Cost of Insider Risks

GLOBAL REPORT

2023

Independently conducted by Ponemon Institute | DTEX

Table of contents

About the cover

The lines on the front cover represent the types and occurrence of insider risks; blue being negligent or mistaken insiders (the most common, as the findings from this study will illustrate) followed by malicious (in red) and outsmarted (purple). The upward direction is indicative of the time and costs following an insider incident; the longer it takes to contain, the higher the cost. Our cover is a visual representation of the current insider risk landscape. It is a cautionary tale for organizations to shift the needle to a proactive state, left of boom.

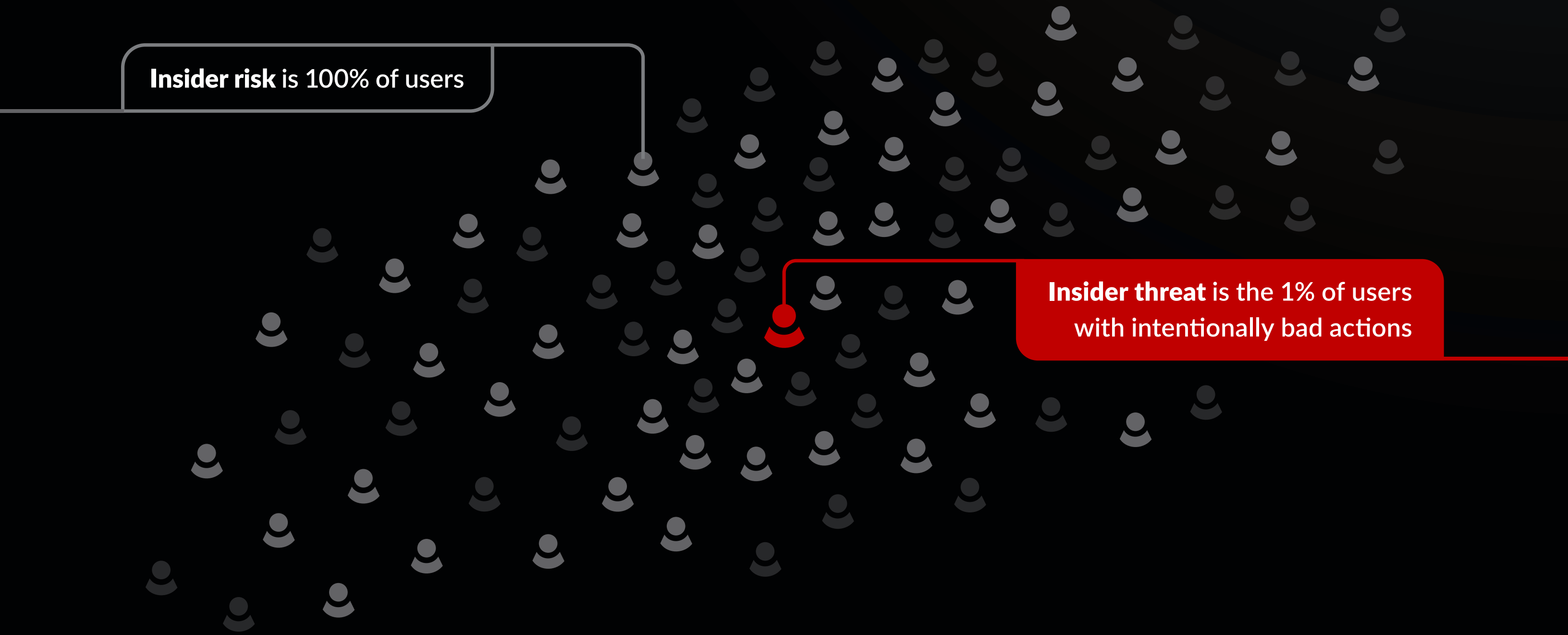
Ponemon Institute is pleased to present the findings of the 2023 Cost of Insider Risks Global Report sponsored by DTEX Systems.

This is the fifth benchmark study conducted to understand the financial consequences that result from insider risks. For the first time, the report features new insights on how organizations are funding their insider risk management programs and strategies.

If you don't understand the risk, you will never understand the threat.

The first Cost of Insider Threats Global Study was conducted in 2016 and focused exclusively on companies in North America. Since then, the research has expanded to include organizations in Europe, Middle East, Africa and Asia-Pacific with a global headcount of 500 to more than 75,000.

> "Not every insider risk becomes an insider threat; however, every insider threat started as an insider risk."
>
> - Gartner



Insider risk is 100% of users

Insider threat is the 1% of users with intentionally bad actions

Study snapshot

309
Organizations that experienced one or more insider incidents

1,075
IT and IT security practitioners

7,343
Total number of insider incidents

24
Incidents per company

In the context of this research, insider risks are defined as:

Malicious

An insider who seeks to cause harm

Non-malicious

An insider who does not seek to cause harm

NEGLIGENT
An insider who causes harm through carelessness or inattentiveness

MISTAKEN
A non-malicious insider who causes harm through a genuine mistake that cannot be attributed to carelessness

OUTSMARTED
A non-malicious insider who causes harm through being reasonably outmaneuvered by an attack or adversary

EXAMPLES

Malicious	Negligent	Mistaken	Outsmarted
Espionage IP threat Unauthorized disclosure Sabotage Fraud Workplace violence	Ignore warnings	Pressing the incorrect button in a very noisy and stressful environment	Being phished by a new, advanced phishing attack that has not previously been seen in the wild

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

Executive summary

Cyber budgets are failing to proactively address the root cause of data breaches: Insider risks

The cost of an insider risk is the highest it's ever been, as organizations spend more time than ever trying to contain insider incidents. In 2023, the total average annual cost of an insider risk increased to $16.2 million per organization while the average number of days to contain an incident stretched to 86 (up from $15.4 million and 85 days in 2022, respectively). Meanwhile, the number of insider incidents in 2023 increased to 7,343 — up from 6,803 in 2022.

Organizations are spending more time and money than ever on containment over prevention

The biggest cost associated with insider risks happened after the incident had occurred, with containment and remediation representing the most expensive activity centers at $179,209 and $125,221 per incident, respectively. The longer it takes to respond, the higher the cost ($18.33 million for incidents that take longer than 91 days to contain).

Non-malicious insiders accounted for 75% of incidents, from either: negligent or mistaken insiders (55%), or outsmarted insiders who were exploited by an external attack or adversary (20%). While malicious insider incidents were less frequent (25%), they were by far the most expensive, costing on average $701,500 per incident.

Despite the risk within, cyber budgets are still being spent in the wrong places

Despite the growing cost and frequency of insider risks, 88% of organizations devoted less than 10% of their IT security budget to insider risk management (8.2% on average).

According to research analyst Gartner, insider risk management refers to "the tools and capabilities to measure, detect and contain undesirable behavior of trusted accounts within the organization."

The remaining 91.8% of budget was spent on external threats, despite more than half of organizations attributing social engineering as a leading cause of all outside attacks.

The silver lining

The good news is that change is on the way. Organizations are increasingly acknowledging the need to home in on the human element to shift the needle to where it needs to be, from reactive to proactive. Fifty-eight percent of organizations agree current levels of insider risk management funding are inadequate, and almost half of organizations (46%) will increase investment in insider risk programs in 2024.

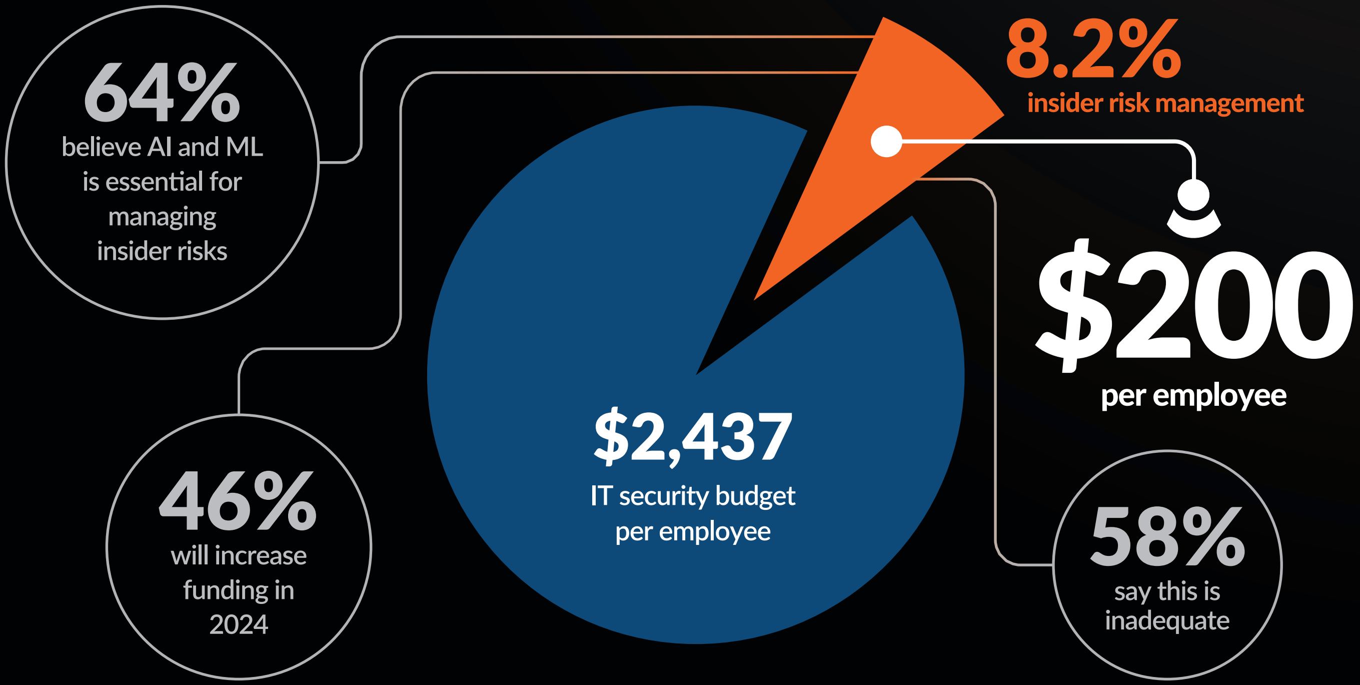
So what?

The upward trends associated with incident costs, frequency, and time to contain demonstrate that current approaches to insider risk are simply not working. In fact, the numbers clearly show we are going backwards.

Funding is being inadvertently misdirected due in part to a widespread misunderstanding of insider risks and how they manifest based on early warning behaviors. A whole-of-industry approach is required to educate and find common ground on how we define and discuss insider risks with enterprise and government entities.

On a positive note, more and more organizations are building insider risk programs and seeking budget and executive buy-in to fund and champion them.

Our research echoes similar findings from other leading analysts and research organizations, notably Forrester, Gartner, MITRE Corporation and Verizon. The human is unquestionably at the center of most data breaches — and increasingly, that human risk is an insider, right under our noses. By homing in on insider risk management, organizations have a powerful opportunity to proactively identify and mitigate insider risks well before a costly incident occurs.



Based on the average number of organizations surveyed. This aligns with other industry studies, including Deloitte Insights: Reshaping the cybersecurity landscape

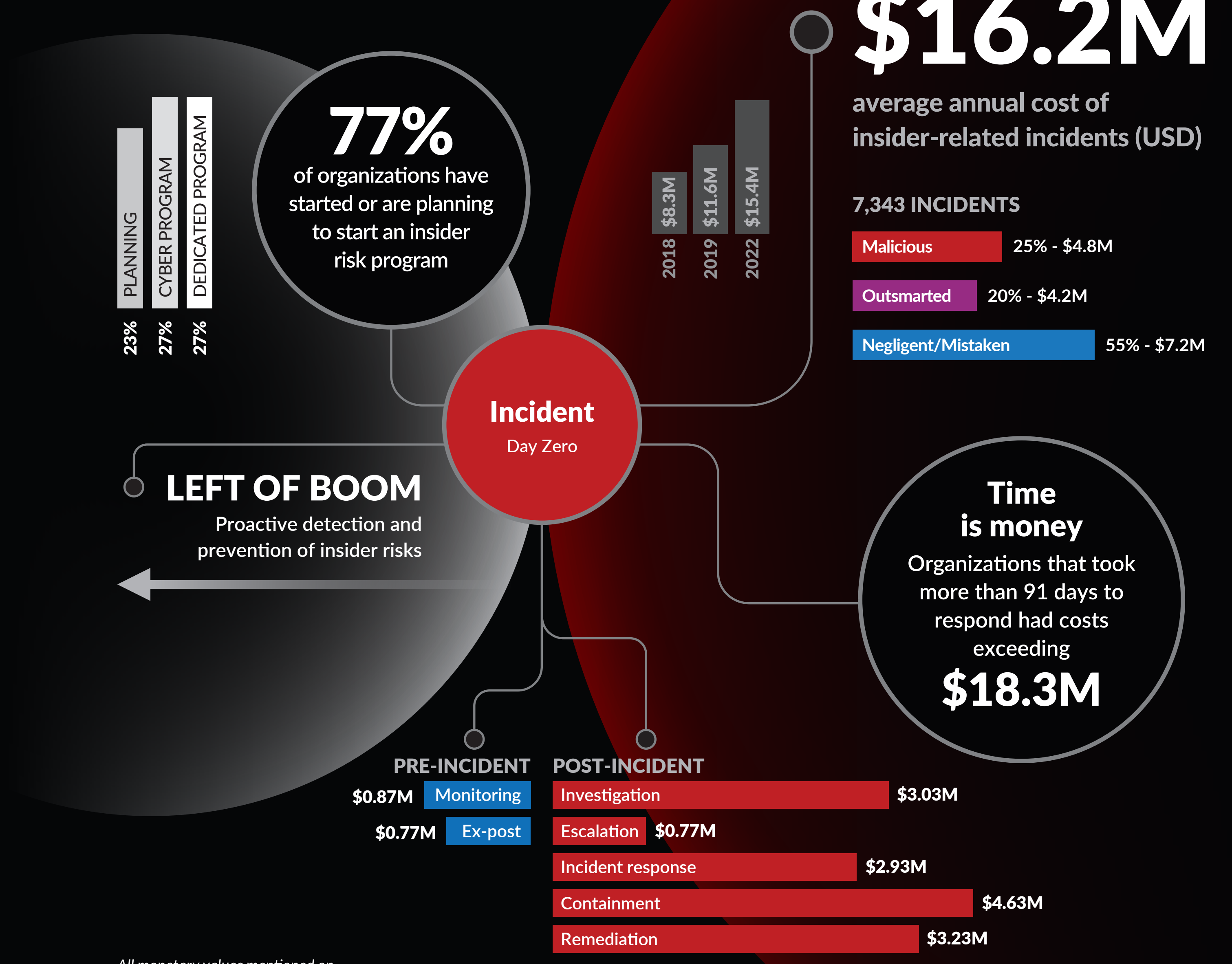
DTEX

It pays to be proactive

The time to contain an insider incident has increased to an average of 86 days.

As revealed in this research, the highest cost burden happens after an incident has occurred. Organizations spend far more money reacting to insider incidents than they do on preventative measures. The longer it takes to respond, the higher the cost ($18.33 million for incidents that take longer than 91 days to contain).

OPPORTUNITY VS COST



PLANNING	23%
CYBER PROGRAM	27%
DEDICATED PROGRAM	27%

77% of organizations have started or are planning to start an insider risk program

2018	$8.3M
2019	$11.6M
2022	$15.4M

$16.2M average annual cost of insider-related incidents (USD)

7,343 INCIDENTS

Malicious	25% - $4.8M
Outsmarted	20% - $4.2M
Negligent/Mistaken	55% - $7.2M

Incident Day Zero

LEFT OF BOOM Proactive detection and prevention of insider risks

Time is money Organizations that took more than 91 days to respond had costs exceeding **$18.3M**

PRE-INCIDENT

$0.87M	Monitoring
$0.77M	Ex-post

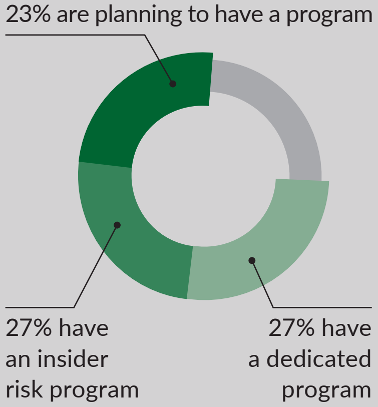
POST-INCIDENT

Investigation	$3.03M
Escalation	$0.77M
Incident response	$2.93M
Containment	$4.63M
Remediation	$3.23M

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

Key findings

77% of organizations have started or are planning to start an insider risk program



For the first time, we asked about how organizations are funding and governing their insider risk management programs and strategies. Our research revealed the following insights.

Organizations are spending less than 10% of their IT security budget per year trying to solve a $16.2 million (and growing) problem.

Organizations had an average IT security budget of $2,437 per employee, yet only 8.2% (equivalent to $200 per employee) was allocated specifically to insider risk management programs and policies.

Most organizations agree this level of funding is not enough.

Fifty-eight percent of organizations said current funding levels for insider risk management are inadequate. This lack of funding has likely put insider risk programs on the back foot, causing many organizations to be reactive instead of proactive.

Most insider risk budget is spent after an insider incident has occurred.

Only 10% of insider risk management budget (averaging $63,383 per incident) was spent on pre-incident activity cost centers: $33,596 on monitoring and surveillance, and $29,787 on ex-post analysis (this includes activities to minimize potential future insider incidents and steps taken to communicate recommendations with key stakeholders). The remaining 90% (averaging $565,363 per incident) was spent on post-incident activity cost centers: $179,209 on containment, $125,221 on remediation, $117,504 on investigation, $113,635 on incident response, and $29,794 on escalation.

Nearly half of organizations expect insider risk management funding will increase.

Thirty percent expect a mild increase (3-10%) in funding, while 16% expect a significant increase (10% or more).

Most organizations have started or are planning to start an insider risk program.

Seventy-seven percent of organizations have started or are planning to start an insider risk program. Of those organizations, 23% are planning to have a program, 27% have an insider risk program as part of their cybersecurity program, and 27% have a dedicated program that sits outside of the cyber function.

Having top-down support is the most critical element of a successful insider risk program.

Fifty-two percent of organizations that have or are planning to have a dedicated insider risk program selected top-down support as a key feature of the program. Having a dedicated team (from legal, HR, lines of business and security) was also selected as a key feature of an insider risk program (51%). The selection of these features is indicative of many organizations' acceptance that insider risk requires a human-centric solution.

Most organizations put insider risk management outside of IT security.

The department most commonly responsible for insider risk management was legal (34%) followed by IT (23%), and risk and compliance (21%). Only 6% of organizations said IT security was responsible for insider risk management, while only 7% said no one function was more responsible.

More key findings

The negligent/mistaken insider causes the most incidents.

