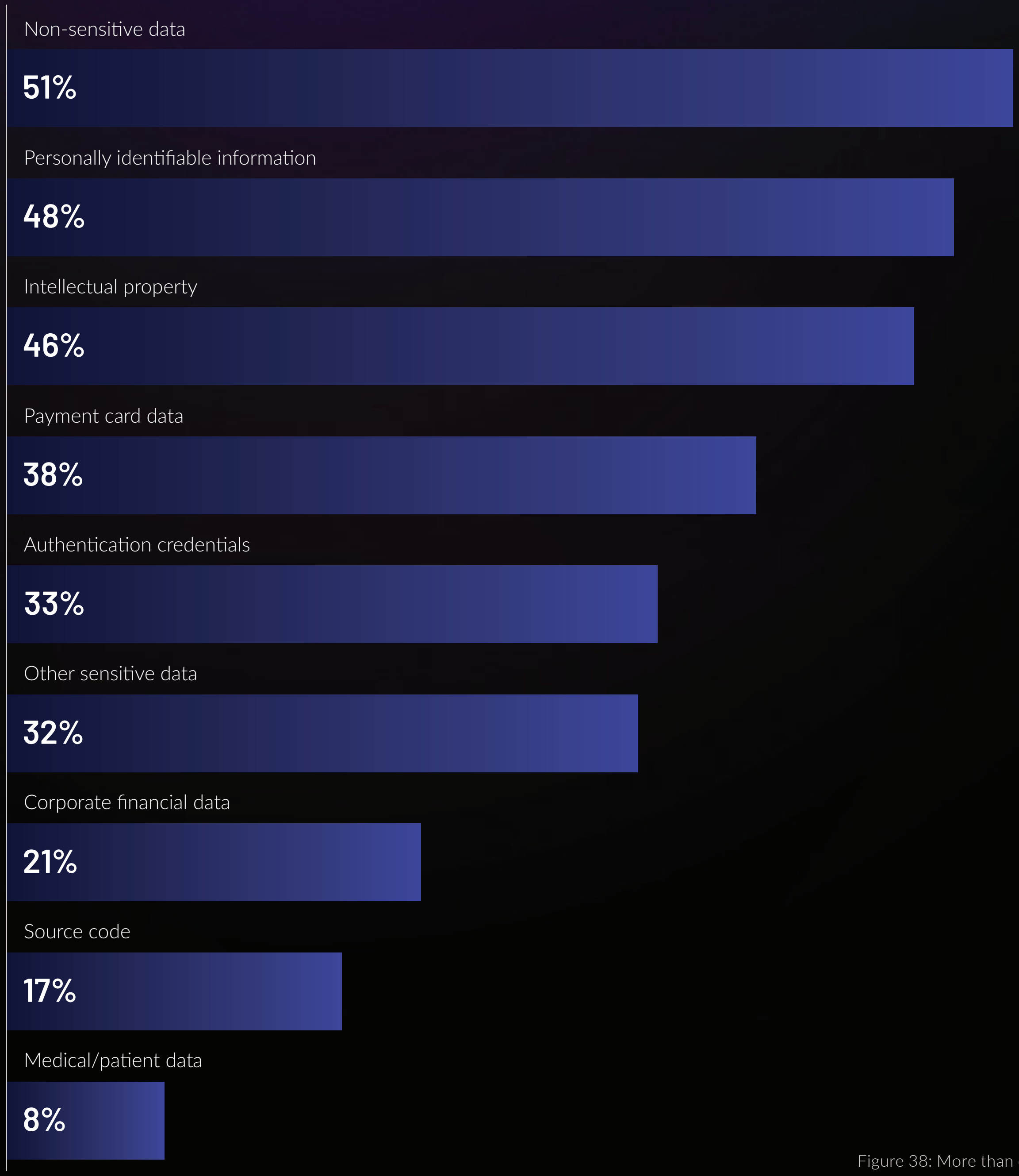


Figure 38: More than one response permitted

DEMOGRAPHICS

Industry sectors of participating organizations

Figure 39 reports the industry distribution of respondents' organizations. This chart identifies financial services (14%) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by industrial (11%), services (9%), and public sector (8%).

