2022 COST OF INSIDER THREATS GLOBAL REPORT

Independently conducted by:

Ponemon INSTITUTE

proofpoint.

TABLE OF CONTENTS

INTRODUCTION

Ponemon Institute is pleased to present the findings of the *2022 Cost of Insider Threats Global Report*.

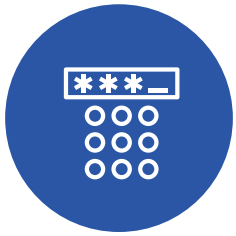
THIS IS THE FOURTH BENCHMARK STUDY CONDUCTED WITH THE EXPLICIT PURPOSE TO UNDERSTAND THE FINANCIAL CONSEQUENCES THAT RESULT FROM INSIDER THREATS. A SECONDARY FOCUS IS TO GAIN INSIGHT INTO HOW WELL ORGANIZATIONS ARE MITIGATING THESE RISKS.

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. In this year's study, we interviewed 1,004 IT and IT security practitioners in 278 organizations that experienced one or more material events caused by an insider. A total of 6,803 insider incidents are represented in this research.

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

A careless or negligent employee or contractor

A criminal or malicious insider



A credential thief

EXECUTIVE SUMMARY

INSIDER THREATS HAVE INCREASED IN BOTH FREQUENCY AND COST OVER THE PAST TWO YEARS. CREDENTIAL THEFTS, FOR EXAMPLE, HAVE ALMOST DOUBLED IN NUMBER SINCE 2020.

However, despite insider threats having increased across all three insider threat profiles, insider threats caused by careless or negligent employees are the most prevalent.

According to the findings, 56% of incidents experienced by organizations represented in this research were due to negligence, and the average annual cost to remediate the incident was $6.6 million.

Research also showed that the cost of an insider threat varies significantly based on the type of incident. This is largely due to the type of activities required following an insider threat incident, including monitoring & surveillance, investigation, escalation, incident response, containment, ex-post analysis and remediation.

Following are some key statistics on the cost of insider-related incidents over a 12-month period:

278 Total number of benchmarked organizations	**6,803** Total number of insider incidents	**$15.4M** Total average annual cost
56% Incidents relating to negligence	**26%** Incidents relating to criminal insider	**18%** Incidents relating to user credential theft
$6.6M Annualized cost for negligence	**$4.1M** Annualized cost for criminal insider	**$4.6M** Annualized cost for credential theft

THE FOLLOWING ARE THE MOST SALIENT FINDINGS FROM THIS RESEARCH.

The time to contain an insider incident increased from the last study.

It took an average of 85 days to contain the incident, an increase from 77 days in the previous study.

Only 12% of incidents were contained in less than 30 days.

Average number of days to contain an incident

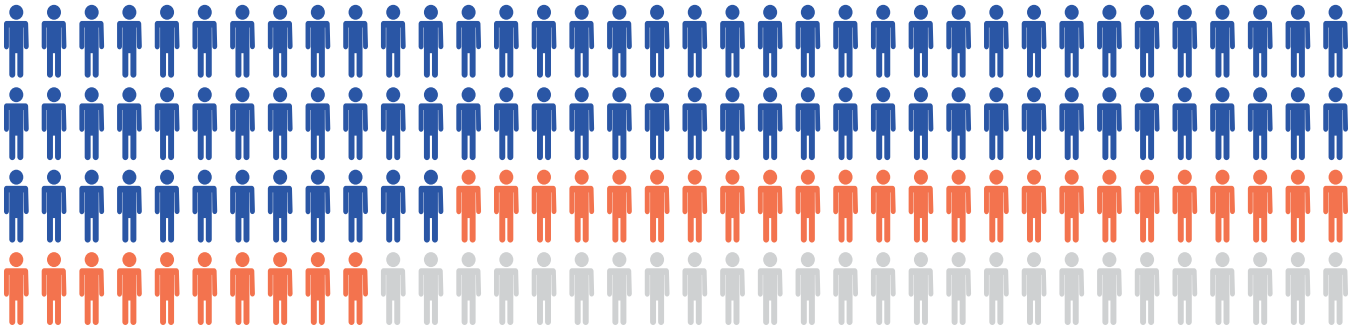
85 DAYS

12% of incidents contained in

≤30 DAYS

34% of incidents contained in

≥90 DAYS



The negligent insider is the root cause of most incidents.

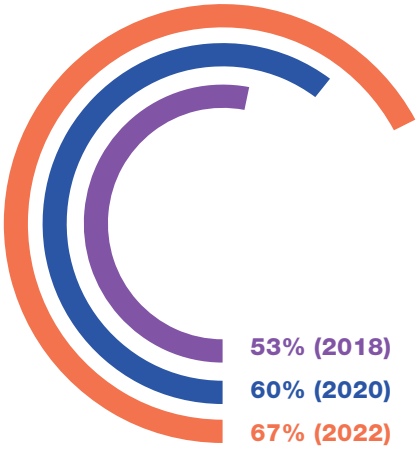
A total of 3,807 attacks, or 56%, were caused by employee or contractor negligence, costing on average $484,931 per incident. This could be the result of a variety of factors, including not ensuring their devices are secured, not following the company's security policy, or forgetting to patch and upgrade.