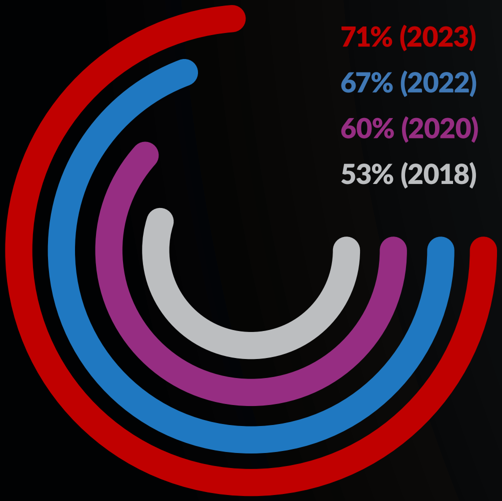
In 2023 there were 4,019 insider incidents related to employee negligence or employee mistakes. This equates to 55% of all incidents experienced by organizations represented in this research, costing on average $505,113 per incident. The average annual cost to remediate these incidents was $7.2 million – up from $6.6 million in 2022. Examples include not ensuring devices are secured, not following the company's security policy, or forgetting to patch and upgrade.

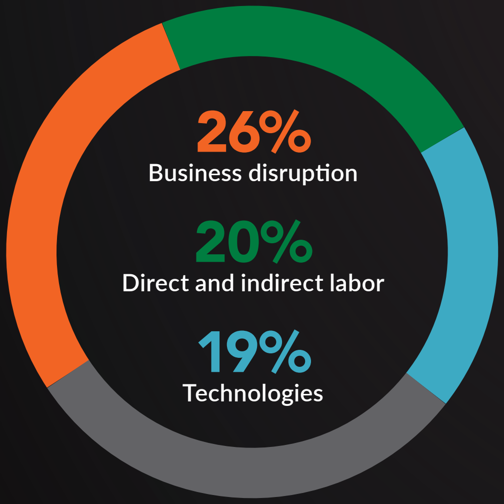
Malicious insiders are less common but cost the most.

Malicious insiders accounted for 1,874 incidents (25%), costing an average of $701,500 per incident. The average annual cost of an incident by malicious insiders was $4.8 million, up from $4.1 million in 2022. Malicious insiders are employees or authorized individuals who use their data access for harmful, unethical, or illegal activities. By virtue of their wider available access to information, malicious insiders are generally harder to detect compared with external attackers or hackers.

Credential theft incidents average $679,621 per incident.

The outsmarting of insiders via social engineering is a go-to tactic for many external attackers looking to steal credentials to get access to critical data and information. In 2023, 1,450 20%) of outsmarted insider incidents involved stolen credentials, at an average annualized cost of $4.2 million – down from $4.6 million in 2022..





More organizations are having more than 21 incidents per year.

According to the 2023 findings, 71% of companies are experiencing between 21 and more than 40 insider incidents per year. This is an increase from 67% in 2022 of companies having between 21 and more than 40 incidents.

Disruption or downtime and direct and indirect labor represent the most significant costs when dealing with insider risks.

The three largest costs are the impact of business disruption due to diminished employee productivity (26% of total cost), direct and indirect labor (20% of total cost) and technology (19% of total cost), which includes the amortized value and the licensing for software and hardware that are deployed in response to insider-related incidents.

Organizational size affects the cost per incident.

The cost of incidents varies according to organizational size. Large organizations with a headcount of more than 75,000 spent an average of $24.60 million over the past year to resolve insider-related incidents. To deal with the consequences of an insider incident, smaller organizations with a headcount below 500 spent an average of $8 million.

Companies spend the most on containment of the insider security incident.

An average of $179,209 is spent to contain the consequences of an insider risk. The least amount of average cost is for escalation at $29,794 and monitoring and surveillance at $33,596. Incidents that took less than 31 days to contain had the lowest average total cost of activities at $11.92 million. In contrast, average activity costs for incidents that take more than 91 days is $18.33 million – up from $17.19 million in 2022.

North American companies are spending more than the average cost on activities that deal with insider risks.

The total average cost of activities to resolve insider risks over a 12-month period is $16.2 million. Companies in North America experienced the highest total cost at $19.09 million. European companies had the next highest cost at $17.47 million.

Financial services and service organizations have the highest average activity costs.

The average activity cost for financial services is $20.68 million and services is $19.63 million. Service organizations include accountancy, consultancy, and professional service firms.

Interviews with participants in this research revealed the following insights into insider risks.

In addition to determining the cost of insider risks for companies in this research, we interviewed participants about their experiences with the risk and what they are doing to reduce risks.

The non-malicious insider risk continues to pose the greatest risk to organizations. Seventy-five percent of respondents say the most likely cause of insider risk is non-malicious: a negligent or mistaken insider (55%), or an outsmarted insider who was exploited by an external attack or adversary (20%).

Sales and customer service are the roles or functions that pose the greatest insider risks (48% and 47%, respectively). Functions that pose the least risk are IT and legal third-party contractors at 23% and 29%, respectively.

Malicious insiders are most likely to email sensitive data to outside parties (67%). They are also very likely to access sensitive data not associated with the role or function (66%) and scan for open ports and vulnerabilities (63%).

Cloud and IoT devices are most likely to be the channels where insider-driven data loss occurs (59% and 56%, respectively). Less likely are corporate-owned endpoints (41%) and BYOD endpoints (43%). The channels organizations are most concerned about are IoT (65%) and cloud (61%).

Malware and social engineering attacks were most likely to cause a non-insider attack that led to a data breach, at 56% and 53%, respectively. In the past 12 months, 58% of organizations had a minimum of two non-insider attacks that caused a data breach. Malware is considered the most important attack to prevent (65% of organizations).

Advanced technologies are considered essential to reducing insider risks. User-behavior-based tools for detecting insider risks are considered essential (31%) or very important (33%). Sixty-four percent of respondents believe AI and machine learning is essential (33%) or very important (31%) to preventing, investigating, escalating, containing and remediating insider incidents. Sixty-one percent say automation is essential (38%) or very important (23%) to managing insider risks.

Reduction in incidents is the top metric for measuring the success of insider risk efforts and programs (50%). This is followed by assessment of insider risks (40%) and length of time to resolve the incident (38%).

Five signs that your organization is at risk:

1. Employees are not trained to fully understand and apply laws, mandates, or regulatory requirements related to their work and that affect the organization's security.

2. Employees are unaware of the steps they should take at all times to ensure the devices they use (both company issued and BYOD) are secured at all times.

3. Employees are sending highly confidential data to an unsecured location in the cloud.

4. Employees circumvent the organization's security policies to simplify tasks.

5. Employees expose the organization to risk if they do not keep devices and services patched and upgraded to the latest versions at all times.

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 May 2023. Our final benchmark sample consisted of 309 separate organizations. A total of 1,075 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 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 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 309 organizations:

- Negligent or mistaken employee or contractor
- Malicious insider including employee or contractor malice
- 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:

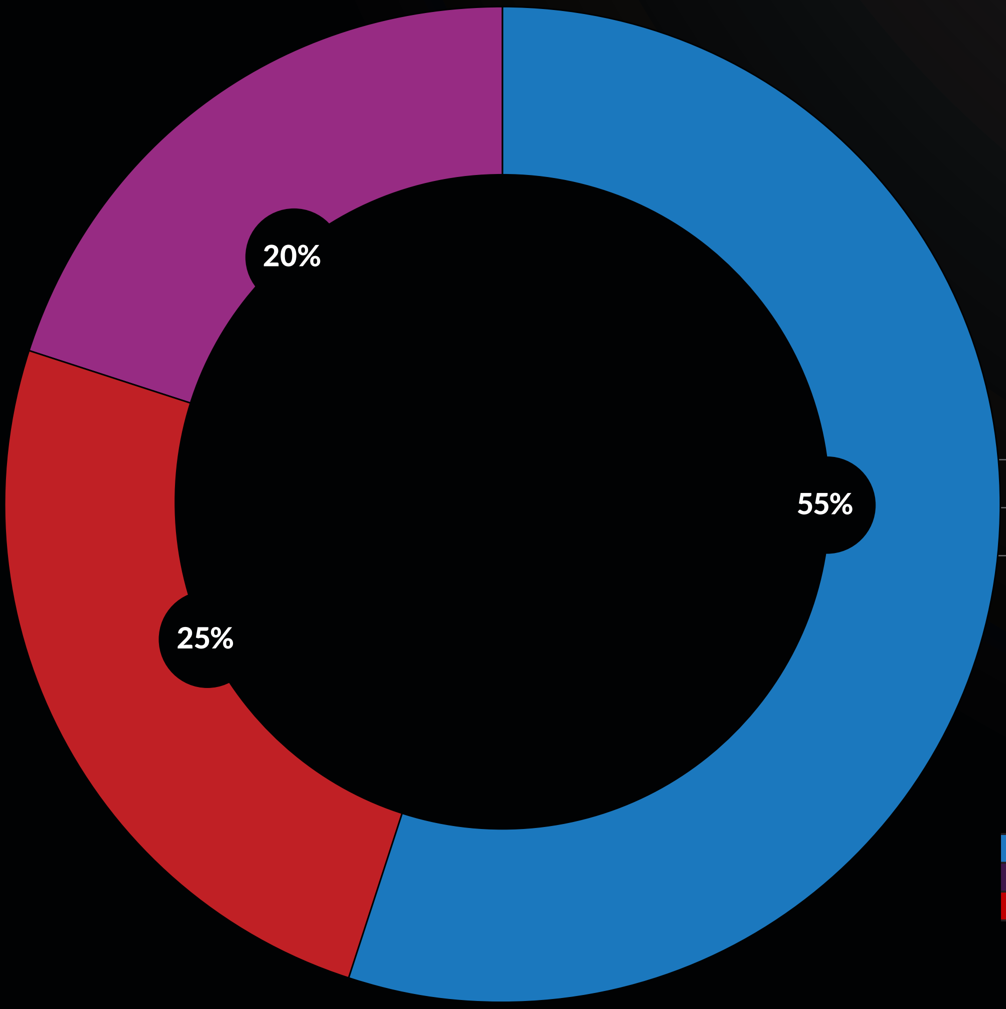
- Working sessions with DTEX Systems to establish areas of inquiry
- Recruitment of benchmark companies
- Development of an activity-based costing framework
- Administration of research program
- Analysis of all results with appropriate reliability checks
- Preparation of a report that summarizes all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

Cost analysis

Employees or contractors continue to be the primary source of an insider risk.

Figure 1. Frequency of 7,343 incidents for three insider profiles

Figure 1 shows the distribution of 7,343 reported attacks analyzed in our sample. A total of 4,019 attacks (or 55%) were caused by employee or contractor negligence/mistakes. Malicious insiders caused another 1,874 attacks (or 25%) and there were 1,450 credential thefts caused by outsmarted insiders (20%).



4,019
Negligent or mistaken insiders

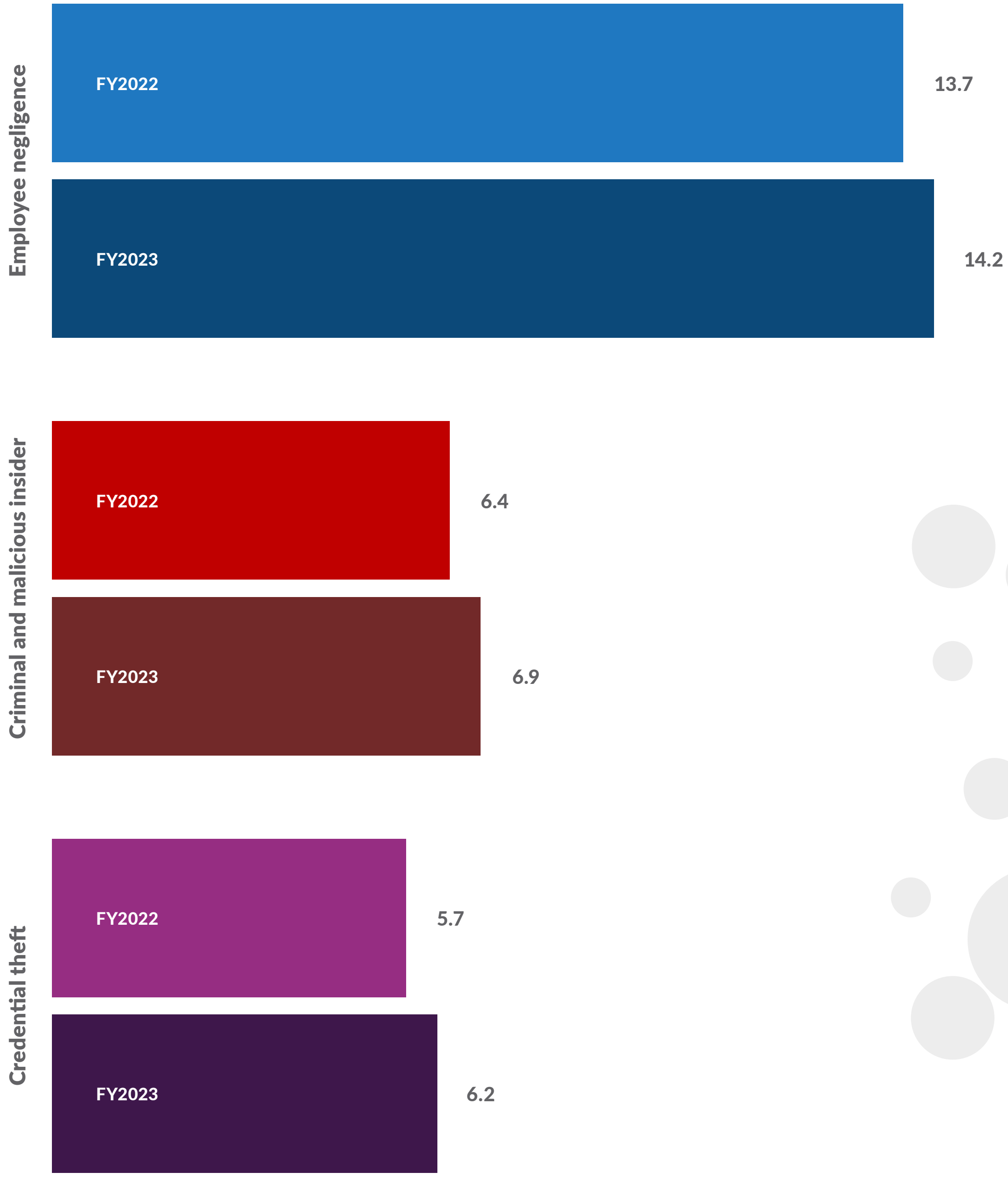
1,874
Malicious or criminal insiders

1,459
Outsmarted insiders (credential theft)

Figure 2. Frequency for three profiles of insider incidents

Employee negligence or employee mistakes are the most frequent insider incidents.

As shown in Figure 2, employee or contractor negligence/mistakes increased slightly from 13.7 to 14.2. Credential theft has increased from an average of 5.7 incidents in 2022 to 6.2 incidents in this year's study. Criminal and malicious insider incidents increased from 6.4 to 6.9.



The 2022 data includes North America, Europe, Middle East and Africa and Asia-Pacific. We believe the data is comparable because US companies represented in the 2016 report are multinationals.

Figure 3. Frequency of insider-related incidents per company over a four-year period

Organizations having more than 40 incidents increased only slightly.

Figure 3 shows the average consolidated frequency of employee or contractor negligence/mistakes, malicious/criminal insider and credential theft incidents per company. According to the 2023 research, 71% of companies (30% + 22% + 19%) are experiencing between 21 and more than 40 incidents per year. This is an increase from 67% in 2022 of companies having between 21 and more than 40 incidents.