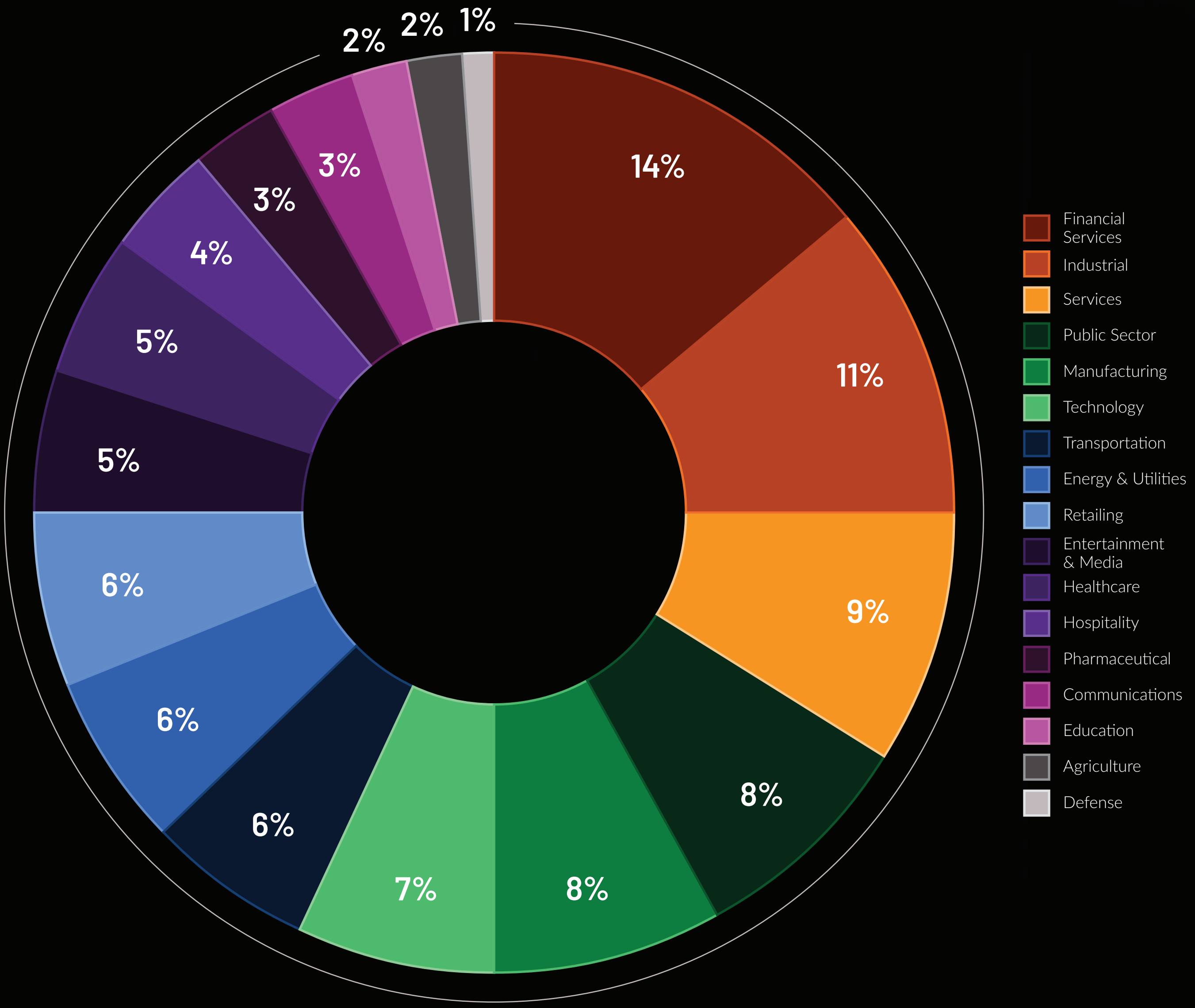


Figure 39

Respondents by position level or function

Figure 40 reports the respondents' organizational level within participating organizations. Sixty-seven percent of respondents are at or above the supervisory levels. The largest category at 18% of respondents is director.