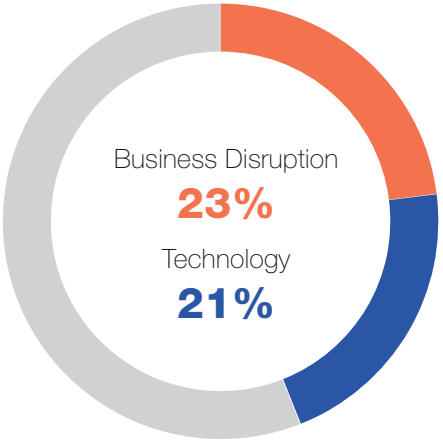
Malicious insiders caused 26% or 1,749 incidents at an average cost per incident of $648,062.

Malicious insiders are employees or authorized individuals who use their data access for harmful, unethical or illegal activities. Because employees are increasingly granted access to more information to enhance productivity in today's work-from-anywhere workforce, malicious insiders are harder to detect than external attackers or hackers.

Credential theft incidents have almost doubled since the last study.

At an average of $804,997 per incident, credential theft is the costliest to remediate. The intent of the credential thief is to steal users' credentials that will grant them access to critical data and information. A favorite technique for many of these credential thieves is social engineering attacks, primarily phishing. A total of an average 1,247 incidents or 18% involved stolen credentials in this year's research.





The frequency of companies experiencing incidents has increased significantly.

According to the 2022 research, 67 percent of companies are experiencing between 21 and more than 40 incidents per year. This is an increase from 60 percent in 2020 and 53 percent in 2018 of companies having between 21 and more than 40 incidents.

Disruption or downtime and investment in technologies represent the most significant costs when dealing with insider threats.

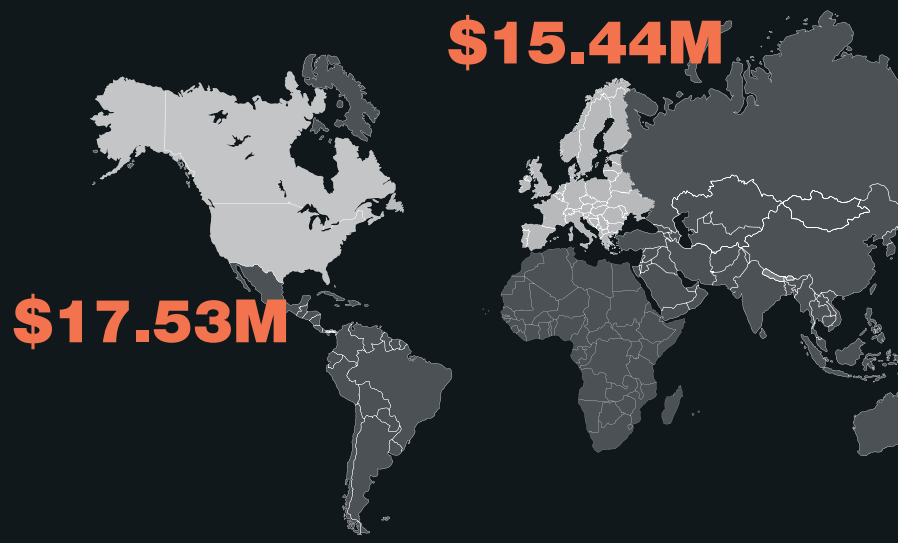
The two largest costs are the impact of business disruption due to diminished employee productivity (23 percent of total cost) and technology, which includes the amortized value and licensing for software and hardware that are deployed in response to insider-related incidents (21 percent).

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

An average of $184,548 is spent to contain the consequences of an insider threat. The least amount of average cost is for escalation $32,228 and monitoring and surveillance $35,080. Incidents that took less than 30 days to contain had the lowest average annual cost of activities at $11.23 million. In contrast, average annual activity costs for incidents that took more than 90 days is $17.19 million.

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

The total average cost of activities to resolve insider threats over a 12-month period is $15.38 million. Companies in North America experienced the highest total cost at $17.53 million. European companies had the next highest cost at $15.44 million.



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

The average activity cost for financial services is $21.25 million and services is $18.65 million. Service organizations represent a wide range of companies including accounting, consultancy and professional service firms.

Organizational size affects the cost per incident.

The annual cost of incidents varies according to organizational size. Large organizations with a headcount of more than 75,000 spent an average of $22.68 million over the past year to resolve insider-related incidents. To deal with the consequences of an insider incident, smaller-sized organizations with a headcount below 500 spent an average of $8.13 million.