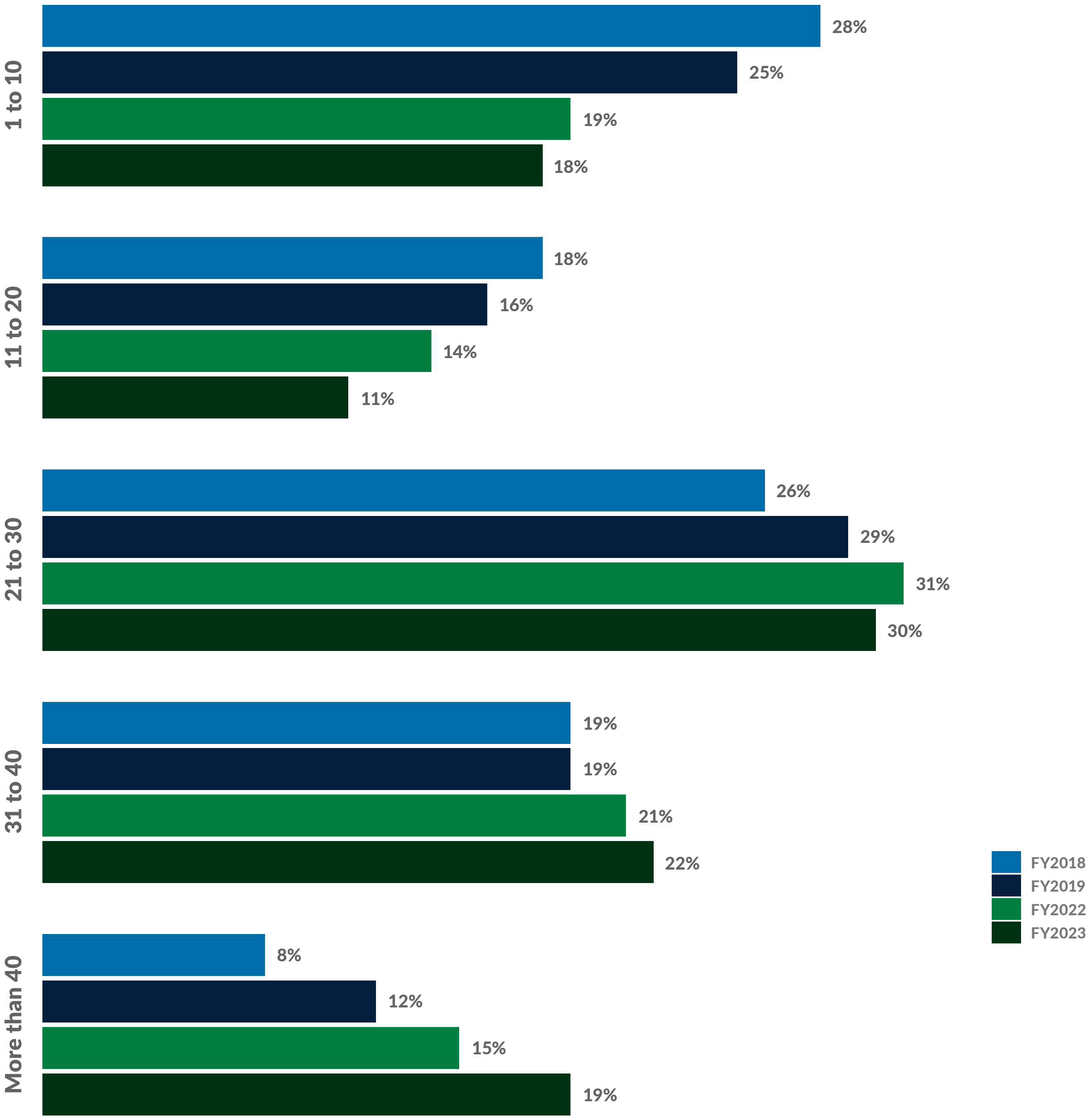
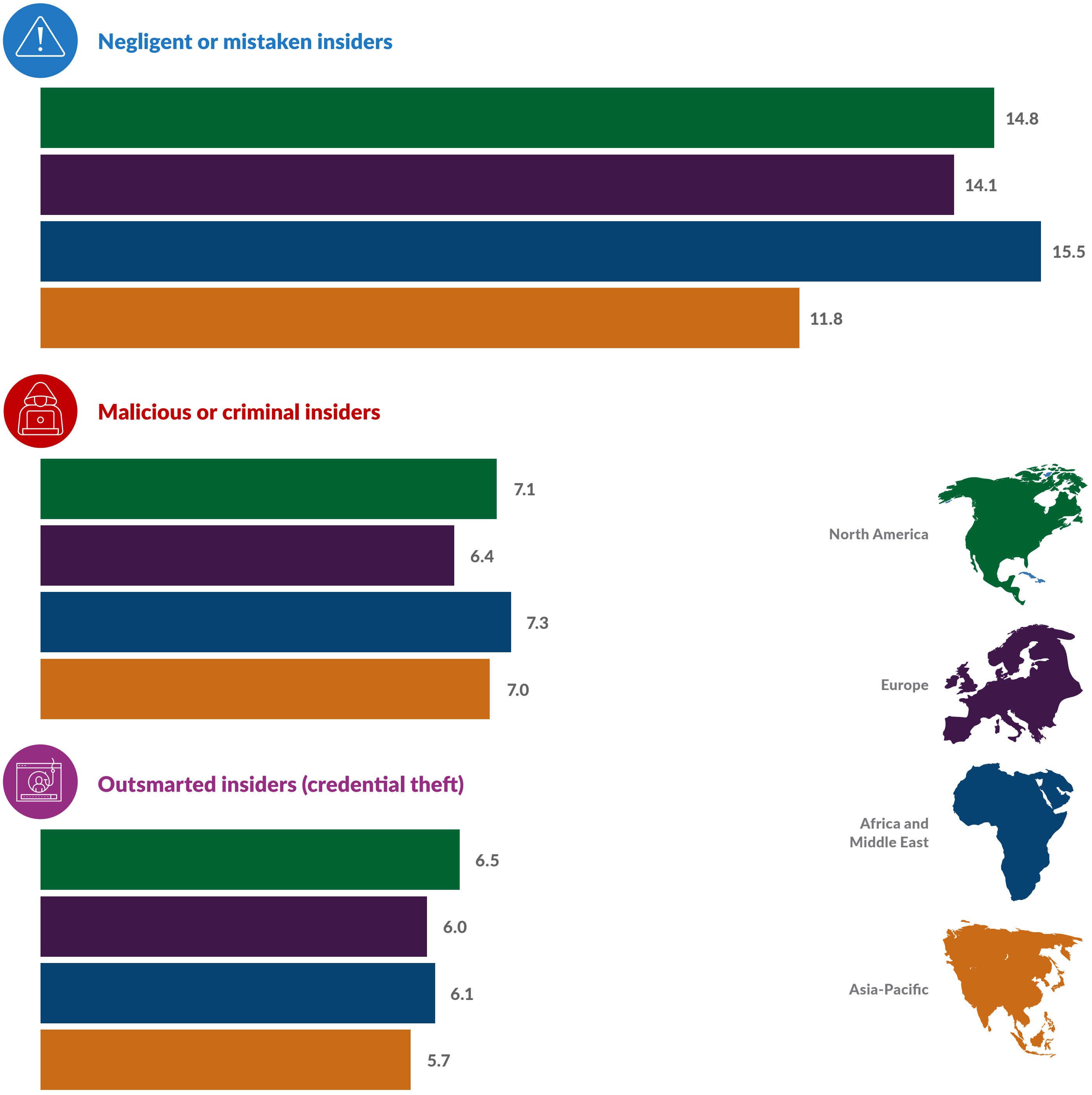


Figure 4. Average incident frequency for three profiles by geographic region

Organizations in the Middle East experienced the most insider incidents, and Asia-Pacific had the least number of incidents.

Figure 4 presents the frequency of insider incidents in the four regions represented in the research. In all regions, employee or contractor negligence incidents occurred the most frequently. North America and the Middle East are most likely to experience credential theft, which is a costly source of insider risk.



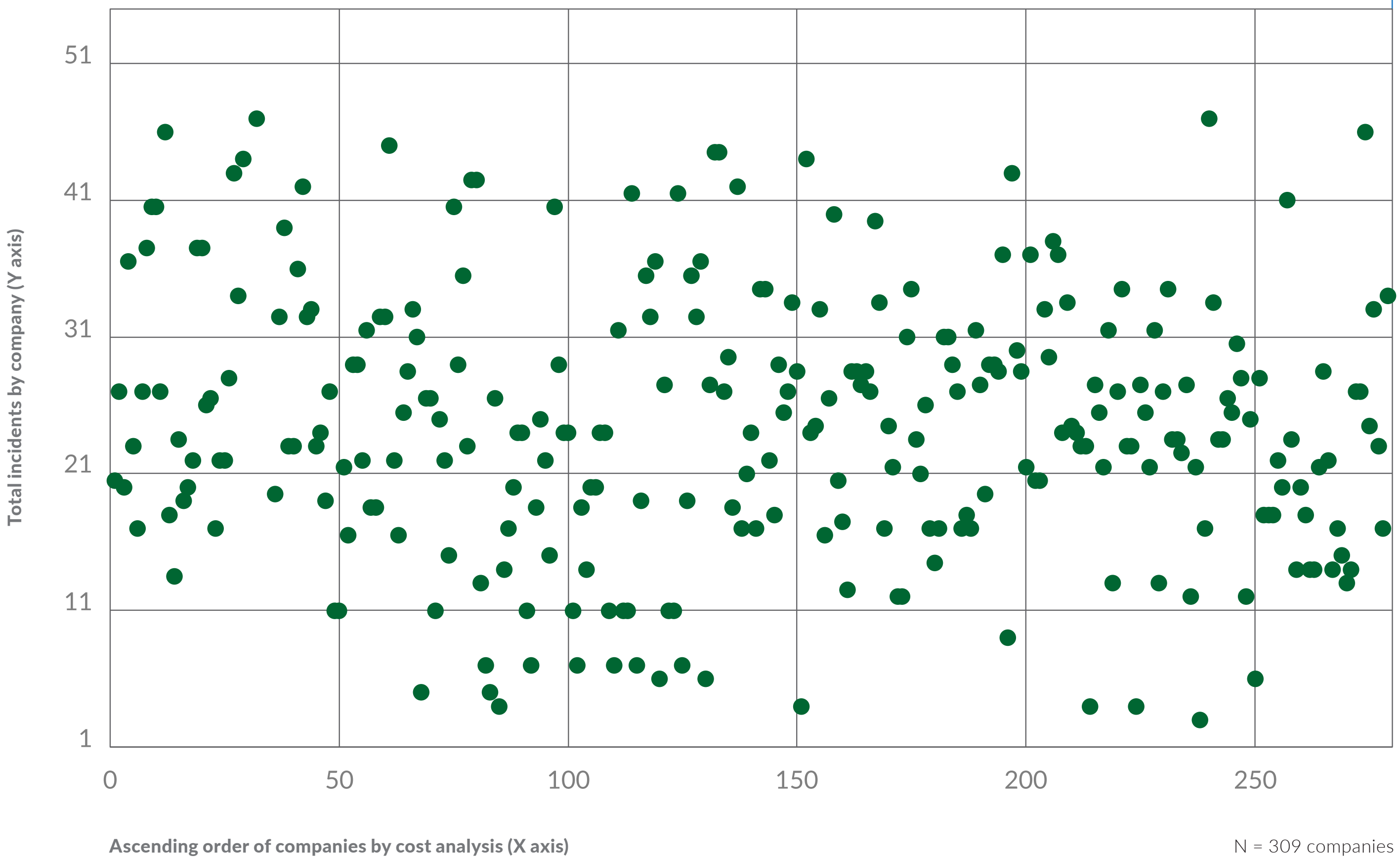


Figure 5. Scattergram of insider-related incidents by company

Figure 5 shows a scattergram of insider incidents per company.

Of the 309 participating companies, 161 (52%) of companies had an average total cost at or below the mean of $16.2 million over the past 12 months. The remaining 148 companies (48%) are above the average of $16.2 million. This finding suggests that the distribution is slightly skewed.

Figure 6. Percentage distribution of insider-related incidents based on the time to contain

Companies are spending an average of 86 days to contain one insider security incident.

According to Figure 6, the time to contain insider-related incidents in our benchmark sample took an average of 86 days to contain the incident. Only 13% of incidents were contained in less than 31 days.

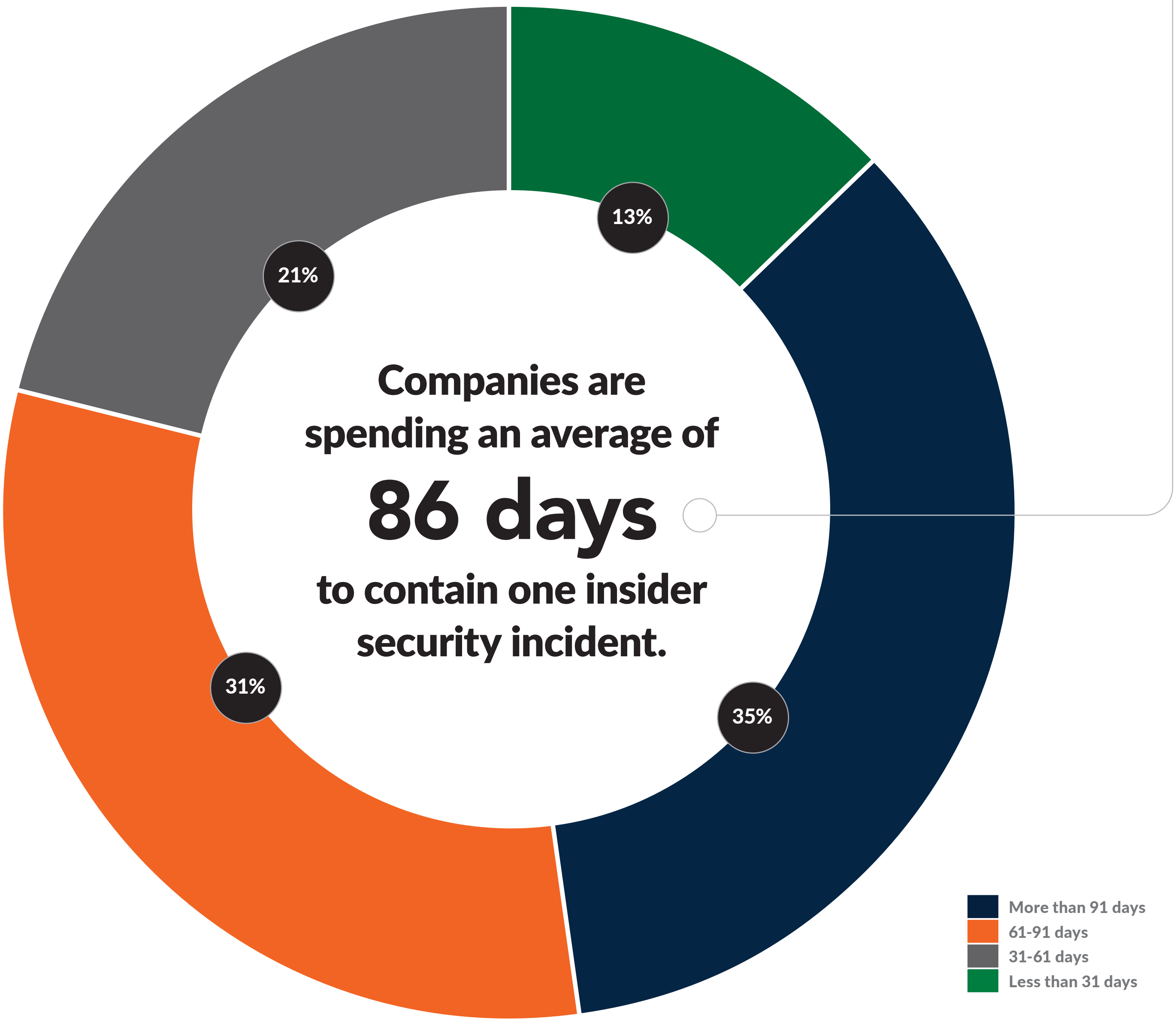
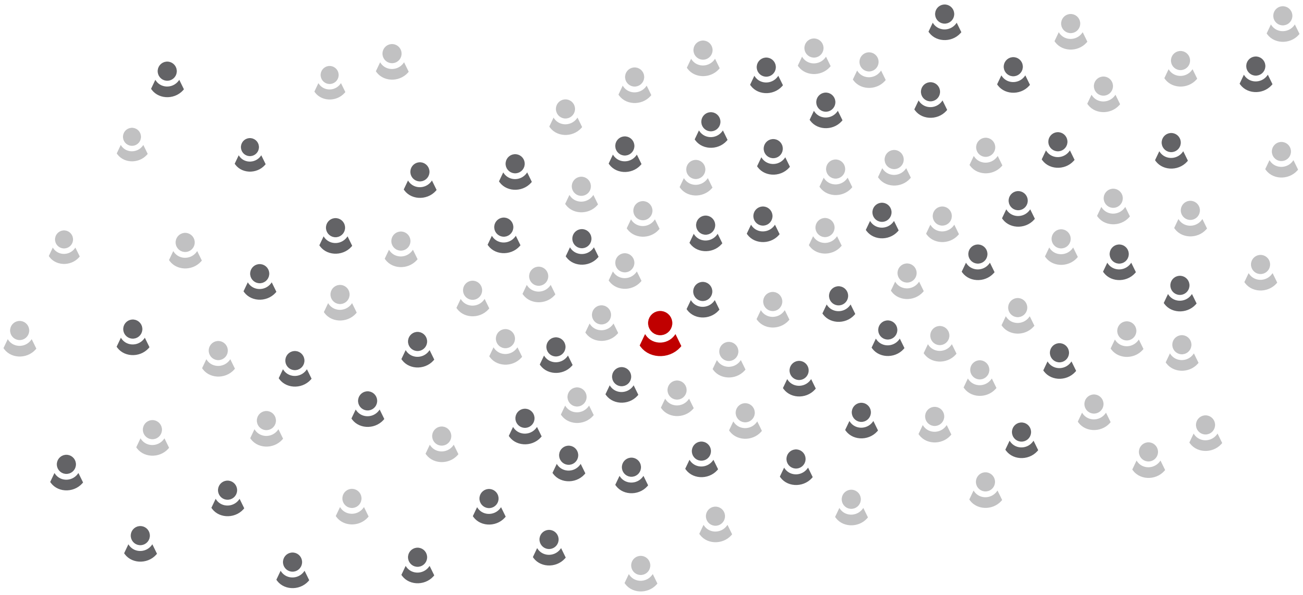


Table 1. Percentage frequency in the use of tools and activities

Most participating companies (72%) are conducting training and awareness programs to reduce insider risks.

Fifty-seven percent of organizations deploy data loss prevention solutions and 56% use SIEM and PAM solutions.

FY2023 Tools and activities that reduce insider risks	Percentage of companies
User training and awareness	72%
Data loss prevention (DLP)	57%
Security incident and event management (SIEM)	56%
Privileged access management (PAM)	56%
User behavior analytics (UBA)	54%
Insider risk management (IRM)	43%
Strict third-party vetting procedures	39%
Employee monitoring and surveillance	38%
Risk intelligence sharing	36%
Network traffic intelligence	27%



The cost of insider risks

Figure 7. Percentage of insider cost by consequence to business organization

Disruption or downtime and direct and indirect labor costs represent the most significant costs when dealing with insider incidents.

Figure 7 reports the percentage of insider cost for careless or negligent employees, malicious insiders and outsmarted employees (credential theft) according to the seven cost categories: Disruption cost (downtime), direct and indirect labor, technology, cash outlays, process/workflow changes, revenue losses and overhead.

The three largest cost categories are the impact of business disruption due to diminished employee/user productivity (26% of total cost), direct and indirect labor (20% of total cost) and technology (19% of total cost), which includes the amortized value and the licensing for software and hardware that are deployed in response to insider-related incidents.

Process costs (11%) include governance and control system activities in response to risks and attacks. Overhead (4%) includes a wide array of miscellaneous costs incurred to support personnel as well as the IT security infrastructure.

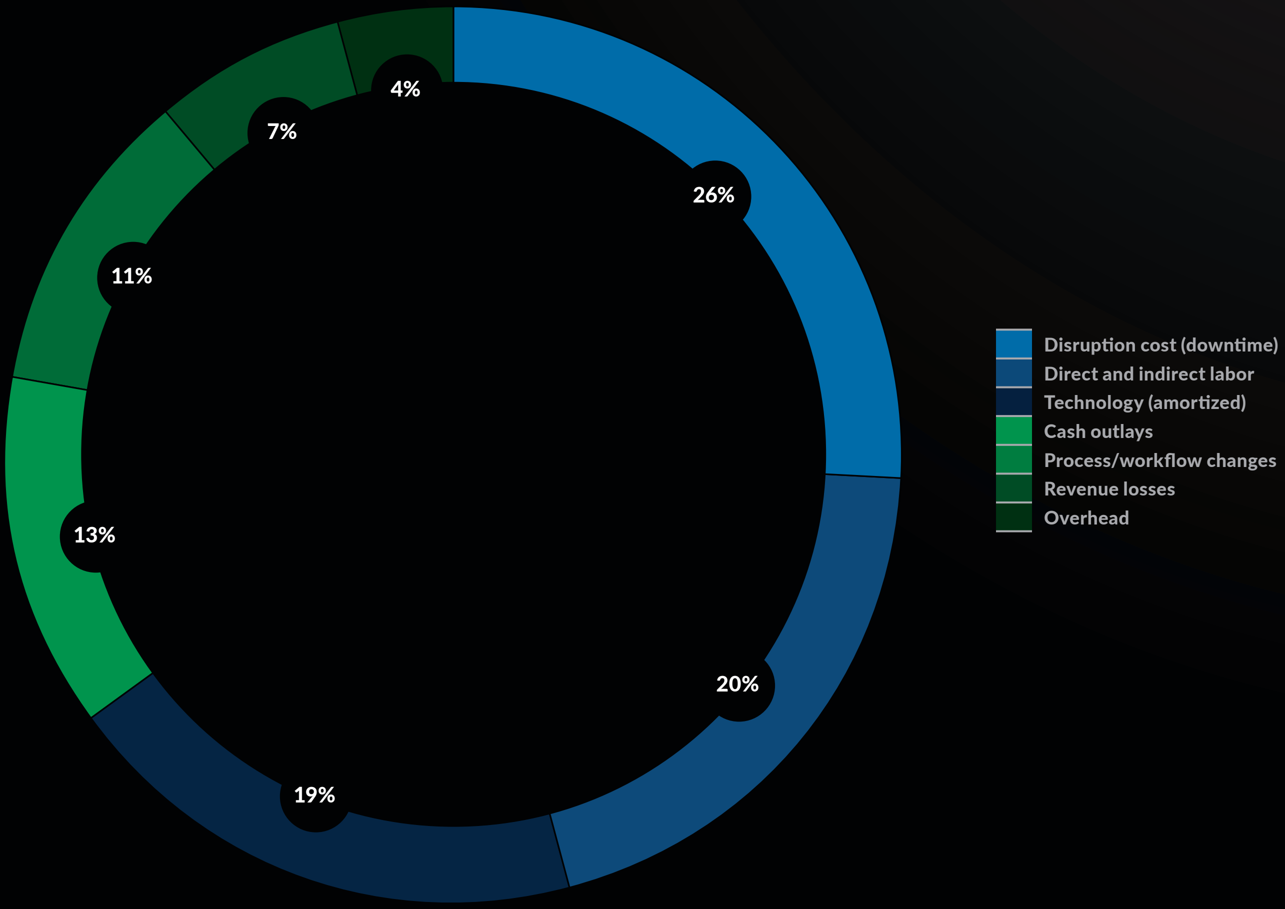


Figure 8. Insider incidents in ascending order by headcount (size)

The larger the organization, the more insider incidents.