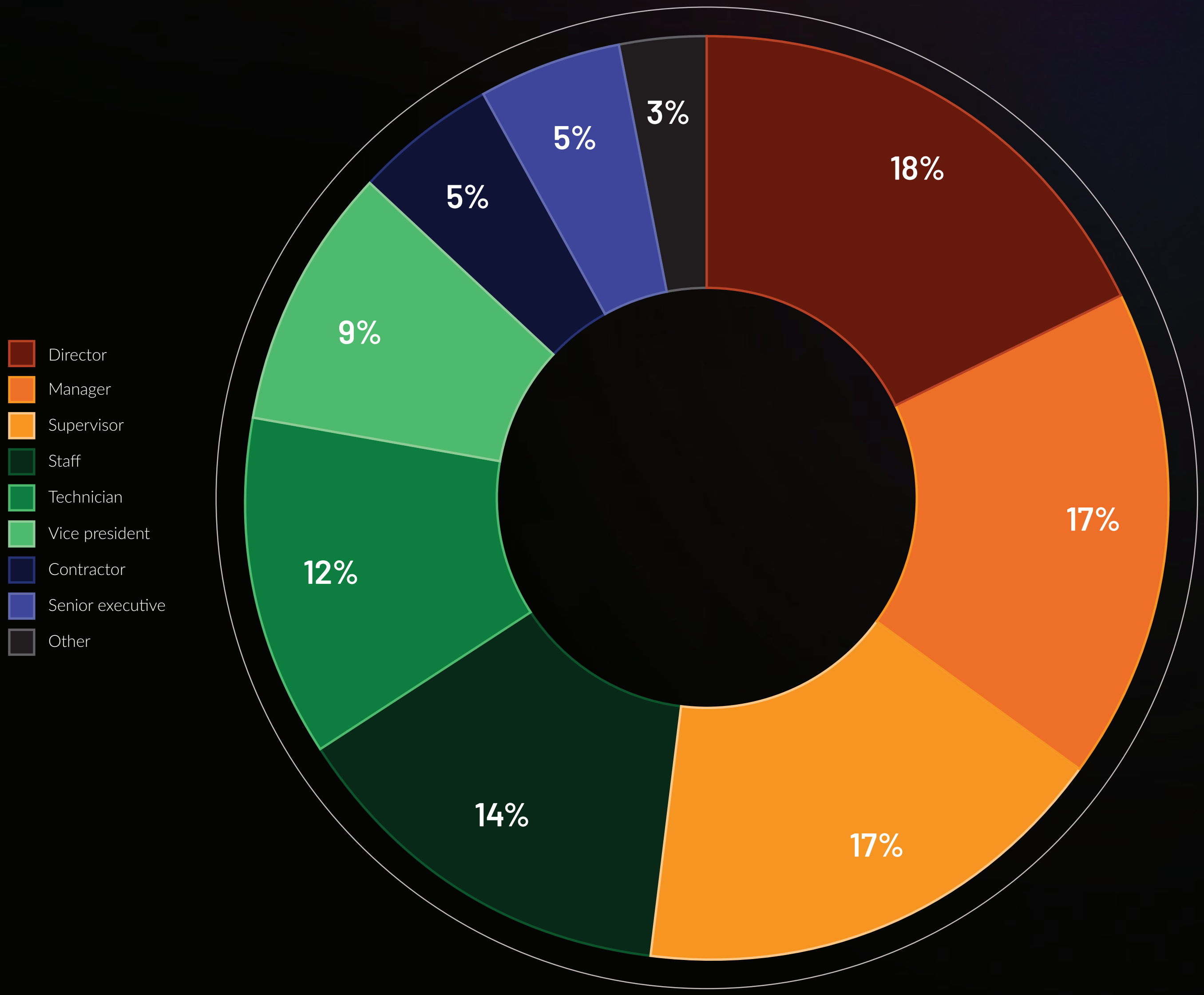


Figure 40

Direct reporting channel

As shown in Figure 41, 19% of respondents report to the chief information officer, 16% of respondents report to the chief information security officer, 12% of respondents report to the business or line-of-business (LOB) leadership, 12% report to the chief risk officer and, 11% report to the chief security officer.