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

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

Of all the types of insider threat in this research, organizations are most concerned about credential theft. Credential thefts have almost doubled since the last study and cost the most to remediate. Fifty-five percent of respondents say they are most concerned about a hacker stealing the valid credentials of an employee. Far fewer respondents (21 percent) are concerned about the negligent insider.

Negligent employees and credential thieves are the root causes of most insider incidents. Fifty-seven percent of respondents say the insider incidents involved employee negligence and 51 percent say a malicious outsider stole data by compromising insider credentials or accounts.

Vulnerable IoT devices are of greatest risk to data loss. Sixty-three percent of respondents say they are worried about unmanaged IoT devices resulting in the loss of sensitive data. This is followed by the cloud (52 percent of respondents) and the network (51 percent of respondents).

Most sensitive data is in employees' email. Sixty-five percent of respondents say email is where employees store their organizations most sensitive data such as personally identifiable information (PII), intellectual property (IP) and other critical business information.

Malicious insiders use corporate email to steal sensitive data. Seventy-four percent of respondents say malicious insiders emailed sensitive data to outside parties followed by scanning for open ports and vulnerabilities (62 percent of respondents) and accessing sensitive data not associated with the role or function (60 percent of respondents).

As the volume and time to contain insider threats increases, advanced technologies such as user behavior tools and automation are important to helping reduce insider threats. User behavior-based tools for detecting insider threats are considered essential or very important to reducing insider threats (62 percent of respondents). This is followed by automation for the prevention, investigation, escalation, containment and remediation of insider incidents (55 percent of respondents) and AI and machine learning to prevent, investigate, escalate, contain and remediate insider incidents (54 percent of respondents).

05

signs that your organization is at risk

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

02 Employees are unaware of the steps they should take at all times to ensure that the devices they use—both company issued and BYOD—are secured at all times.

03 Employees are sending highly confidential data to an unsecured location in the cloud, exposing the organization to risk.

04 Employees break your organization's security policies to simplify tasks.

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

ABOUT THE 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 threats:

- 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 cost
- 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 2021. Our final benchmark sample consisted of 278 separate organizations. A total of 1,004 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
- Locations throughout the following regions: North America, Europe, Middle East & Africa and Asia-Pacific
- Central IT function with control over on-premise and/or cloud environment
- Experienced one or more material incidents caused by careless, malicious or criminal 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 278 organizations:

- Careless or negligent employee or contractor
- Criminal insider including employee or contractor malice
- Employee/user credential theft (a.k.a. imposter risk)

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:

01 Working sessions to establish areas of inquiry

02 Recruitment of benchmark companies

03 Development of an activity-based costing framework

04 Administration of research program

05 Analysis of all results with appropriate reliability checks

06 Preparation of a report that summarizes all salient research findings

BENCHMARKED SAMPLE

IN BENCHMARK RESEARCH, THE UNIT OF ANALYSIS IS THE ORGANIZATION.

FIGURE 1.

Industry sectors of participating organizations

Figure 1 shows the percentage distribution of companies across 13 industry segments. The three largest segments are financial services, services and industrial & manufacturing. Financial service organizations include banking, insurance, investment management and brokerage. Service organizations represent a wide range of companies, including accounting, consultancy and professional service firms.