Figure 8 shows the distribution of insider incidents in ascending order by headcount or size of the participating companies. As can be seen, the upward slope suggests that the frequency of insider incidents is positively correlated with organizational size. The correlation is most salient for larger-sized companies.

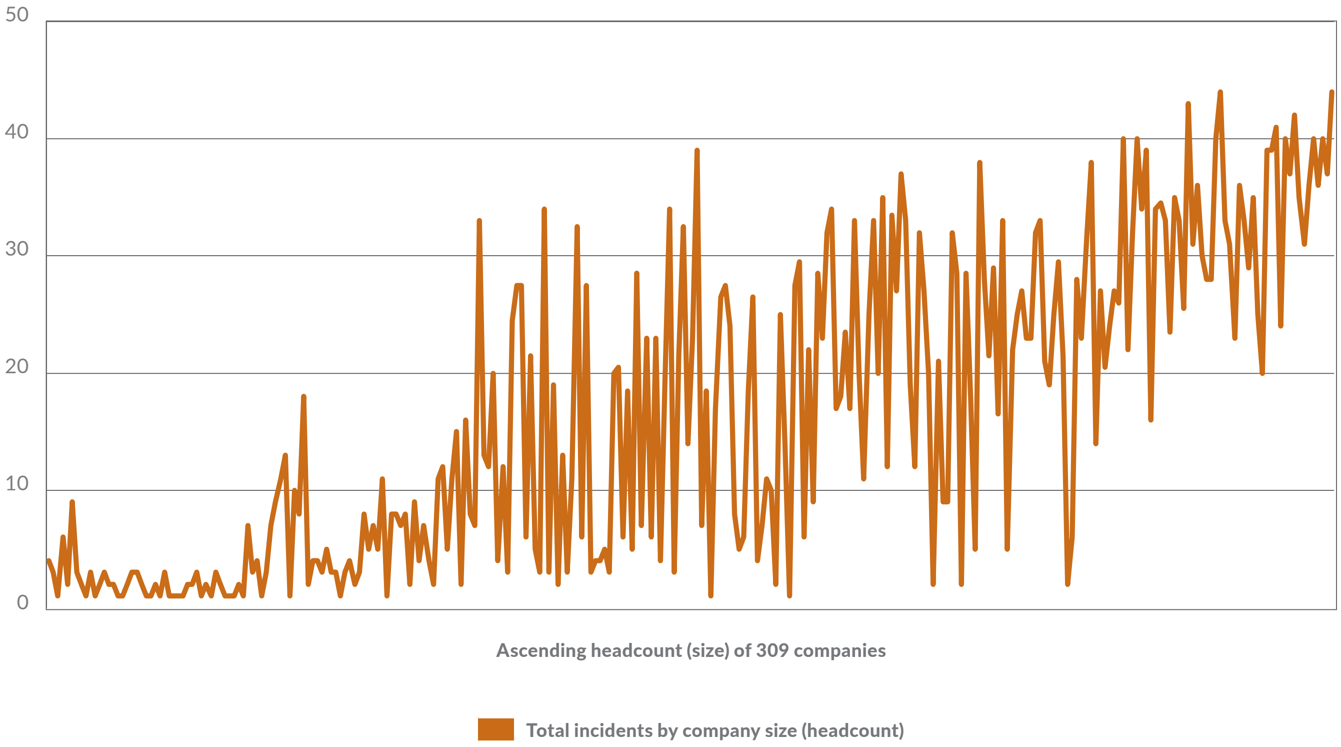


Table 2. The average annual cost per incident for the three types of incidents

Malicious and criminal insider and credential thief incidents continue to be more costly per incident than employee or contractor negligence.

Table 2 presents the average cost per incident, the average number of incidents and the average annualized cost per year. As shown, employee or contractor negligence is most frequent (14 incidents). However, the average cost for this type of incident is less than credential theft and malicious insider incidents.

The cost of malicious insider incidents steadily increased between 2018 and 2019 from $614,192 to $755,761 but declined to $701,500 in 2023. The average number of credential thefts has increased since 2018 and the average cost for remediating these incidents is $679,621 in this year's research.

FY2018 CASE PROFILES	Average cost per incident	Mean number of incidents per year	Average annualized cost
Non-malicious insider (negligent/mistaken)	$277,557	13.2	$3,663,752
Malicious and criminal insider	$614,192	4.6	$2,825,283
Outsmarted insider (credential theft)	$672,112	2.7	$1,814,702
			$8,303,737

FY2019 CASE PROFILES	Average cost per incident	Mean number of incidents per year	Average annualized cost
Non-malicious insider (negligent/mistaken)	$317,111	14.9	$4,724,954
Malicious and criminal insider	$755,761	5.4	$4,081,109
Outsmarted insider (credential theft)	$871,686	3.2	$2,789,395
			$11,595,458

FY2022 CASE PROFILES	Average cost per incident	Mean number of incidents per year	Average annualized cost
Non-malicious insider (negligent/mistaken)	$484,931	13.7	$6,643,555
Malicious and criminal insider	$648,062	6.4	$4,147,597
Outsmarted insider (credential theft)	$804,997	5.7	$4,588,483
			$15,378,635

FY2023 CASE PROFILES	Average cost per incident	Mean number of incidents per year	Average annualized cost
Non-malicious insider (negligent/mistaken)	$505,113	14.2	$7,172,605
Malicious and criminal insider	$701,500	6.9	$4,840,350
Outsmarted insider (credential theft)	$679,621	6.2	$4,213,650
			$16,226,605

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:

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.
2. **Investigation:** Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents.
3. **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.
4. **Incident response:** Activities relating to the formation and engagement of the incident response team including the steps taken to formulate a final management response.
5. **Containment:** Activities that focus on stopping or lessening the severity of insider incidents or attacks. These include shutting down vulnerable applications and endpoints.
6. **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.
7. **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.

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.

Table 3. Average trend in activity cost for seven activity centers

Companies spend the most on containment of the insider security incident.

As discussed, the average time to contain an incident is 86 days in this year's research. Table 3 summarizes the average cost of insider-related incidents for the three types of incidents and seven activity centers. As shown, containment and remediation of the incident represent the most expensive activity centers at $179,209 and $125,221, respectively. Least expensive are ex-post analysis and escalation at $29,787 and 29,794, respectively.

Activity cost centers	FY2016	FY2018	FY2019	FY2022	FY2023
Monitoring and surveillance	$9,620	$12,634	$22,124	$35,080	$33,596
Investigation	$41,461	$78,398	$103,798	$128,056	$117,504
Escalation	$8,919	$12,542	$21,805	$32,228	$29,794
Incident response	$66,371	$91,263	$118,317	$120,391	$113,635
Containment	$122,796	$173,161	$211,553	$184,548	$179,209
Ex-post analysis	$8,498	$11,491	$19,480	$26,563	$29,787
Remediation	$91,397	$138,532	$147,776	$119,131	$125,221
Overall	**$349,060**	**$517,921**	**$644,853**	**$645,997**	**$628,745**

Figure 9. Percentage net increase in average cost from FY2016 to FY2023

Since 2016, it has become far more costly to respond to an insider risk incident.

As shown in Figure 9, ex-post analysis and monitoring and surveillance have increased the most since 2016, 111%. Importantly, these are the only pre-incident activities. This finding suggests attempts have been made to take a proactive approach to managing insider risks.

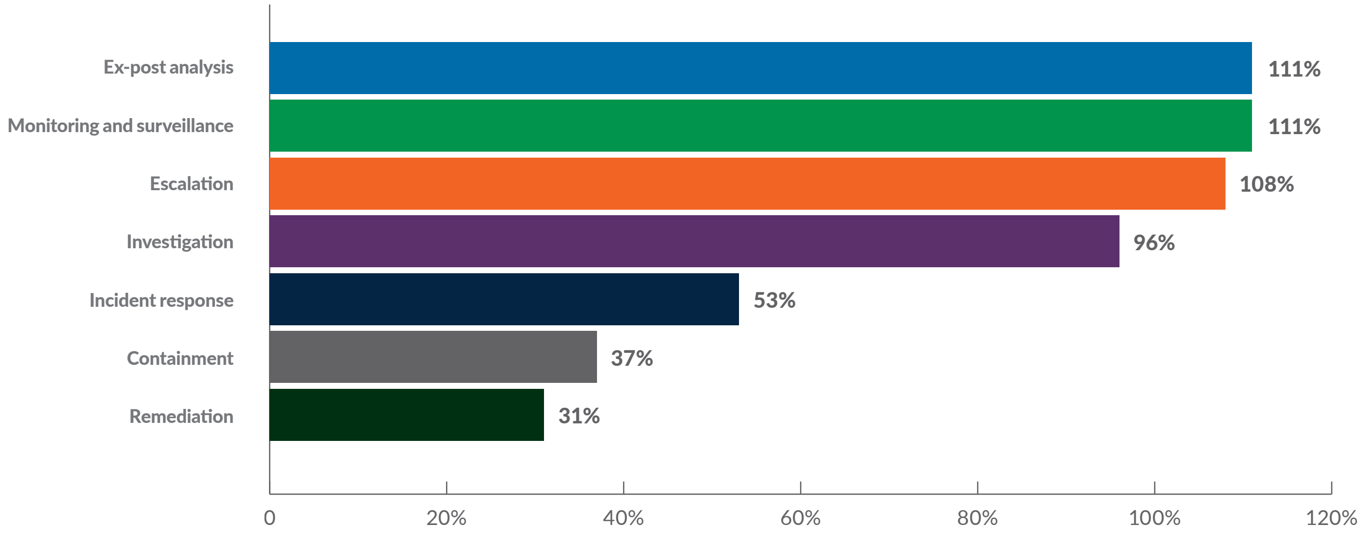


Table 4. 2023 cost of seven activities by the type of incident

Containing the insider incident is most costly for malicious or criminal insider and credential theft incidents.

Table 4 presents the average annualized cost for the seven activities according to the type of incident.

FY2023 activity cost centers	Negligent or mistaken	Malicious or criminal	Outsmarted (credential theft)	Average cost
Monitoring and surveillance	$21,869	$38,420	$40,499	$33,596
Investigation	$103,388	$136,096	$113,026	$117,504
Escalation	$24,337	$41,552	$23,492	$29,794
Incident response	$105,941	$133,330	$101,635	$113,635
Containment	$140,312	$198,545	$198,769	$179,209
Ex-post analysis	$19,834	$28,349	$41,176	$29,787
Remediation	$89,433	$125,208	$161,023	$125,221
Total	**$505,113**	**$701,500**	**$679,621**	**$628,745**

Figure 10. 2023 average activity cost per incident for the three types of incidents

The average activity cost is highest for malicious or criminal insiders.

Figure 10 demonstrates the significant difference in activity cost between employee or contractor negligence and credential theft.

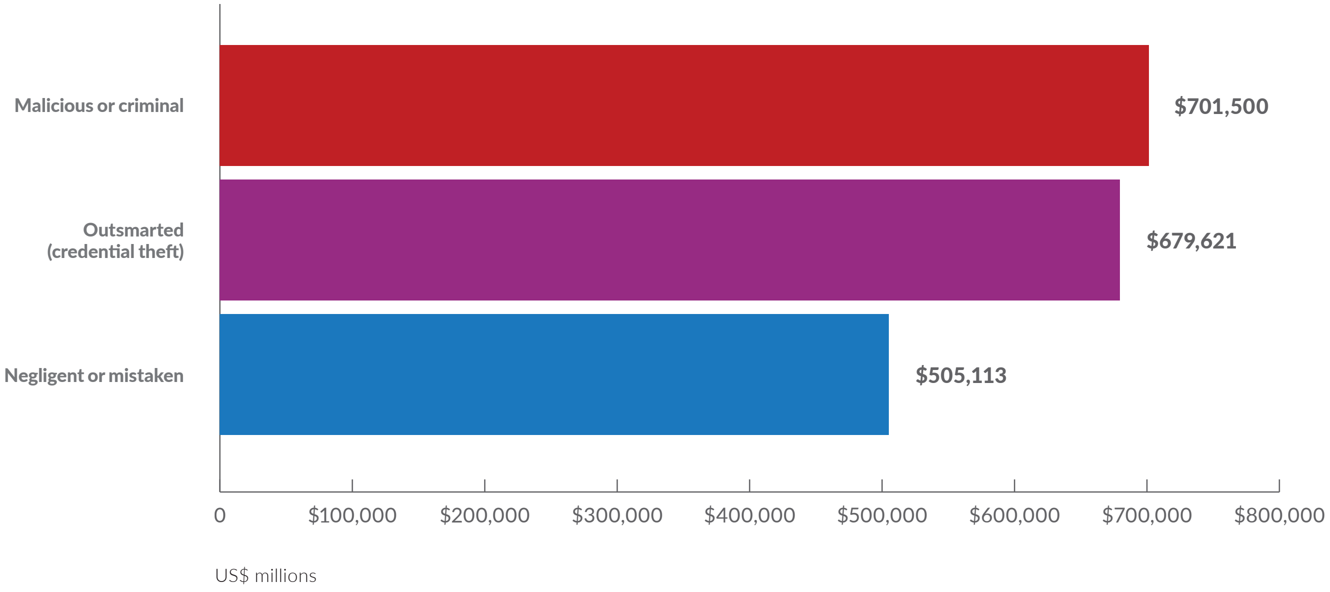


Figure 11. Average activity cost by global region

North American companies are spending significantly more than the average cost on activities that deal with insider risks.

The total average cost of activities to resolve insider risks over a 12-month period is $16.2 million. As shown in Figure 11, companies in North America experienced the highest total cost at $19.09 million. European companies had the next highest cost at $17.47 million. Asia-Pacific had an average cost much lower than average total cost for all 309 companies ($12.17 million).

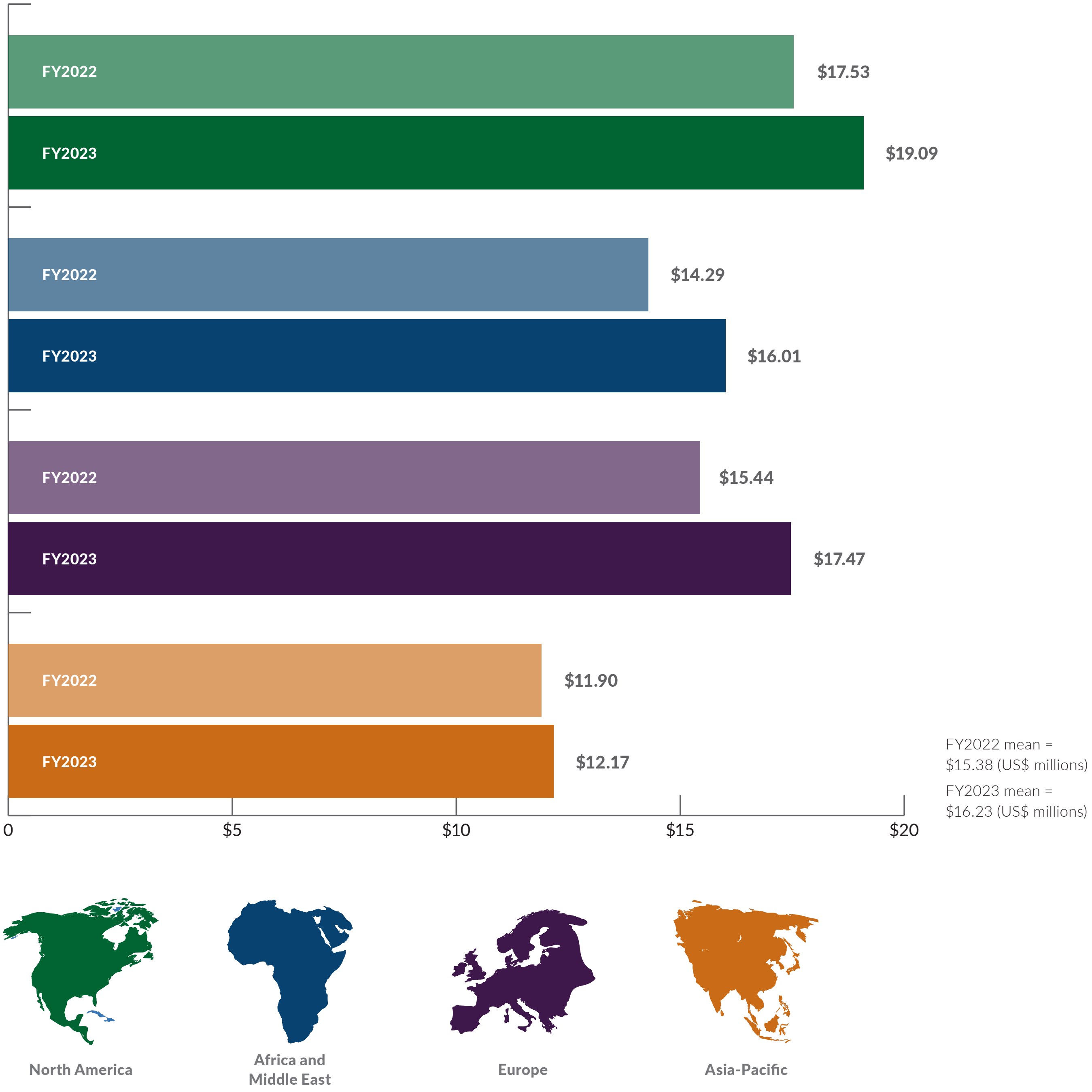


Figure 12. Average activity cost by headcount

Larger organizations spend the most on the activities to resolve an insider risk incident.