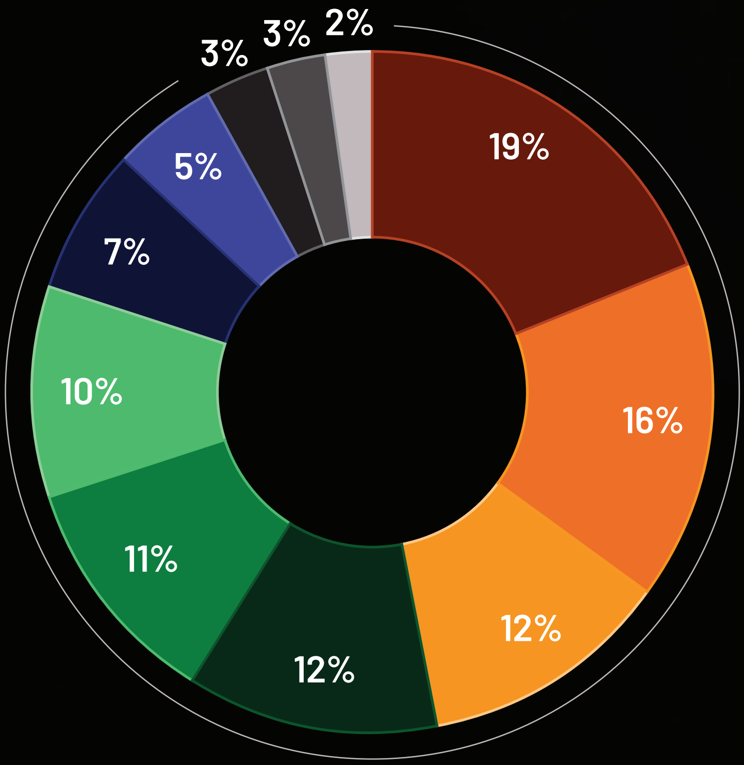


Figure 41

Headcount (size) for participating organizations companies

Figure 42 shows the percentage distribution of companies according to global headcount, which is a surrogate for organizational size.

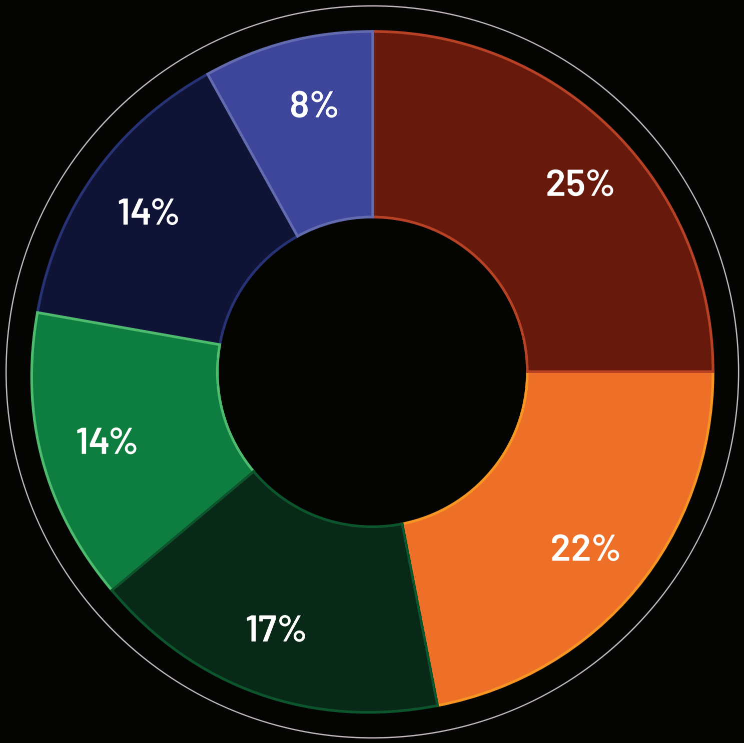


Figure 42

CONCLUSION

From proof to practice. Closing the AI-insider gap

The evidence is clear: organizations have come a long way. Insider risk management programs are delivering measurable results. Preventing an average of seven incidents per year, cutting containment time by 17%, and avoiding $8.2M in costs are not theoretical gains; they reflect a maturing discipline that works.