n = 278 companies

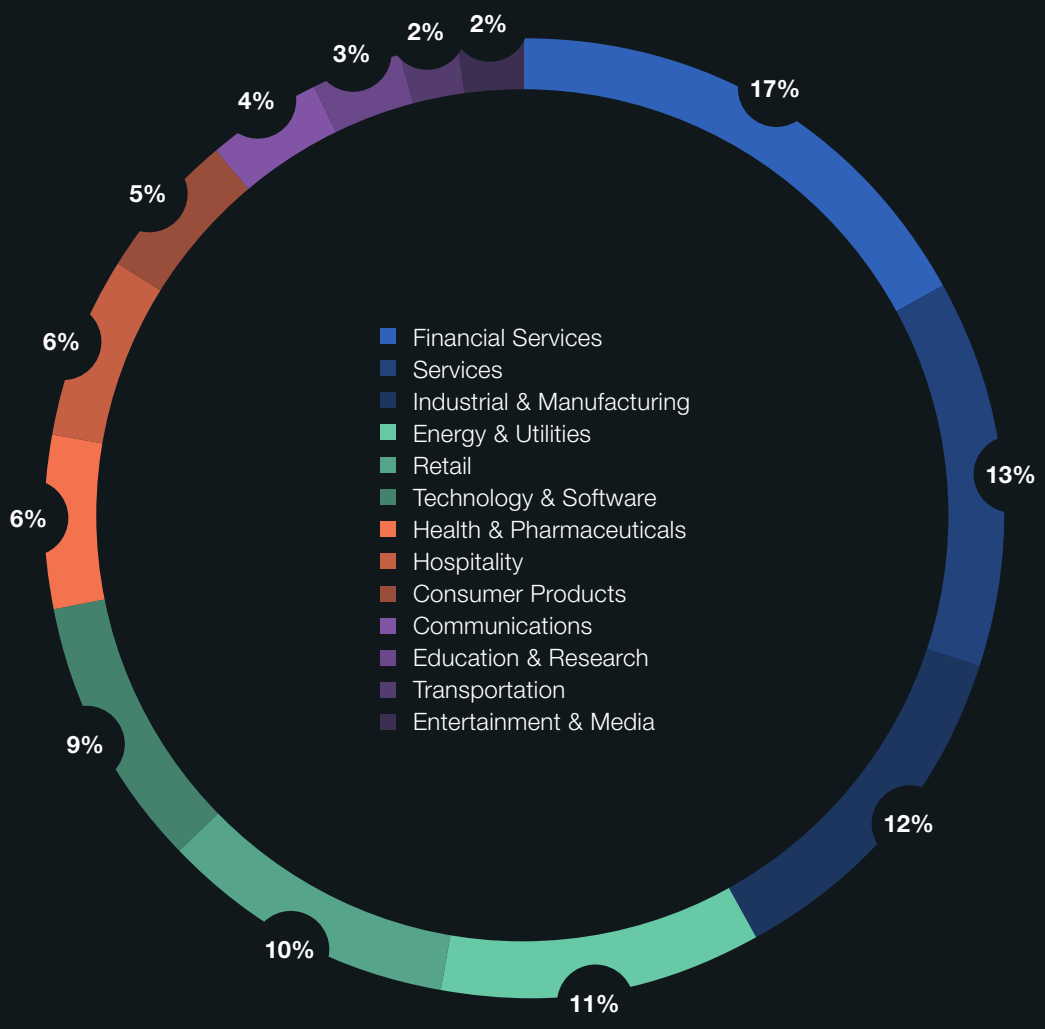


FIGURE 2.

Headcount (size) for participating organizations

Figure 2 shows the percentage distribution of companies according to global headcount, which is a surrogate for organizational size. As can be seen, 50 percent of the sample includes larger-sized companies with more than 5,000 full-time equivalent employees.