As shown in Figure 12, organizations with a headcount of between 25,000 and 75,000 are spending significantly more on activities needed to resolve the incident, an average of $19.70.

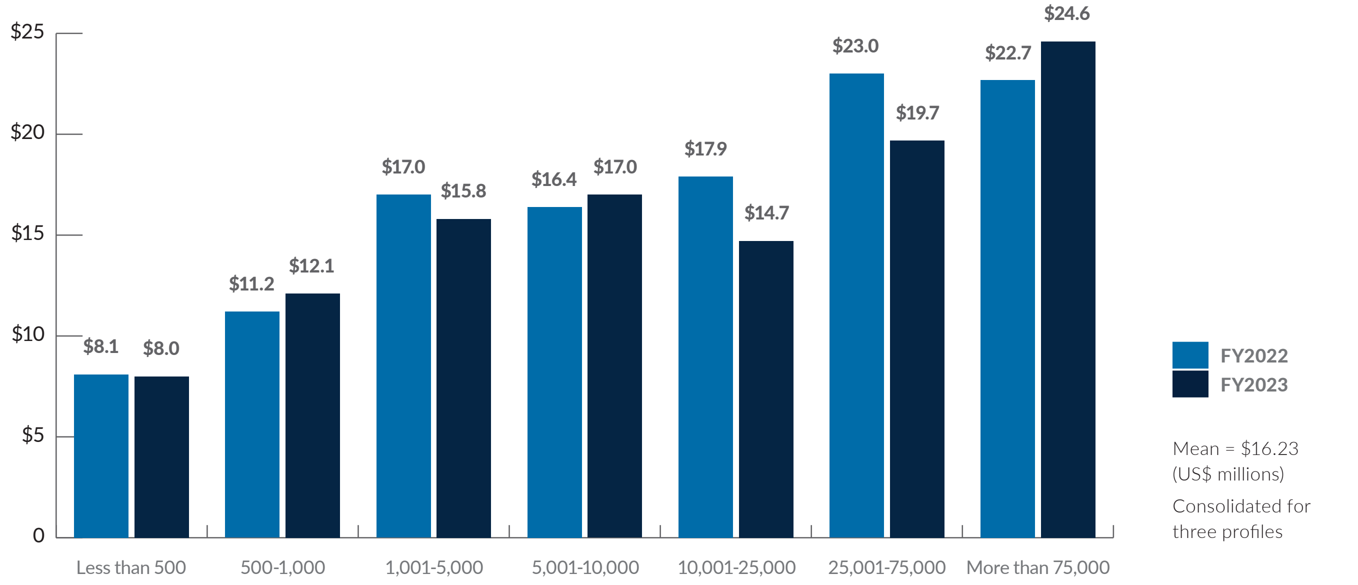


Figure 13. Average activity cost by days to contain the incidents

The faster containment occurs, the lower the activity cost.

The total annualized cost appears to be positively correlated with the time to contain insider-related incidents. As shown in Figure 13, incidents that took more than 91 days to contain had the highest average total cost per year ($18.33 million). In contrast, incidents that took less than 31 days to contain had the lowest total cost. ($11.92 million). The average annual cost is $16.23 million.

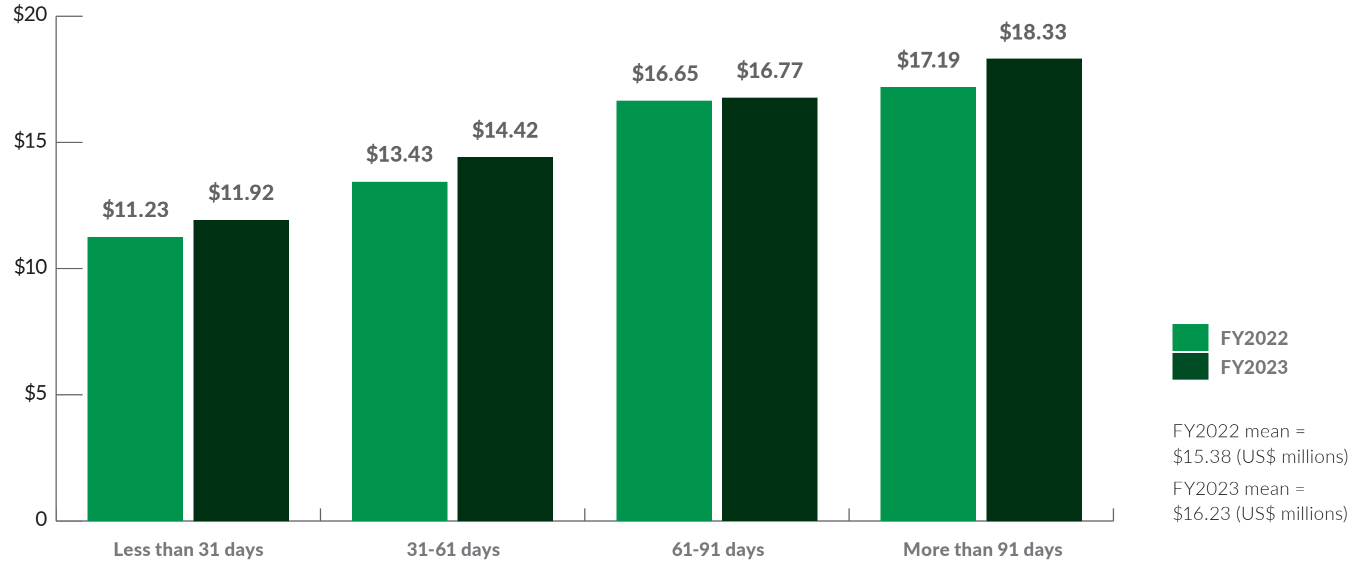
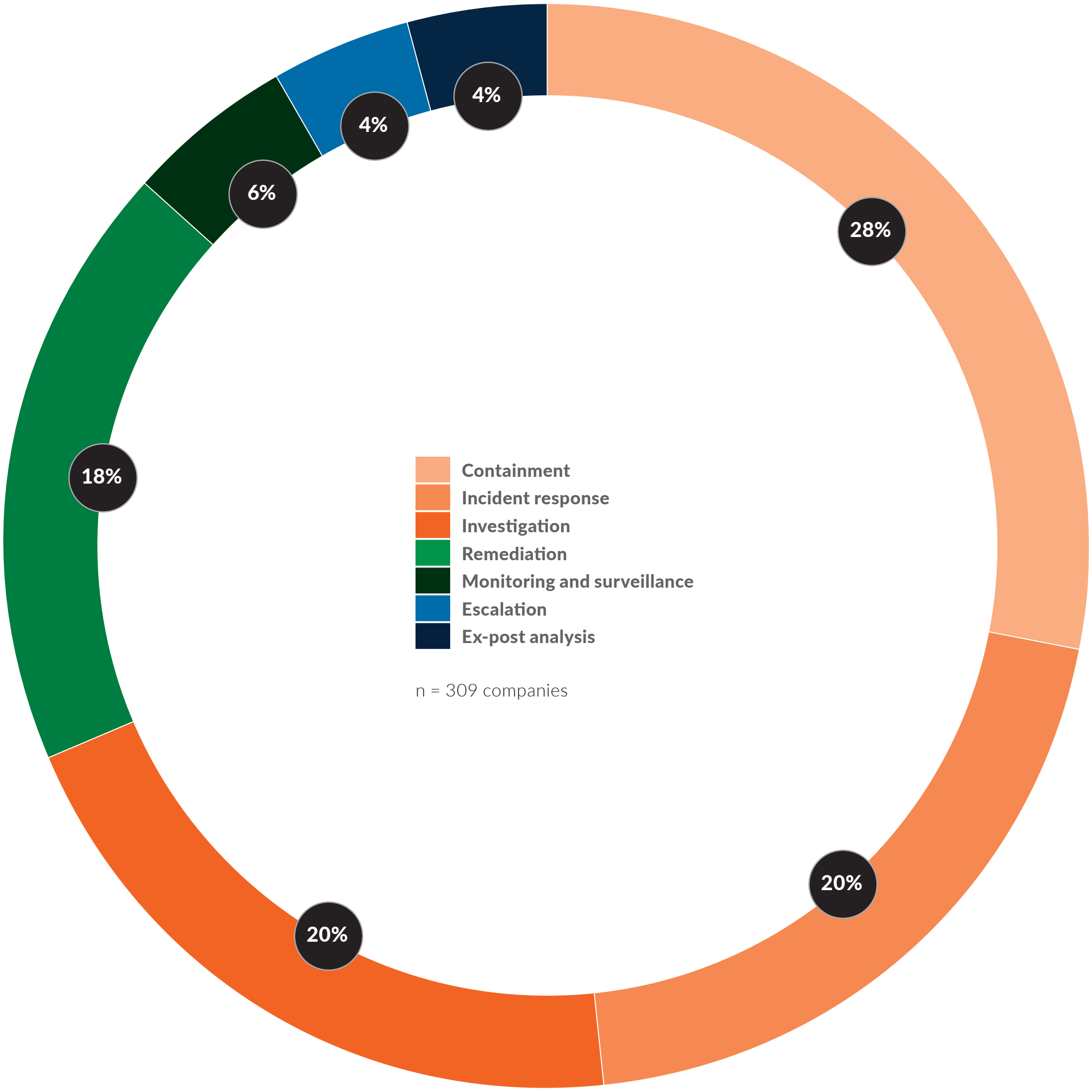


Figure 14. Percentage cost of insider incidents by activity center

Containment accounts for one-third of all costs.

The following pie chart shows the percentage cost for seven activity centers. According to Figure 14, containment represents 28% of total annualized insider-related activity costs. Activities relating to investigation and incident response represent 20% of total cost, respectively.



n = 309 companies

Figure 15. Annualized activity cost by industry

Activity costs are higher for financial services and services.

According to Figure 15, the average activity cost for financial services is $20.68 million and services is $19.63 million, much higher than the average of $16.2 million. Services includes such companies as law, consulting and accounting firms.

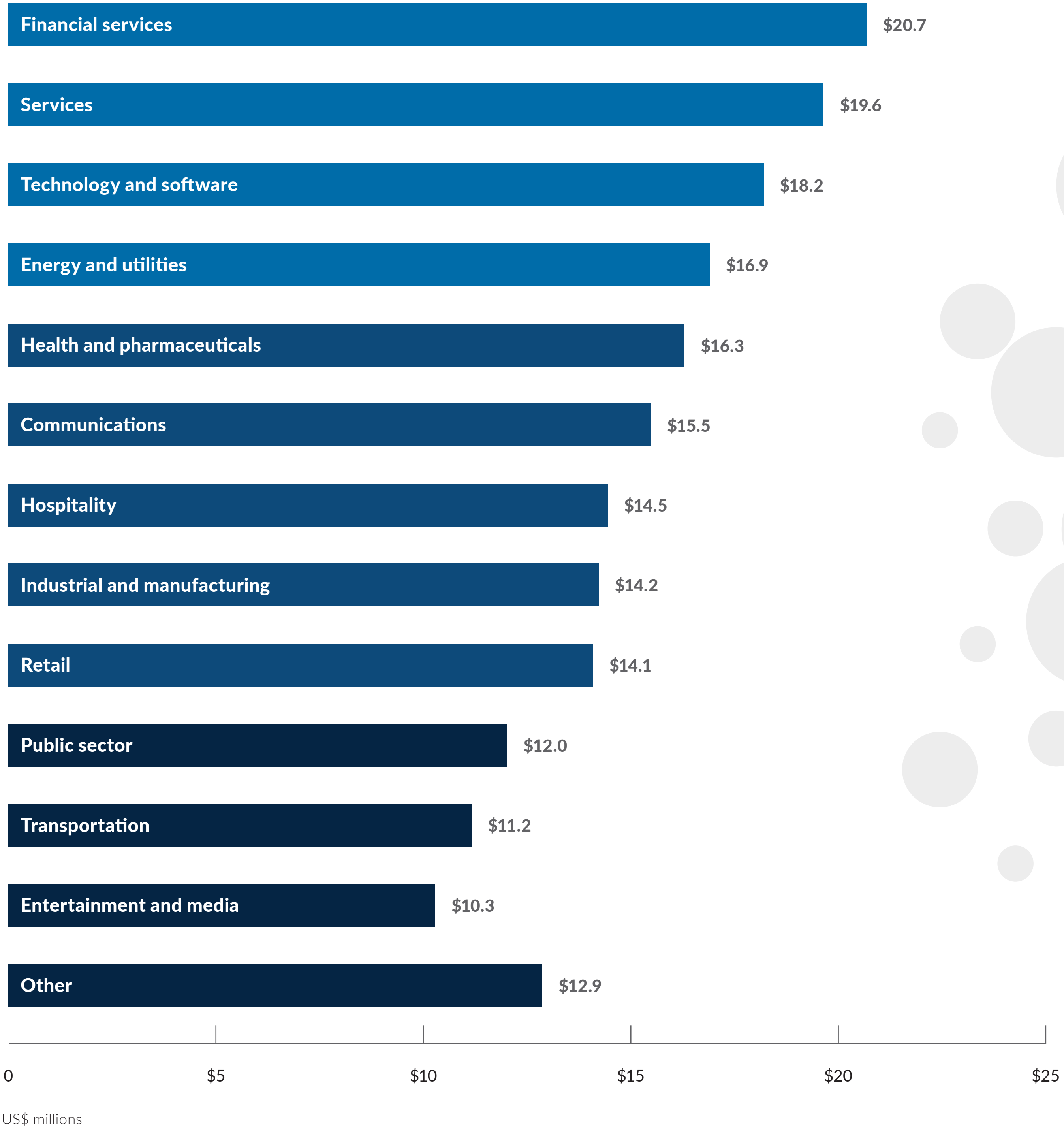
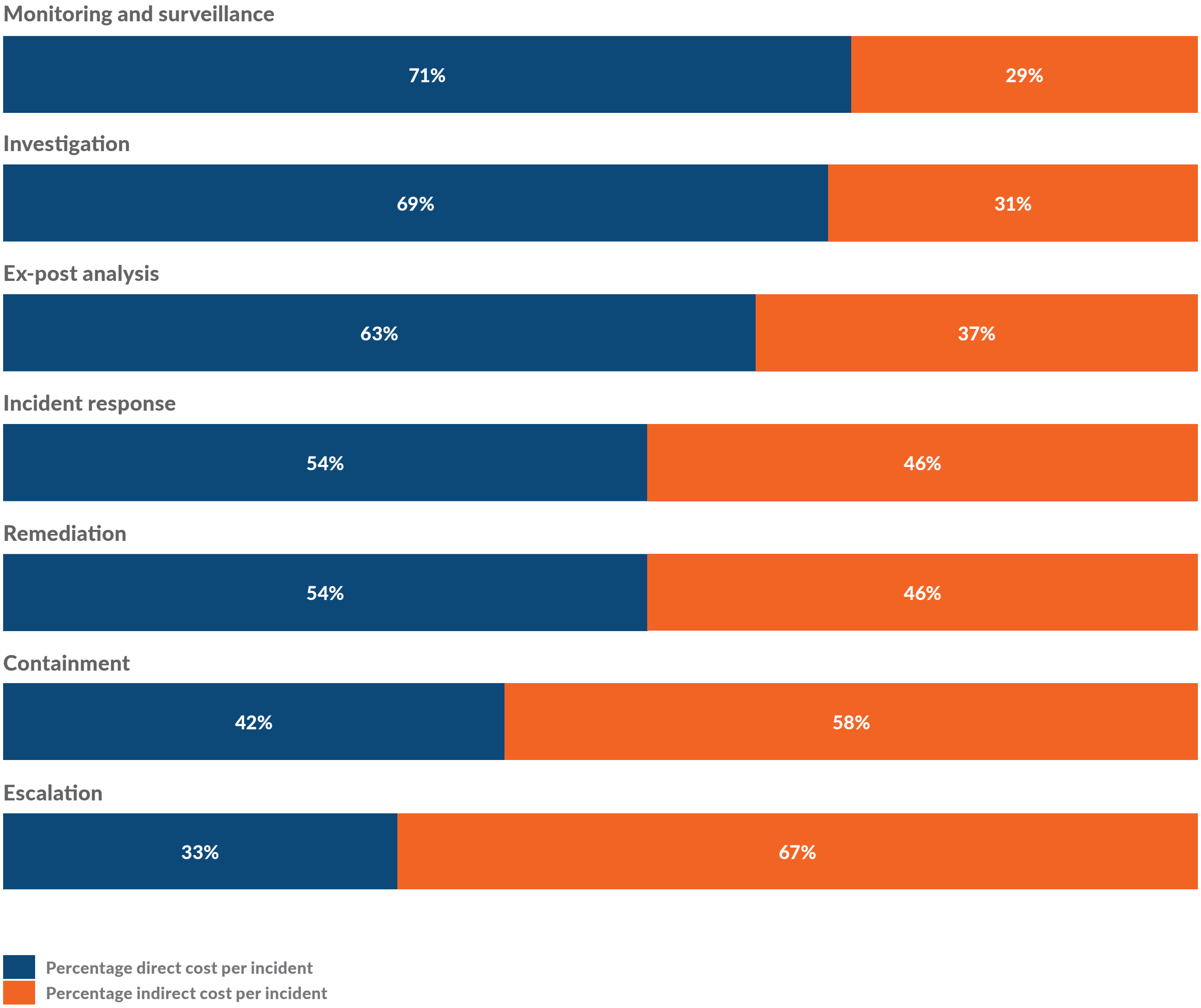


Figure 16. Percentage of direct vs. indirect costs for activity centers

Companies were asked to estimate the direct and indirect costs 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 16 shows the proportion of direct and indirect costs for seven internal activity cost centers. As can be seen, the cost for monitoring and surveillance and investigation has the highest percentage of direct cost (71% and 69%, respectively). The highest percentage of indirect cost for activities are for containment (58%) and escalation (67%).



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.

Managing insider risks

In addition to determining the cost of insider risks, we interviewed study participants about their ability to manage malicious and non-malicious insider risks.

Figure 17. Which insider incidents are you most concerned about?

Of all insider risks, organizations are most concerned about malicious or criminal insiders.

This is despite that 75% of insider incidents were non-malicious in nature (55% of incidents were attributed to negligence, while 20% were attributed to credential theft).