What the data also makes clear is where to focus next.

Insider risk is now driven less by intent and more by behavior, amplified by AI, expanding identities, and visibility gaps.

As AI reshapes how work gets done, risk increasingly emerges from interactions between people, machines, and data. Programs anchored only in traditional controls will struggle to keep pace.

The opportunity is to double down on what works:

- Behavioral intelligence to surface early, non-obvious risk signals before incidents escalate.
- Identity-centric security that governs humans, service accounts, and AI agents with equal rigor.
- Defensive AI that improves precision, reduces false positives, and enables risk-aware prevention at scale.
- Governance and data classification as foundational controls to close AI-driven exposure gaps.
- A mindset shift from human-only risk to human-plus-machine risk, recognizing AI as an operational insider.

AI is testing every organization's risk posture. The opportunity is to build on what already works, close the remaining gaps, and align programs with how work is actually performed. Organizations that do so will be better positioned to contain incidents faster, reduce losses, and sustain progress as insider risk continues to evolve.

FRAMEWORK

The purpose of this research is to provide guidance on what an insider risk can cost an organization.

This cost study is unique in addressing the core systems and business process-related activities that drive a range of expenditures associated with a company's response to insider incidents arising from negligence/mistakes, compromise (i.e., credential theft), or malicious/criminal behaviors. In this study, we define an insider-related incident as one that results in the diminishment of a company's core data, networks, or enterprise systems.

Our benchmark methods attempt to elicit the actual experiences and consequences of insider-related incidents. Based on interviews with a variety of senior-level individuals in each organization we classify the costs according to two different cost streams:

- The costs related to minimizing insider risks or what we refer to as the internal cost activity centers.
- The costs related to the consequences of incidents, or what we refer to as the external effect of the event or attack.

We analyze the internal cost centers sequentially starting with monitoring and surveillance of the insider risk landscape and ending with remediation activities. Also included are the costs due to lost business opportunities and business disruption. In each of the cost activity centers we asked respondents to estimate the direct costs, indirect costs and, when applicable, opportunity costs.

These are defined as follows:

- **Direct cost:** The direct expense outlay to accomplish a given activity.
- **Indirect cost:** The amount of time, effort and other organizational resources spent, but not as a direct cash outlay.
- **Opportunity cost:** The cost resulting from lost business opportunities as a consequence of reputation diminishment after the incident.

External costs such as the loss of information assets, business disruption, equipment damage, and revenue loss were captured using shadow-costing methods. Total costs were allocated to seven discernible cost vectors.[3]

[3] We acknowledge that these seven cost categories are not mutually independent and they do not represent an exhaustive list of all cost activity centers.

This study addresses the core process-related activities that drive a range of expenditures associated with a company's response to insider-related incidents.

The seven internal cost activity centers in our framework include:[4]

- **Monitoring and surveillance:** Activities that enable an organization to reasonably detect and possibly deter insider incidents or attacks. This includes allocated (overhead) costs of certain enabling technologies that enhance mitigation or early detection.
- **Investigation:** Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents.
- **Escalation:** Activities taken to raise awareness about actual incidents among key stakeholders within the company. The escalation activity also includes the steps taken to organize an initial management response.
- **Incident response:** Activities relating to the formation and engagement of the incident response team including the steps taken to formulate a final management response.
- **Containment:** Activities that focus on stopping or lessening the severity of insider incidents or at-tacks. These include shutting down vulnerable applications and endpoints.
- **Ex-post response:** Activities to help the organization minimize potential future insider-related incidents and attacks. It also includes steps taken to communicate with key stakeholders both within and outside the company, including the preparation of recommendations to minimize potential harm.
- **Remediation:** Activities associated with repairing and remediating the organization's systems and core business processes. These include the restoration of damaged information assets and IT infrastructure.