n = 278 companies

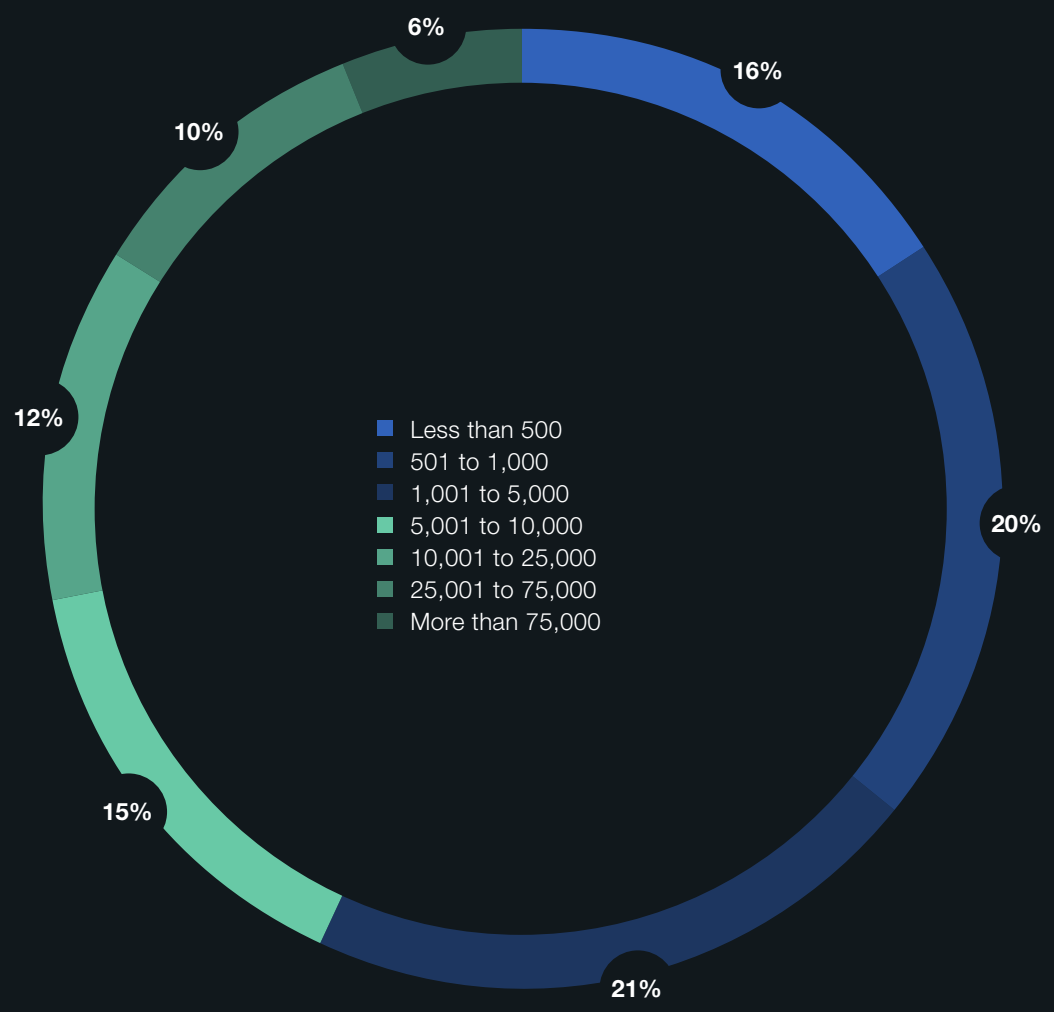


FIGURE 3.

Interviewees by position level or function

According to Figure 3, 1,004 individuals participated in field-based interviews. Each case study involved an average of 4.7 individuals. The three largest segments include: CISO (15 percent), IT operations (14 percent), CIO (12 percent) and IT technician (11 percent).