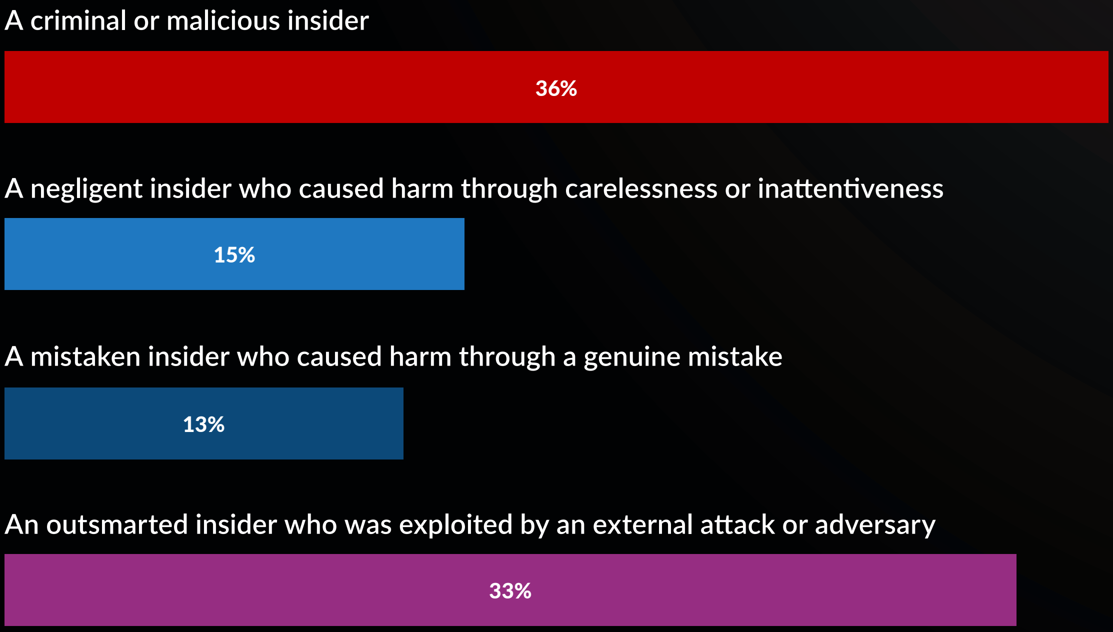
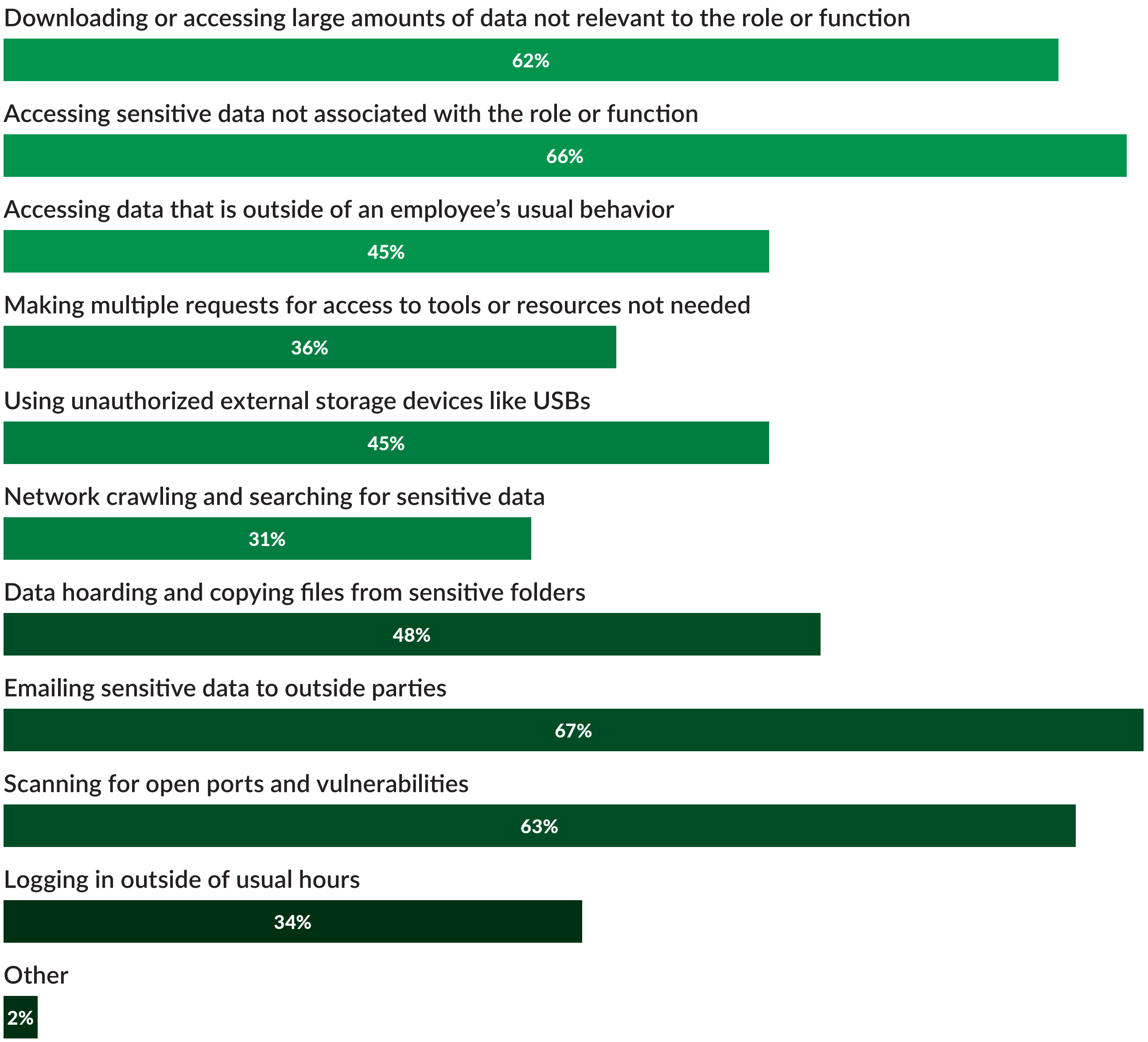


Figure 18. Did malicious insiders do any of the following in your organization?

Malicious insiders were likely to access and share sensitive data unrelated to their job role or function, often in large volumes.

Volume and frequency, data sensitivity and job function have all been validated as early warning indicators for malicious insider risk. This was made evident in two Pentagon incidents in 2023: the Discord leaks and the 'critical compromise' of Air Force communications. While these indicators might seem harmless in isolation, the risk profile is elevated when the indicators are aggregated and correlated, especially with psycho-social data via HR feeds.

More than one response permitted.



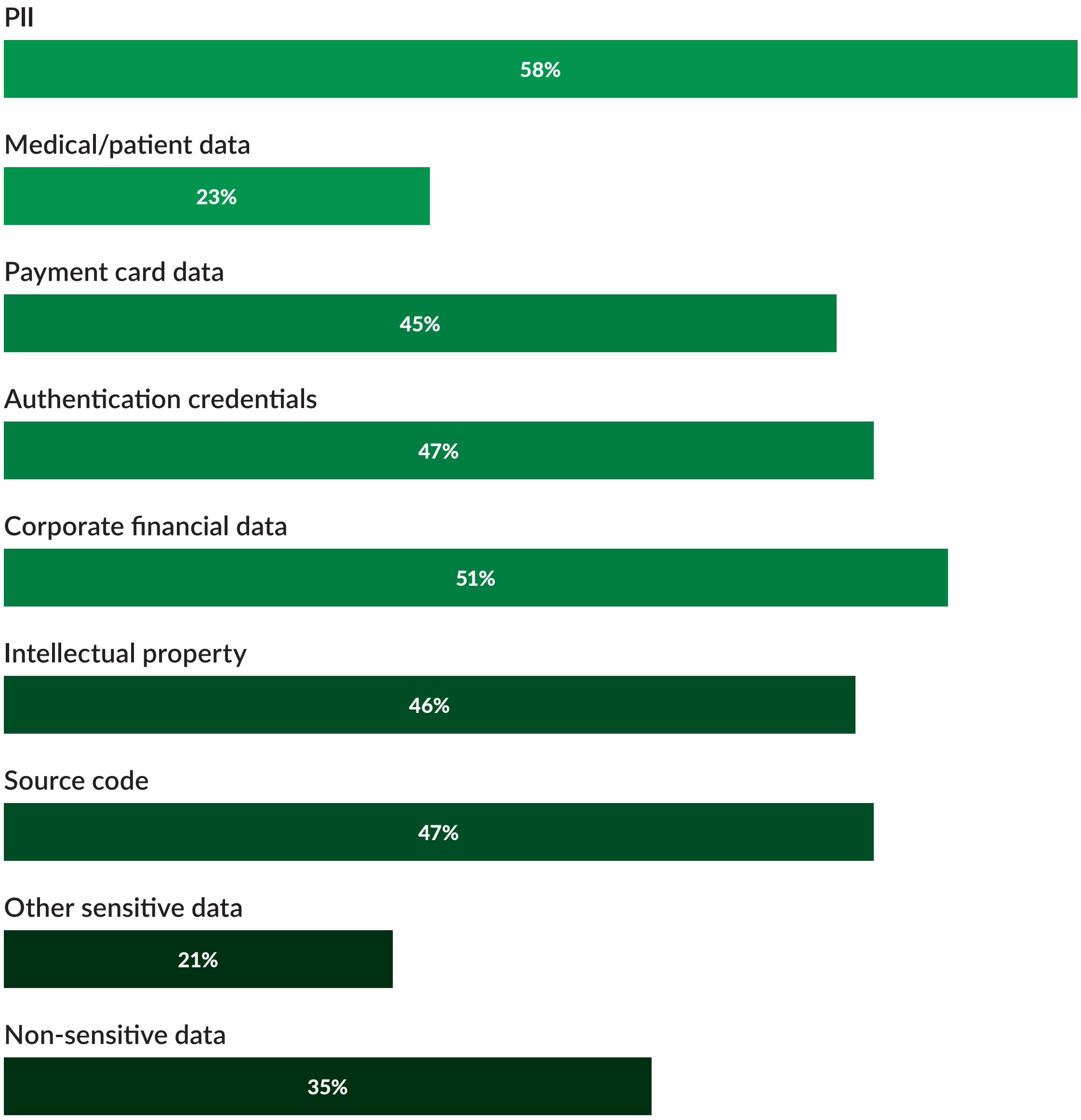
Total (FY2023) = 499%

Figure 19. Which data types were involved in the insider incidents?

Intellectual property (IP) holds the most value for organizations and is involved in nearly half of all insider incidents.

Intellectual property can be sensitive or non-sensitive. Sensitive IP can include customer data, employee data, health records, sales contracts and more, often via clipboard and device sync capabilities, while non-sensitive IP can include corporate presentations and templates.

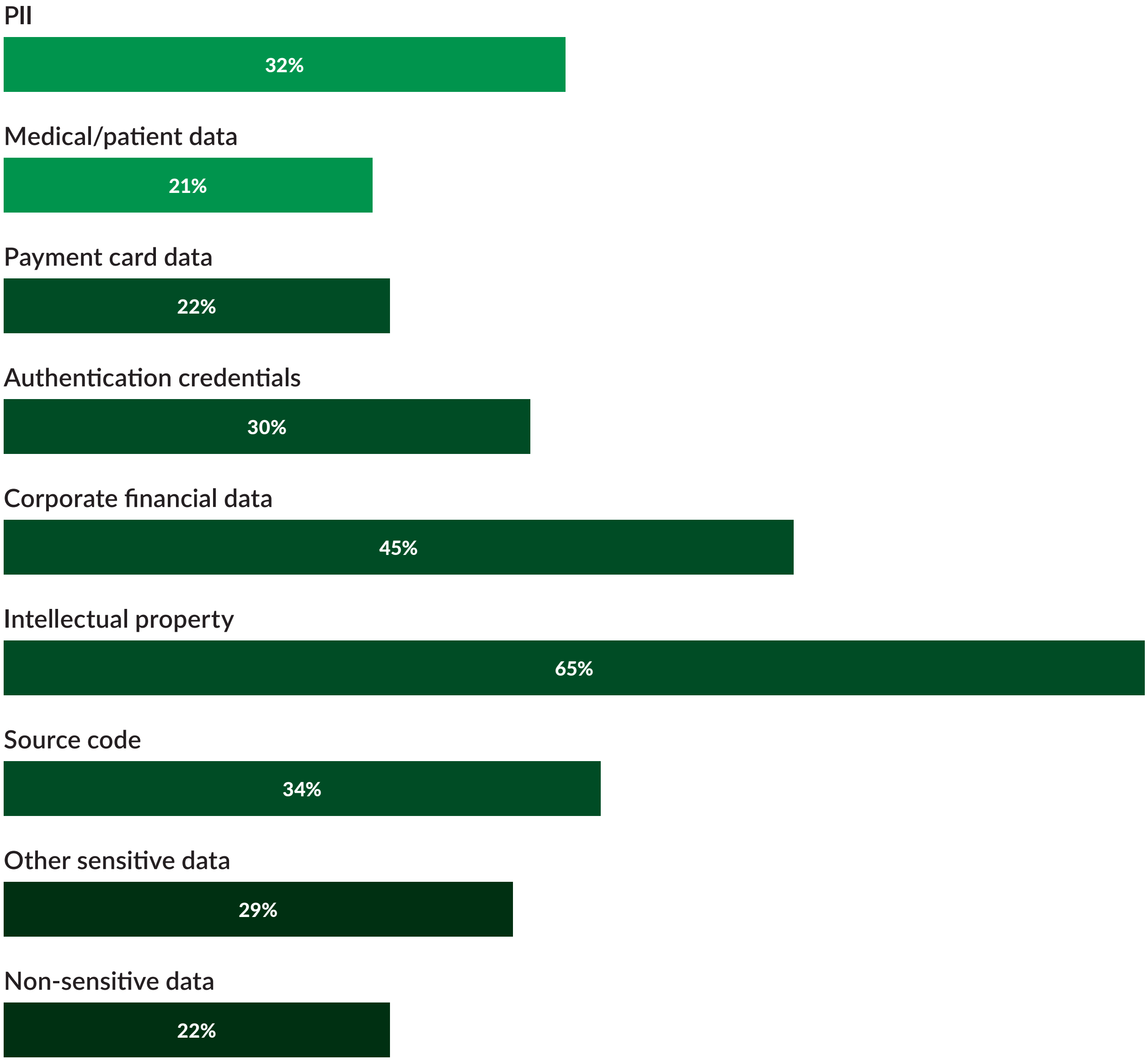
More than one response permitted.



Total (FY2023) = 373%

Figure 20. Which data types are the most valuable to your organization?

Three responses permitted.

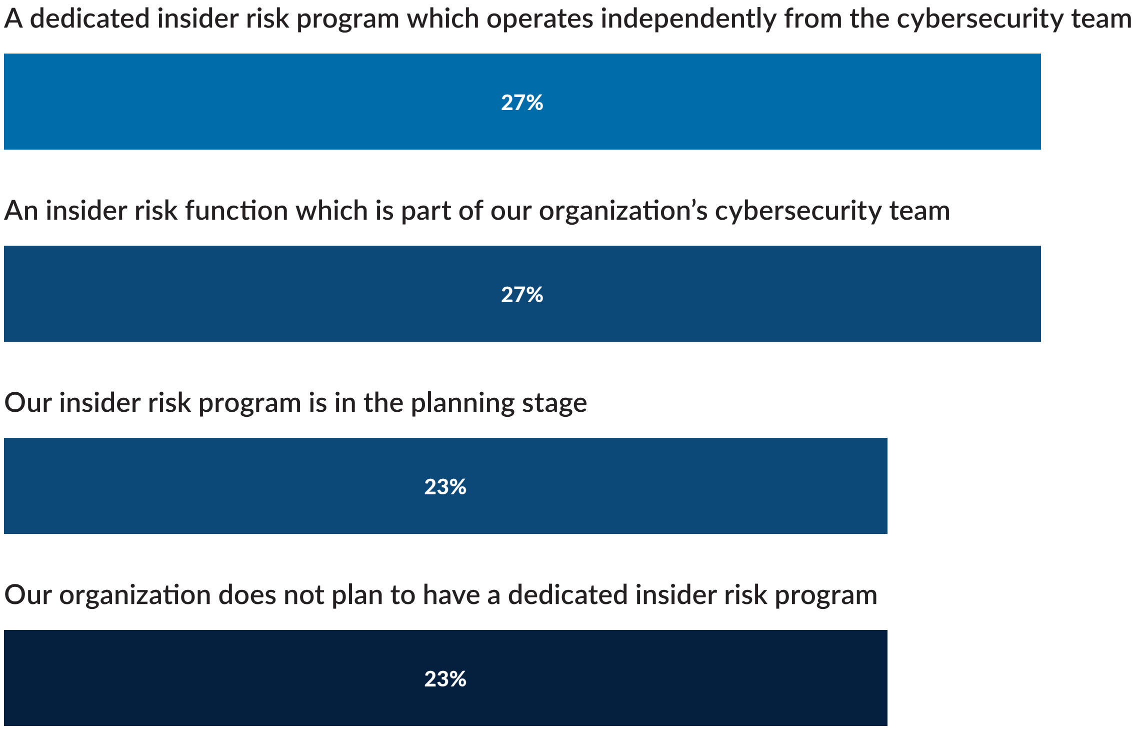


Total (FY2023) = 300%

Figure 21. Does your organization have a dedicated insider risk program?

Having a human-centric insider risk program has become a top priority for most organizations.

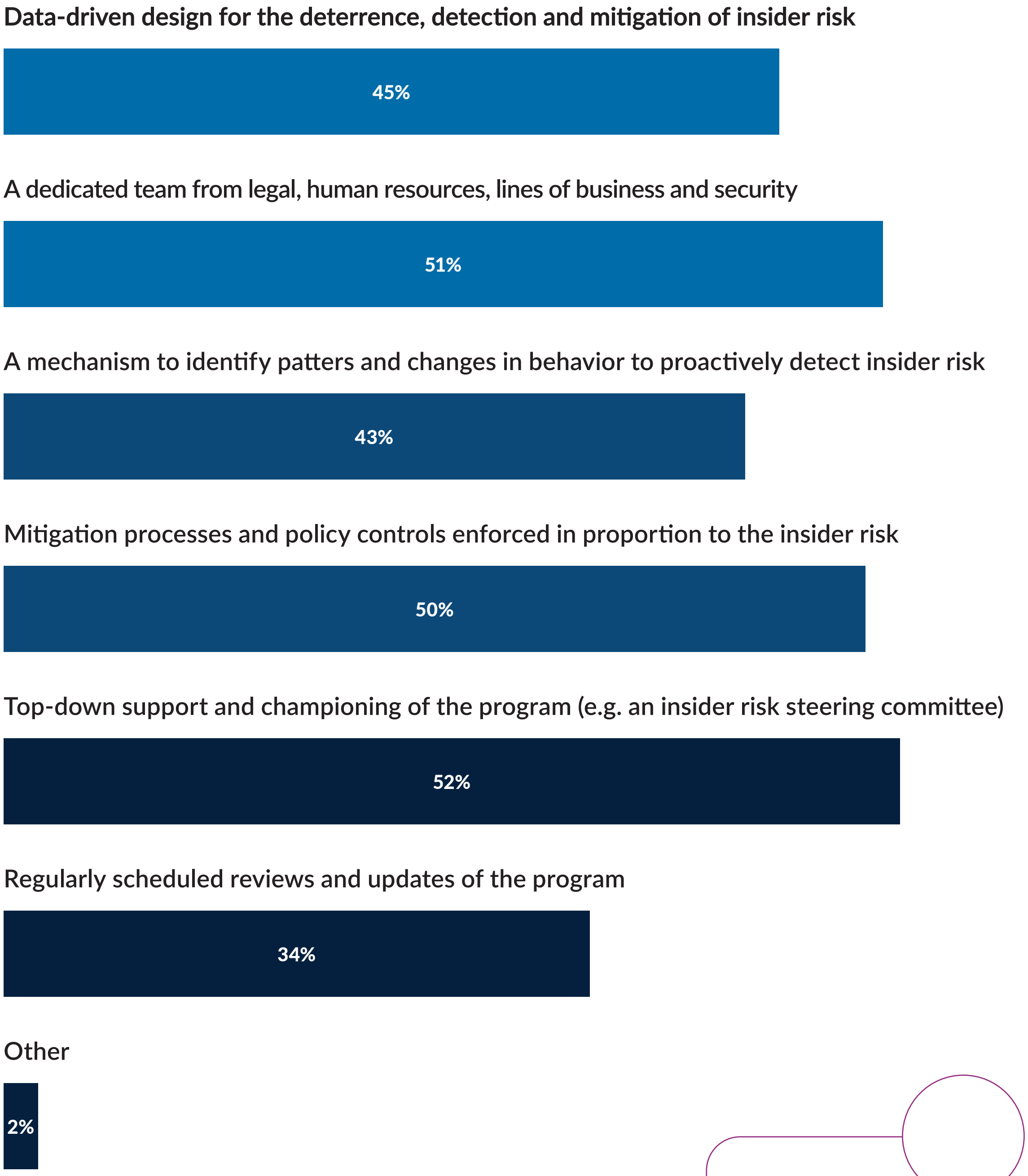
Seventy-seven percent of organizations are planning or have started an insider risk program. More than half (52%) believe top-down support is a key feature of an insider risk program, while 51% believe the program should include a cross-functional dedicated team.