In addition to the above process-related activities, organizations often experience external consequences or costs associated with the aftermath of incidents. Our research shows that four general cost activities associated with these external consequences are as follows:

- **Cost of information loss or theft:** Loss or theft of sensitive and confidential information as a result of an insider attack. Such information includes trade secrets, intellectual properties (including source code), customer information, and employee records. This cost category also includes the cost of data breach notification in the event that personal information is wrongfully acquired.
- **Cost of business disruption:** The economic impact of downtime or unplanned outages that prevent the organization from meeting its data processing requirements.
- **Cost of equipment damage:** The cost to remediate equipment and other IT assets as a result of in-sider attacks to information resources and critical infrastructure.
- **Lost revenue:** The loss of customers (churn) and other stakeholders because of system delays or shutdowns as a result of an insider attack. To extrapolate this cost, we use a shadow costing method that relies on the 'lifetime value' of an average customer as defined for each participating organization.

[4] Internal costs are extrapolated using labor (time) as a surrogate for direct and indirect costs. This is also used to allocate an overhead component for fixed costs such as multiyear investments in technologies.

BENCHMARKING

Our benchmark instrument is designed to collect descriptive information from IT, information security and other key individuals about the actual costs incurred either directly or indirectly as a result of insider-related incidents or attacks actually detected. Our cost method does not require subjects to provide actual accounting results, but instead relies on estimation and extrapolation from interview data over a four-week period.

Cost estimation is based on confidential diagnostic interviews with key respondents within each benchmarked organization. Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant. Within each category, cost estimation was a two-stage process. First, the benchmark instrument required individuals to rate direct cost estimates for each cost category by marking a range variable defined in the following number line format.

How to use the number line:

The number line provided under each data breach cost category is one way to obtain your best estimate for the sum of cash outlays, labor, and overhead incurred. Please mark only one point somewhere between the lower and upper limits set above. You can reset the lower and upper limits of the number line at any time during the interview process.

Post your estimate of direct costs here for [presented cost category]

The numerical value obtained from the number line rather than a point estimate for each presented cost category preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

Cost estimates were then compiled for each organization based on the relative magnitude of these costs in comparison to a direct cost within a given category. Finally, we administered general interview questions to obtain additional facts, including estimated revenue losses as a result of the insider-related incident or attack.

The size and scope of survey items was limited to known cost categories that cut across different industry sectors. In our experience, a survey focusing on process yields a higher response rate and better quality of results. We also used a paper instrument, rather than an electronic survey, to provide greater assurances of confidentiality.

To maintain complete confidentiality, the survey instrument did not capture company-specific information of any kind. Subject materials contained no tracking codes or other methods that could link responses to participating companies.

We carefully limited items to only those cost activities considered crucial to the measurement of cost to keep the benchmark instrument to a manageable size. Based on discussions with learned experts, the final set of items focused on a finite set of direct or indirect cost activities. After collecting benchmark information, each instrument was examined carefully for consistency and completeness. In this study, a few companies were rejected because of incomplete, inconsistent, or blank responses.

LIMITATIONS

Our study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research.

However, there are inherent limitations with this benchmark research that need to be carefully considered before drawing conclusions from findings.

- **Non-statistical results:** Our study draws upon a representative, non-statistical sample of organizations experiencing one or more insider-related incidents during the past 12 months. Statistical inferences, margins of error, and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.
- **Non-response:** The current findings are based on a small representative sample of benchmarks. In this study, 354 companies completed the benchmark process. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of underlying data breach cost.
- **Sampling-frame bias:** Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.
- **Company-specific information:** The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category.
- **Unmeasured factors:** To keep the interview script concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined.
- **Extrapolated cost results:** The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy, and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant, or improper questions.

Unified security for the human and AI enterprise

DTEX is the leader in risk-adaptive security, unifying human, data, and AI risk through a behavioral intelligence platform. Built for enterprise scale, it detects threats early and prevents breaches. Organizations and governments worldwide rely on DTEX to protect sensitive data, accelerate innovation, and safeguard trust with privacy-by-design telemetry and adaptive controls. The DTEX Platform integrates insider risk management, data loss prevention, user and entity behavior analytics, user activity monitoring, and AI security into one cohesive solution. To learn more about DTEX, visit dtex.ai

Unified security for the human and AI enterprise

dtex.ai

DTEX