n = 1,004 respondents

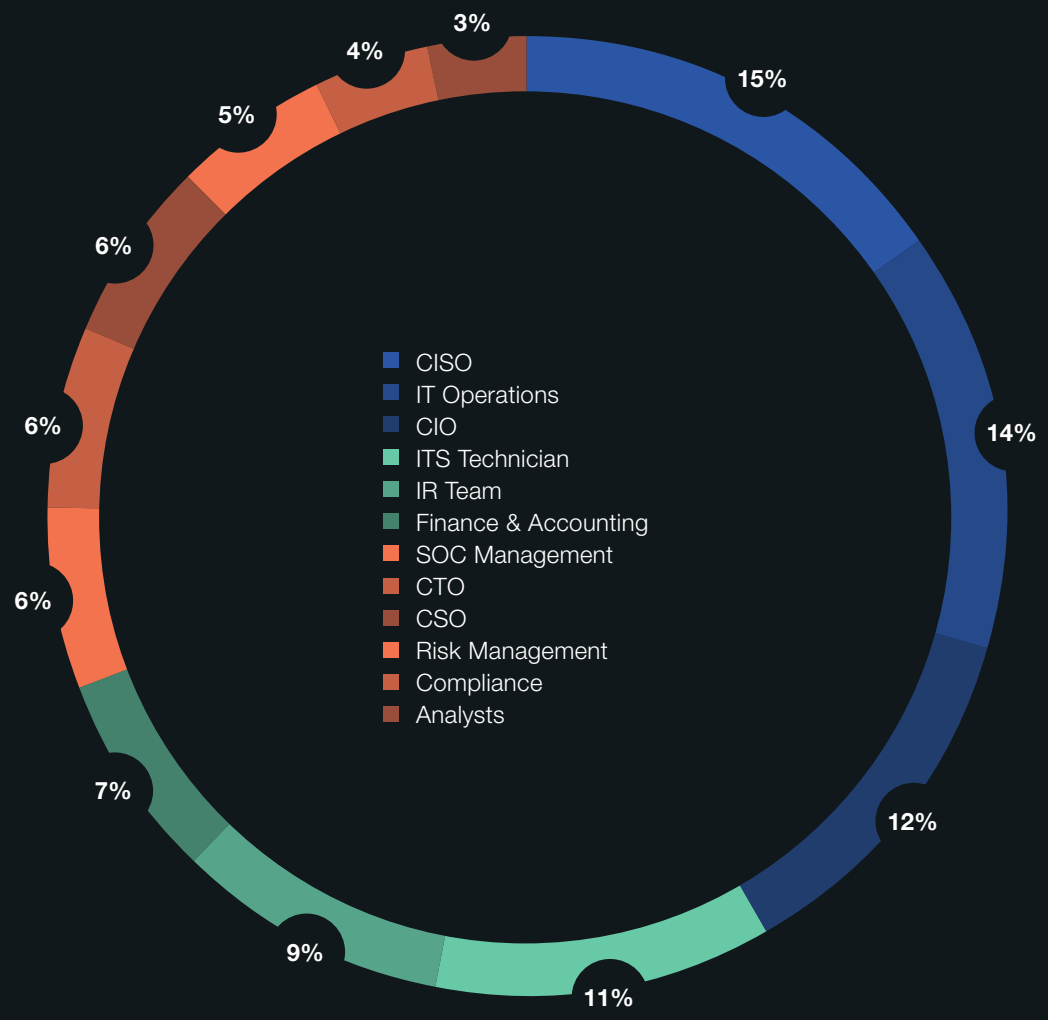
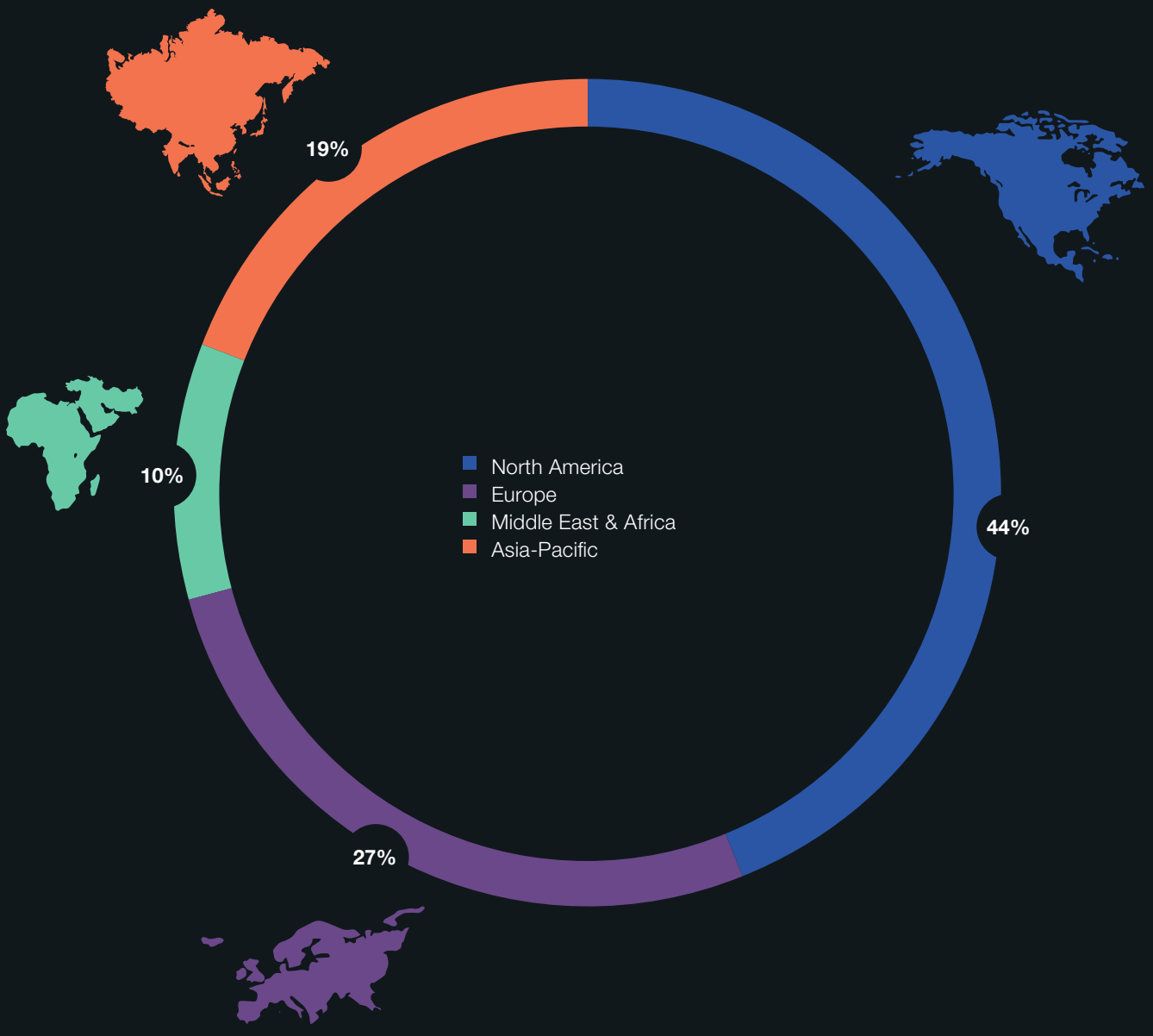


FIGURE 4.

Regional distribution of global organizations

Figure 4 shows the global regions participating in this research. North America represents the largest segment (44 percent of companies) and the Middle East and Africa is the smallest segment (10 percent of companies).

n = 278 companies



KEY FINDINGS

THE LARGEST NUMBER OF REPORTED INCIDENTS FOR A GIVEN COMPANY IS 46 AND THE SMALLEST NUMBER OF INCIDENTS IS ONE.

Employee or contractor negligence

3,807

Criminal or malicious insider

1,749

Credential thief (imposter risk)

1,247

FIGURE 5.

Frequency of 6,803 incidents for three insider profiles

Employees or contractors continue to be the primary source of an insider threat. Figure 5 shows the distribution of 6,803 reported attacks analyzed in our sample. A total of 3,807 attacks (or 56 percent) were caused by employee or contractor negligence. Criminal or malicious insiders caused another 1,749 attacks (or 26 percent) and there were 1,247 credential thefts (18 percent).