Total (FY2023) = 100%

Figure 22. If your organization has or will have a dedicated insider risk program, what features are/will be included?

More than one response permitted.

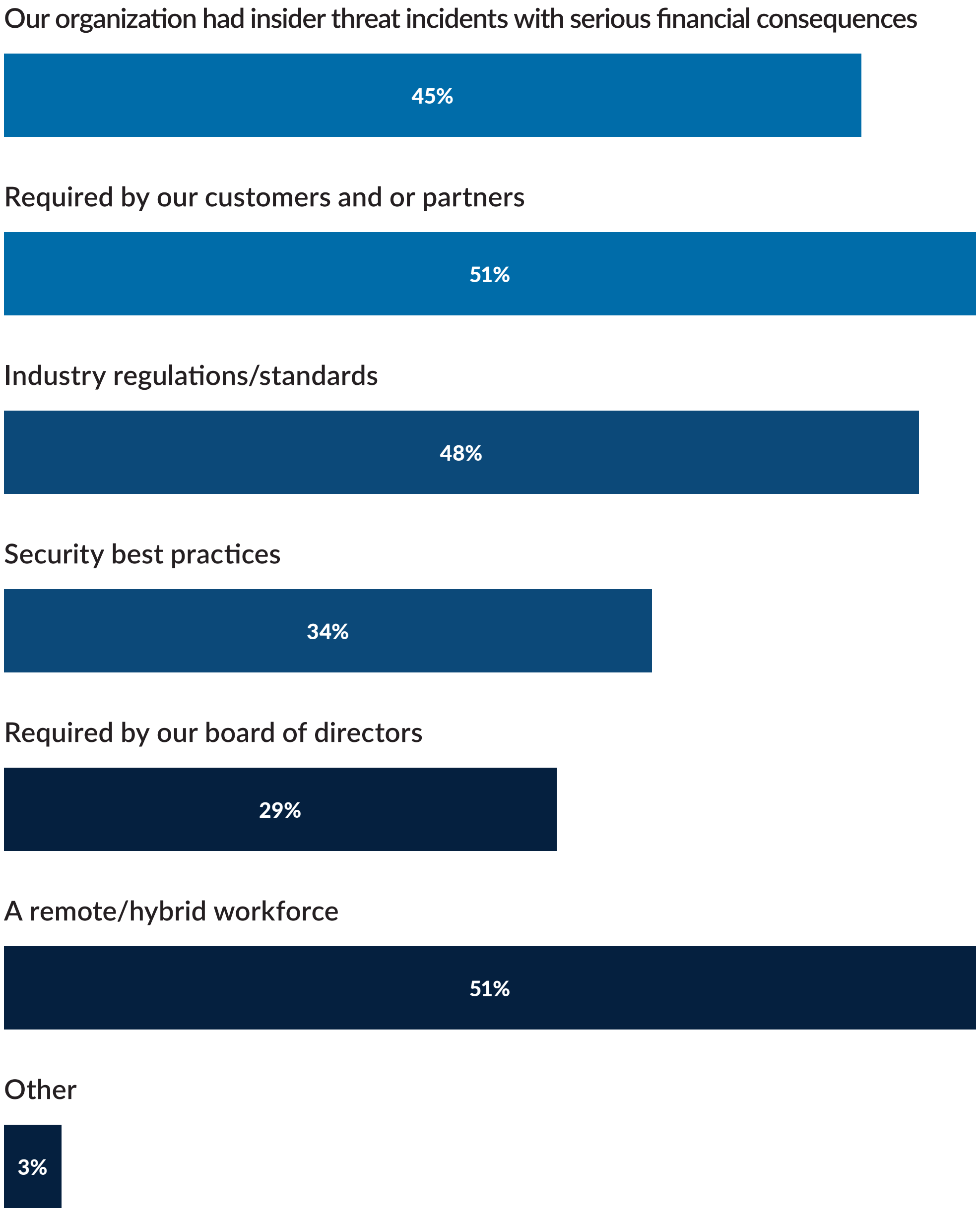


Total (FY2023) = 277%

Figure 23. What are the primary business reasons for having an insider risk program?

Customer and partner requirements, the demands of a hybrid workforce and industry regulations are the primary business reasons for having an insider risk program.

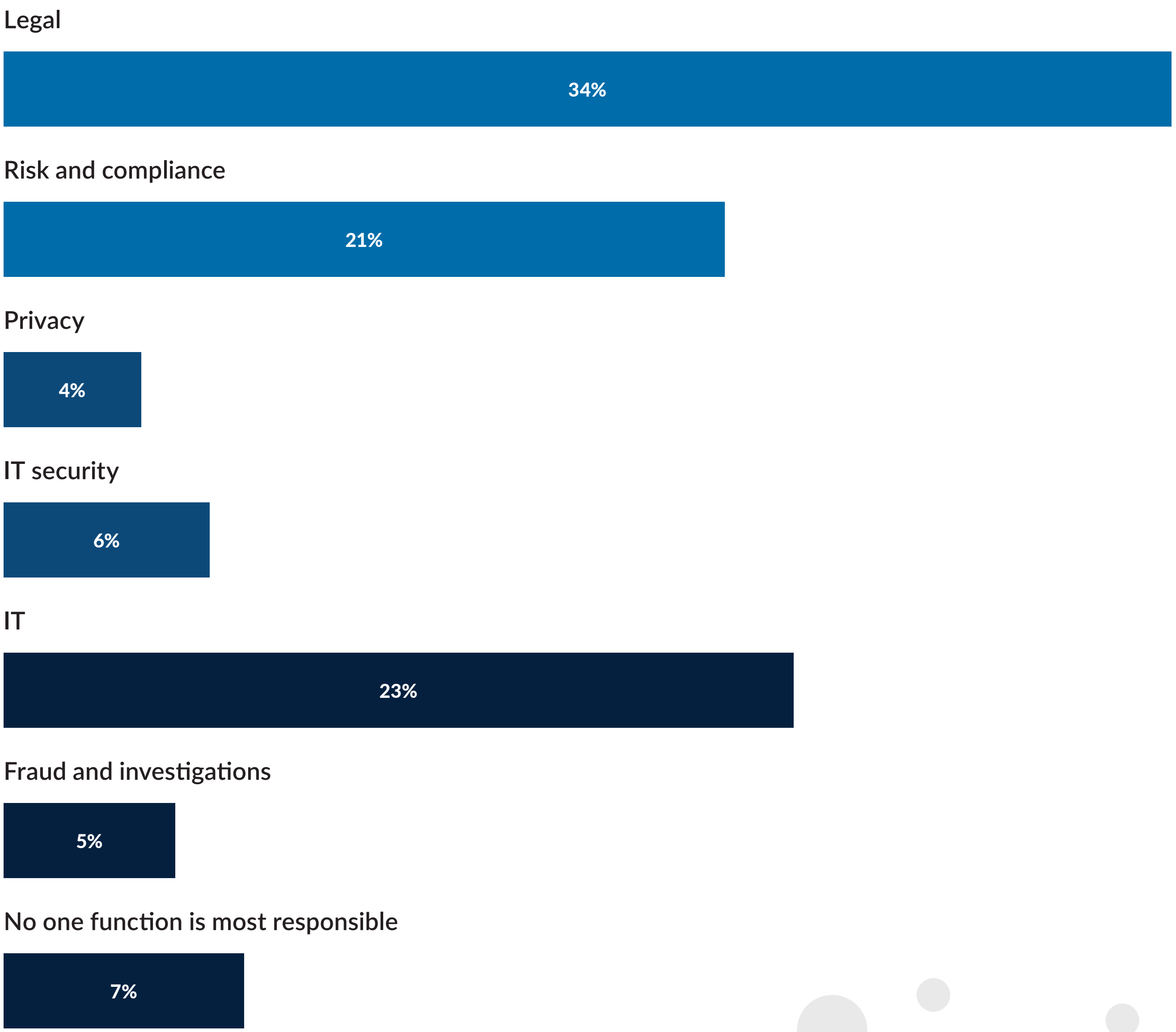
More than one response permitted.



Total (FY2023) = 261%

Figure 24. Which department is most responsible for insider risk management in your organization?

Legal (34%), IT (23%) and risk and compliance (21%) typically bear the most responsibility for insider risk management.

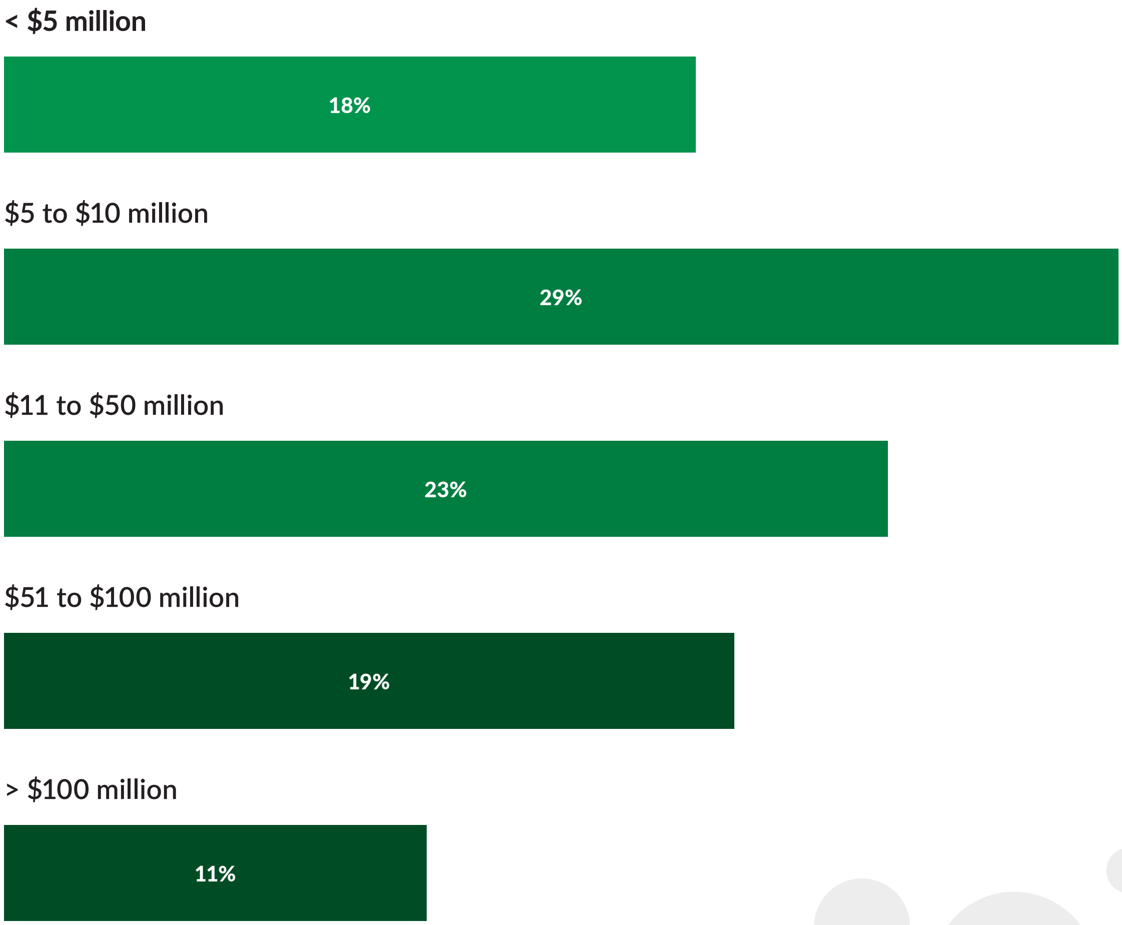


Total (FY2023) = 100%

Figure 25. Approximately, what is the dollar range that best describes your organization's IT security budget this year?

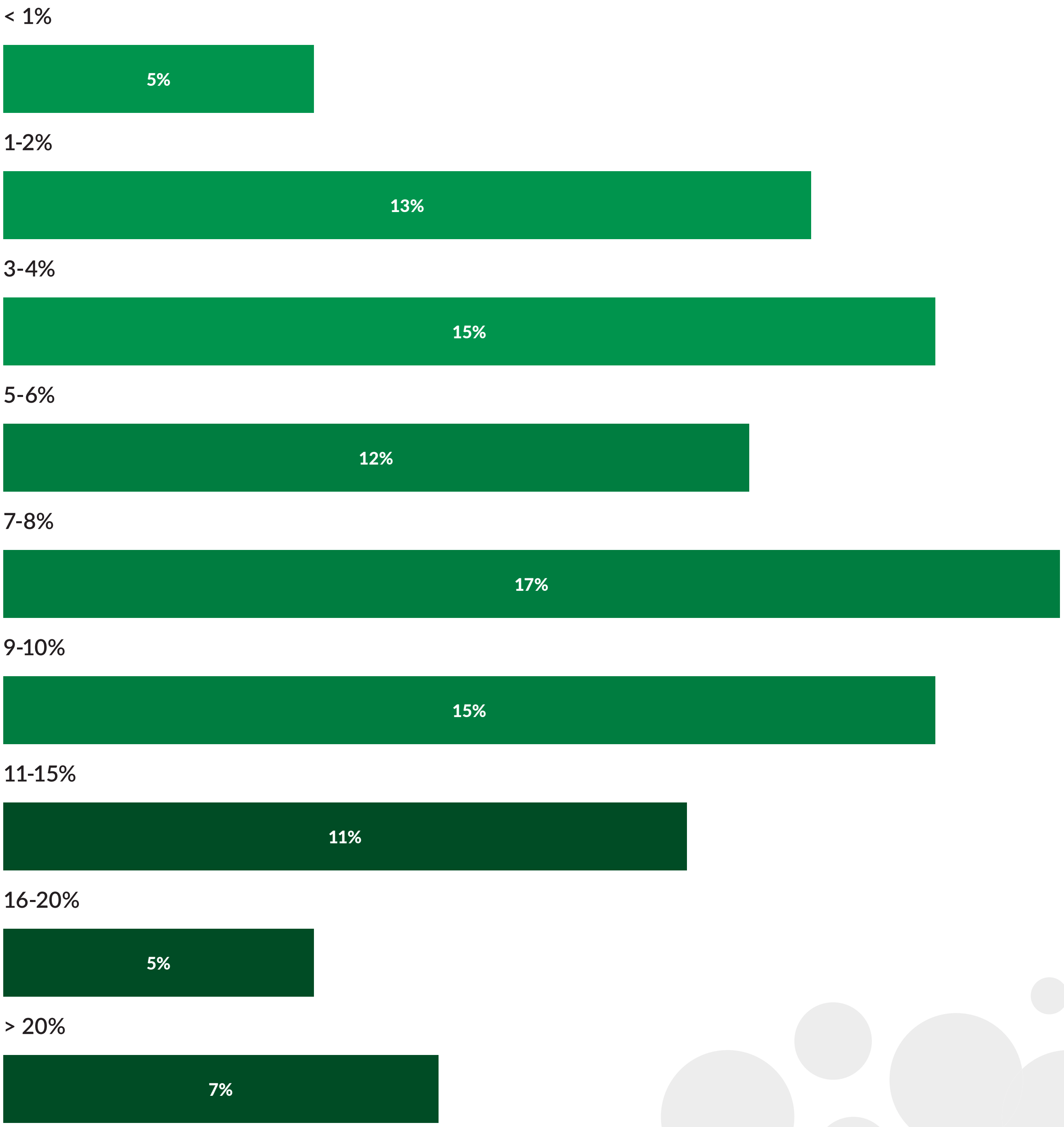
Organizations are trying to fix a $16.2 million problem with just 8.2% of their overall IT security budget.

Organizations had an IT security budget of $2,437 per employee, yet only 8.2% ($200 per employee) was allocated specifically to insider risk management programs and policies.



Total (FY2023) = 100%

Figure 26. What percentage of your organization's IT security budget is allocated to insider risk management?



Total (FY2023) = 100%

Conclusions

If the findings from our study reveal anything, it's that more energy is required to fund and drive proactive insider risk management.

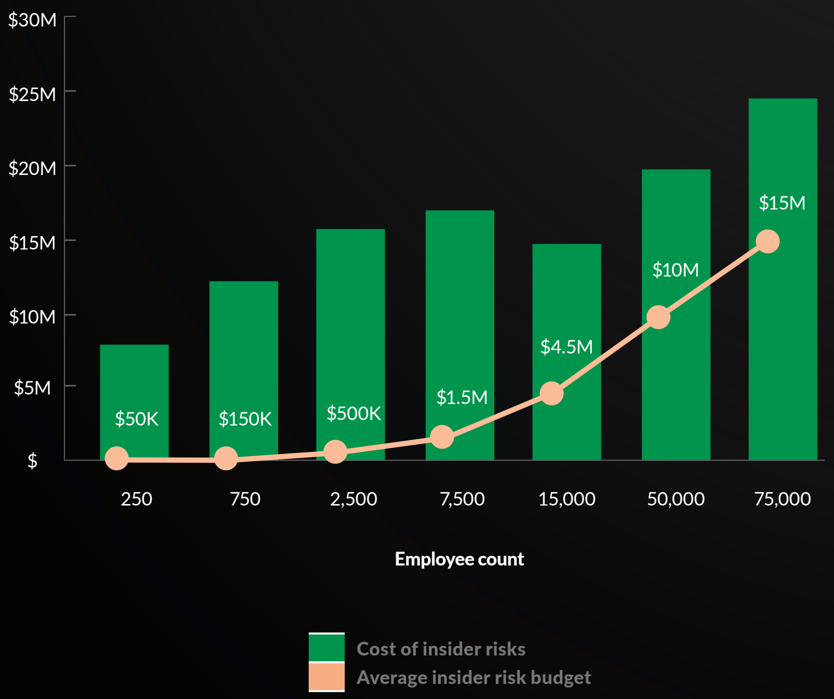
To stop insider risks from escalating into costly incidents, organizations must prioritize a proactive and human-centric approach that cuts across people, processes, technology, and systems. Having an insider risk program can no longer be perceived as a "nice to have", but rather the backbone from which all preventative insider risk mitigation efforts flow.

To date, most budgets have been pivoted on post-incident activities. In fact, of the 8.2% budget allocated to insider risk management, 91.2% is spent reacting to the incident.

This has to change.

To get left of boom, organizations must focus their energy on activities that are specifically designed to prevent insider incidents from occurring in the first place. This is where artificial intelligence (AI) offers great potential.

Figure 27. Insider risk: Cost vs budget



The power of AI

It is encouraging that most organizations (64%) consider AI and machine learning (ML) "essential" to preventing insider incidents. Understanding why people become insider risks means understanding human behavior and why people do the things they do — and AI can help achieve this in spades.

Using AI and ML, analysts can capture early warning signals and apply analysis quickly, easily and at scale. In the case of non-malicious insiders, AI can also help drive automated education and awareness communications to provide "teachable moments" to risky employees in near real time. Given non-malicious insiders are behind most incidents (75%), this is a powerful way for organizations to proactively exercise proportionality when resolving insider risks in a way that is both cost effective and fair.

Benchmark sample

In benchmark research, the unit of analysis is the organization.

Figure 28. Industry sectors of participating organizations

Figure 28 shows the percentage distribution of companies across 13 industry segments. The three largest segments are financial services, industrial and manufacturing, and health and pharmaceuticals. Financial service organizations include banking, insurance, investment management and brokerage. Service organizations represent a wide range of companies, including professional service firms.

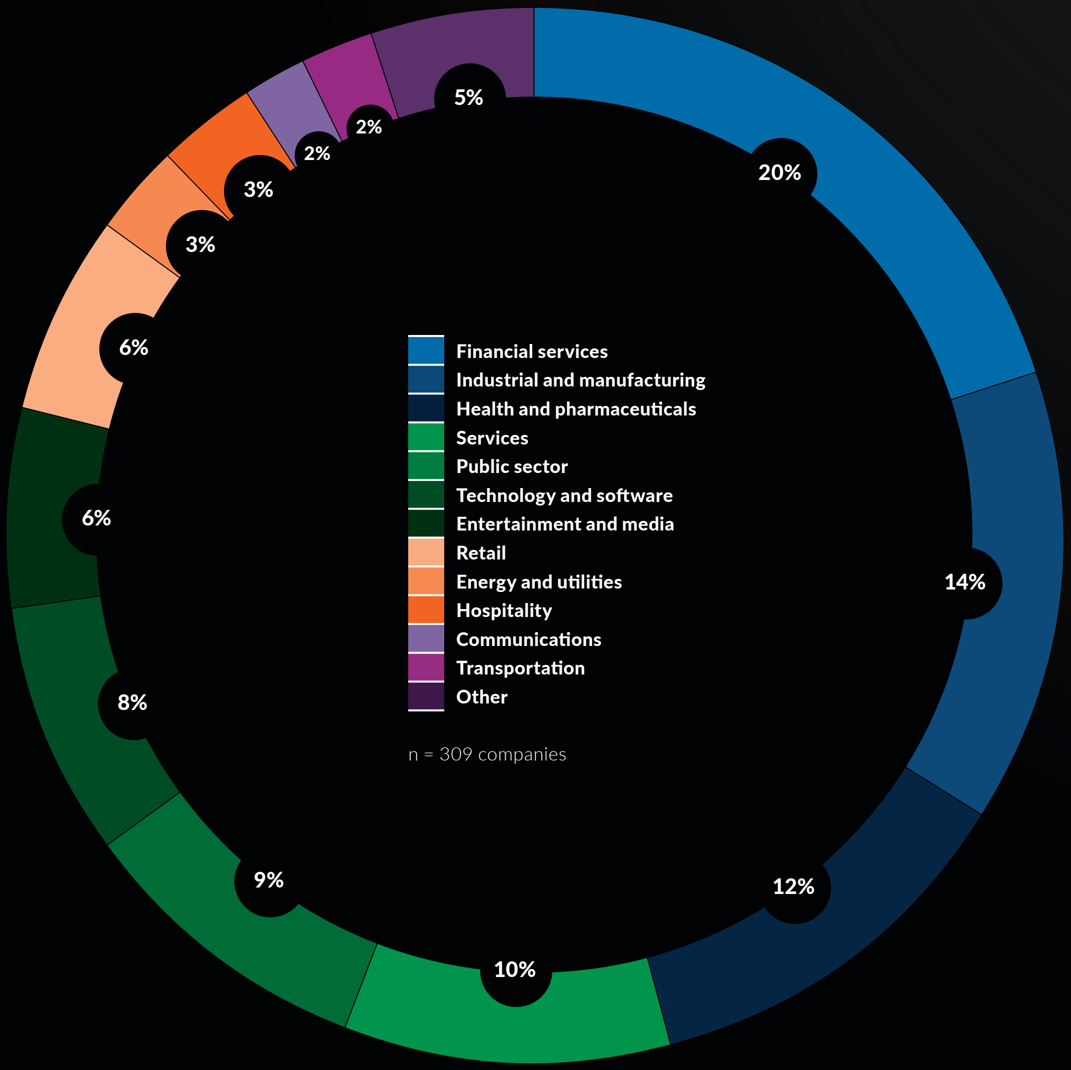


Figure 29. Headcount (size) for participating organizations companies

Figure 29 shows the percentage distribution of companies according to global headcount, which is a surrogate for organizational size. As can be seen, 42% of the sample includes larger-sized companies with more than 5,000 full-time equivalent employees.

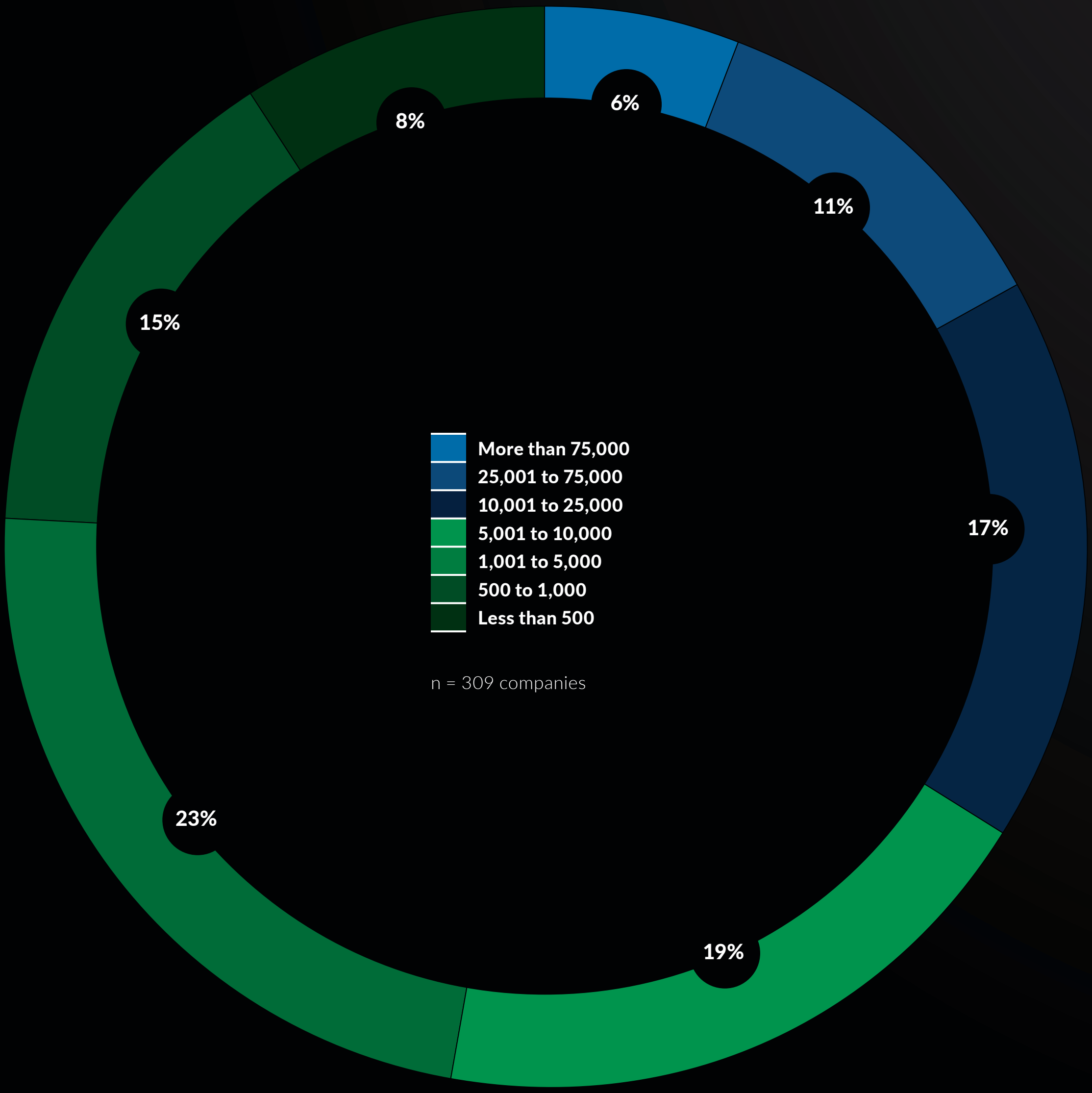


Figure 30. Interviewees by position level or function

According to Figure 30, 1,075 individuals participated in field-based interviews. Each case study involved an average of 4.7 individuals. The three largest segments include: CISO (14%), IT security technician and CIO (12%, respectively).

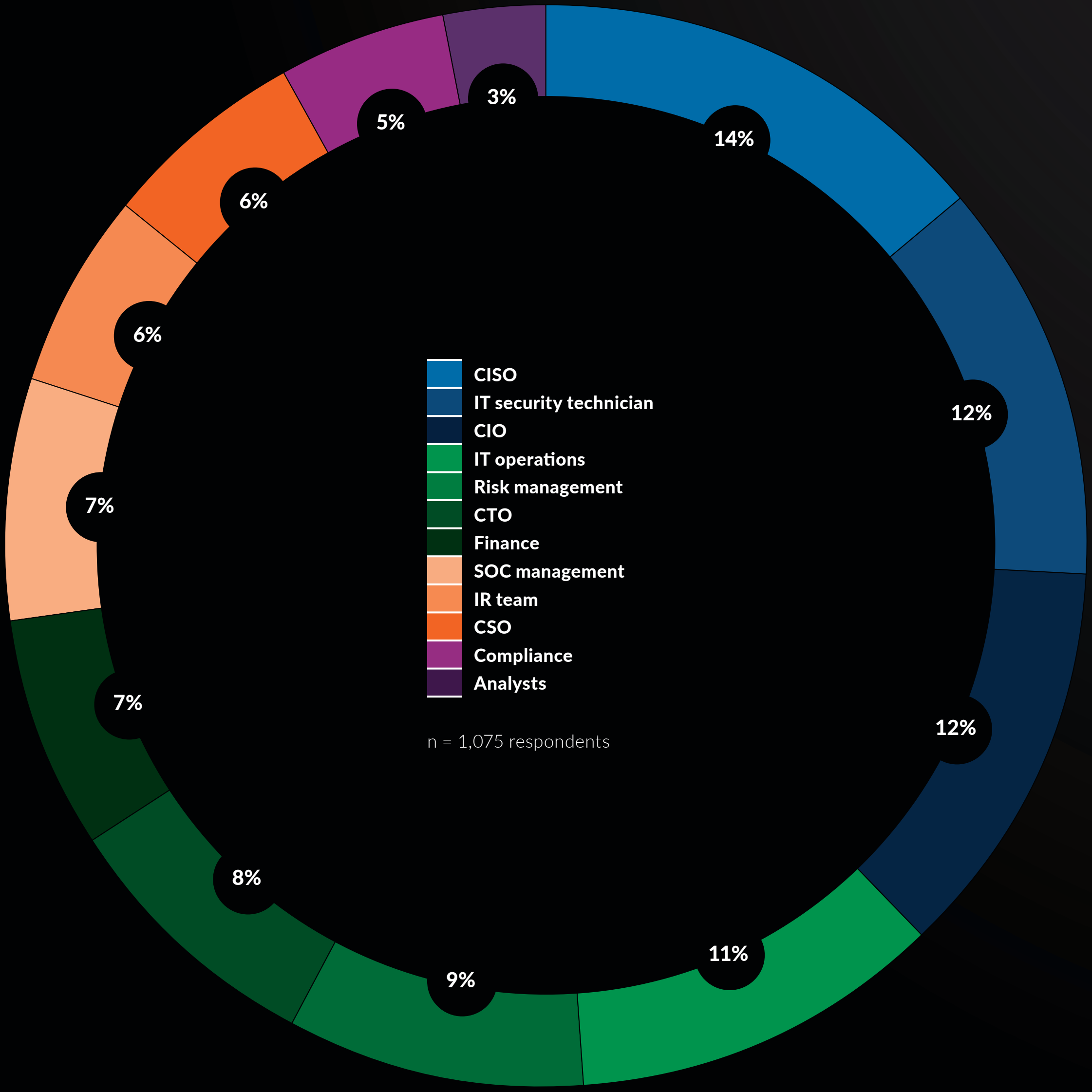
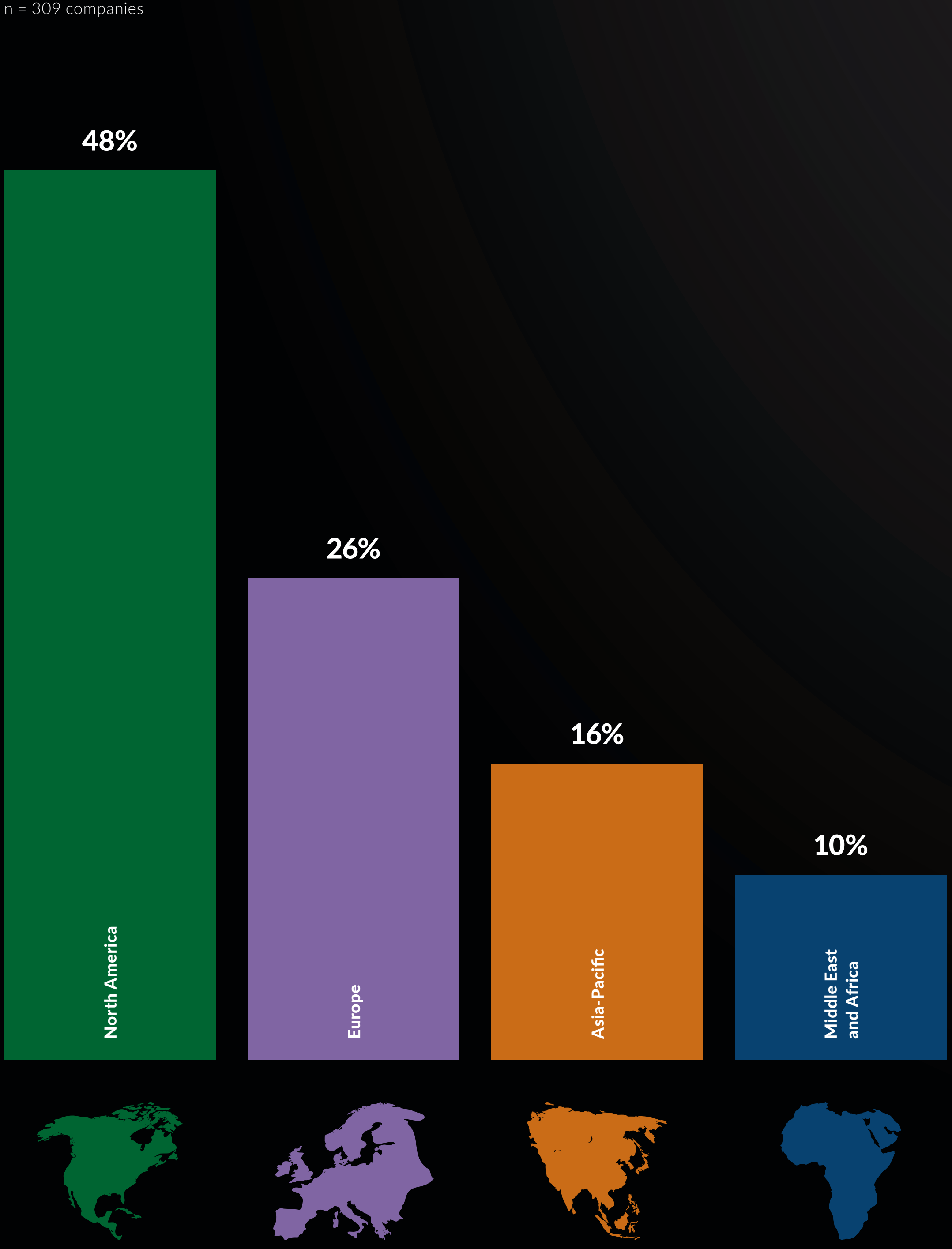


Figure 31. Regional distribution of global organizations

Figure 31 shows the global regions participating in this research. North America represents the largest segment (48% of companies) and the Middle East is the smallest segment (10% of companies).



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 negligence and malicious or 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. It also includes attacks perpetrated by external actors who steal the credentials of legitimate employees/users (i.e., imposter risk).

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.[1]

[1] 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:[2]

- **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.

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 insider 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.

[2] 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 multi-year 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]

LL ________________|_________________UL

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.

Field research was launched in May 2023. To maintain consistency for all benchmark companies, information collected about the organizations' experience was limited to four consecutive weeks. This time frame was not necessarily the same time period as other organizations in this study. The extrapolated direct and indirect costs were annualized by dividing the total cost collected over four weeks (ratio = 4/52 weeks).

Research 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, 159 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.

Ponemon INSTITUTE

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.

DTEX

The Global Leader for Insider Risk Management

As the global leader for insider risk management, DTEX empowers organizations to prevent data loss and support a trusted workforce by stopping insider risks from becoming insider threats. Its InTERCEPT™ platform consolidates the essential elements of Data Loss Prevention, User Behavior Analytics and User Activity Monitoring in a single light-weight platform to detect and mitigate insider risks well before data loss occurs. Combining AI/ML with behavioral indicators, DTEX enables proactive insider risk management at scale without sacrificing employee privacy or network performance.

To learn more about DTEX and how to achieve proactive insider risk management, please visit dtexsystems.com.