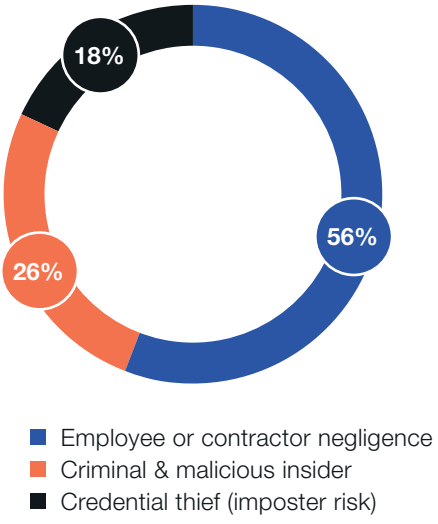
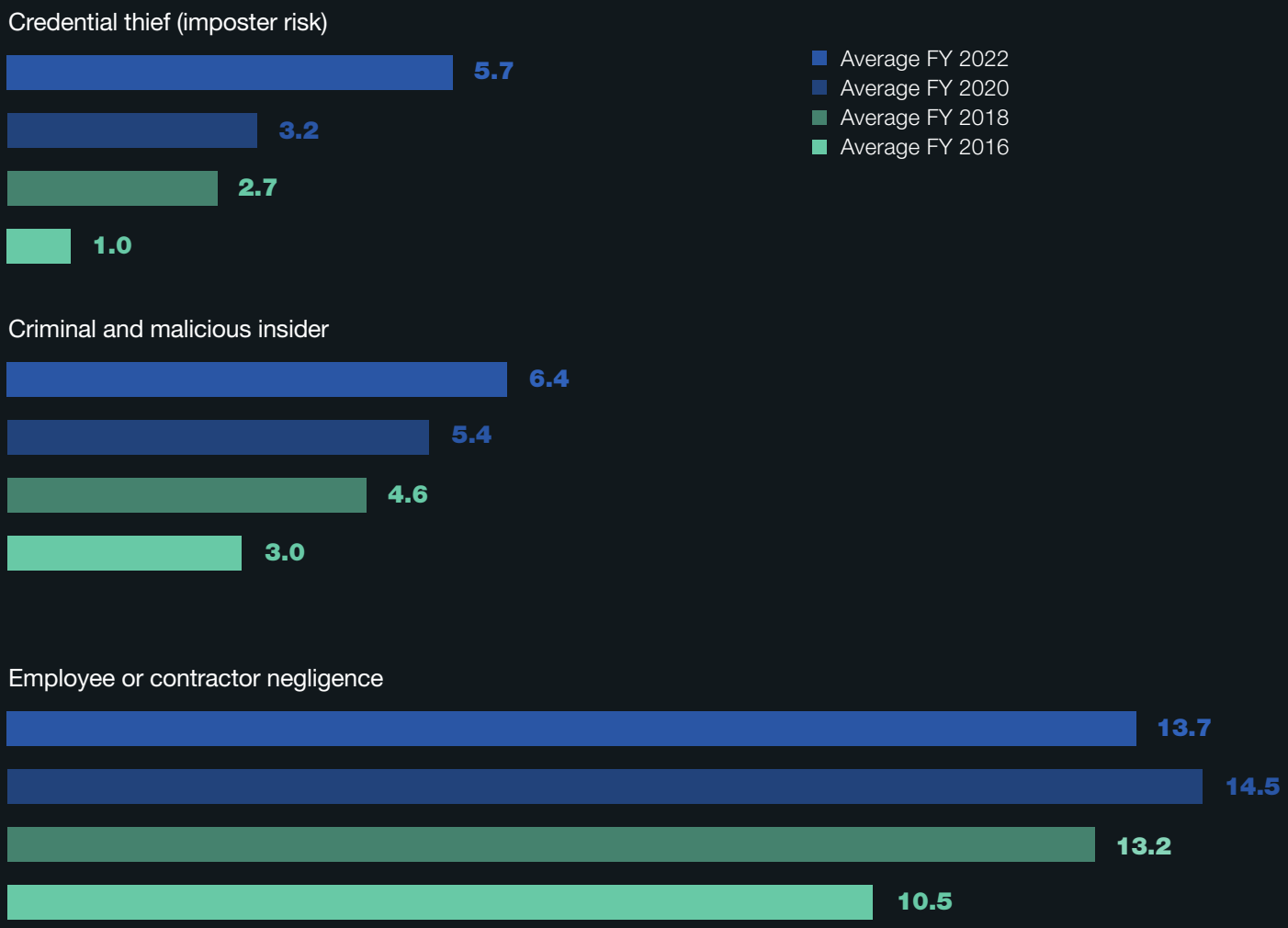


FIGURE 6.

Frequency for three profiles of insider incidents

The average number of criminal and credential theft incidents have almost doubled. As shown in Figure 6, credential theft has increased from an average of 3.2 incidents in 2020 to 5.7 incidents in this year's study. Criminal and malicious insider incidents increased from 5.4 to 6.4.[1] Employee or contractor negligence decreased slightly from 14.5 to 13.7.



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

FIGURE 7.

Frequency of insider-related incidents per company

The frequency of incidents per company has increased significantly. Figure 7 shows the average consolidated frequency of employee/contractor negligence, criminal/ malicious insider and credential theft incidents per company. According to the 2022 research, 67 percent of companies are experiencing between 21 and more than 40 incidents per year. This is an increase from 60 percent in 2020 and 53 percent in 2018 of companies having between 21 and more than 40 incidents.

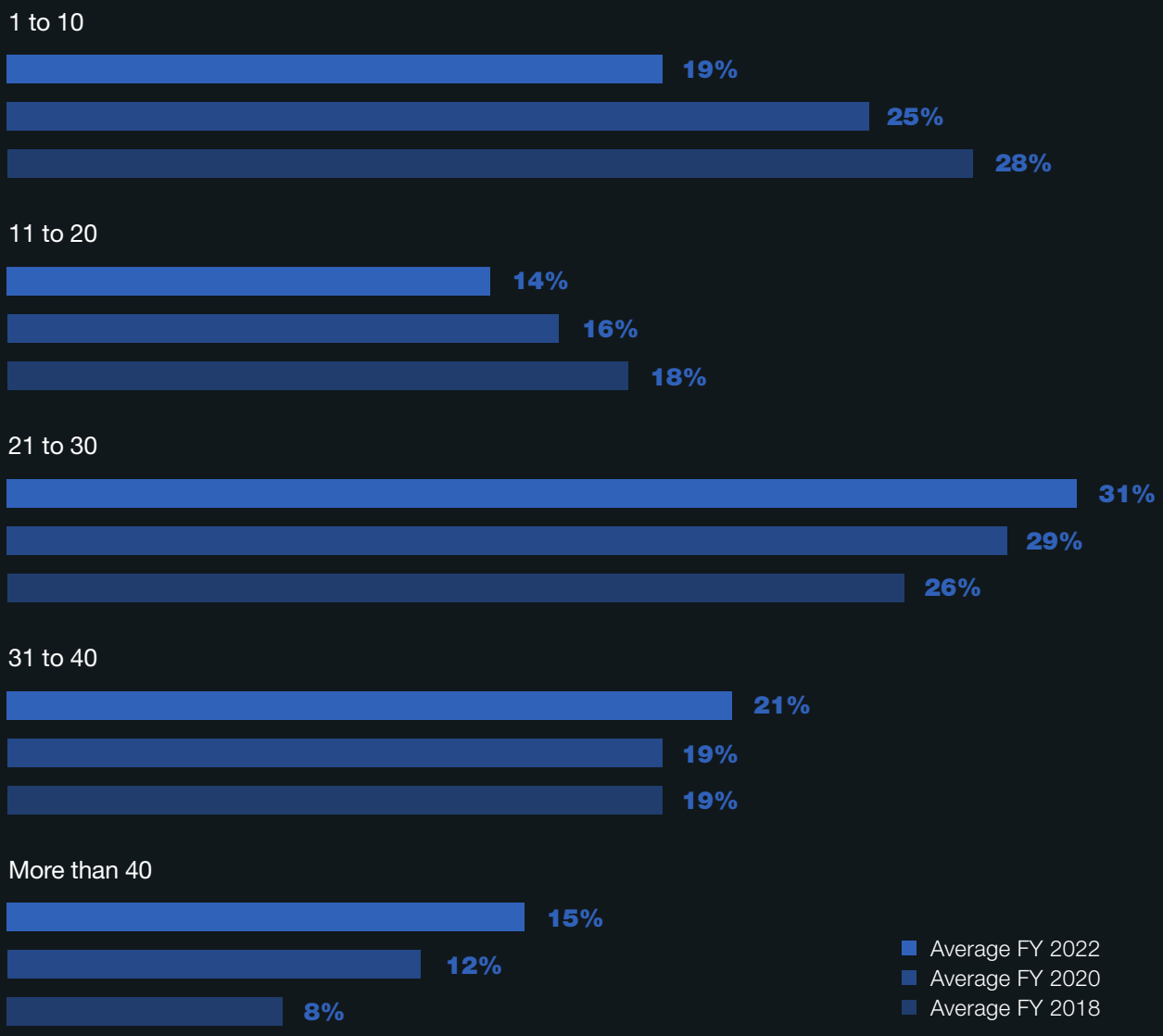


FIGURE 8.

Average incident frequency for three profiles by geographic region

Companies in the Middle East and Africa experience the most insider incidents and Asia-Pacific had the least incidents. Figure 8 presents the frequency of insider incidents in the four regions represented in the research. In all regions, employee or contractor negligence occur most frequently. North America and the Middle East and Africa are most likely to experience credential theft.

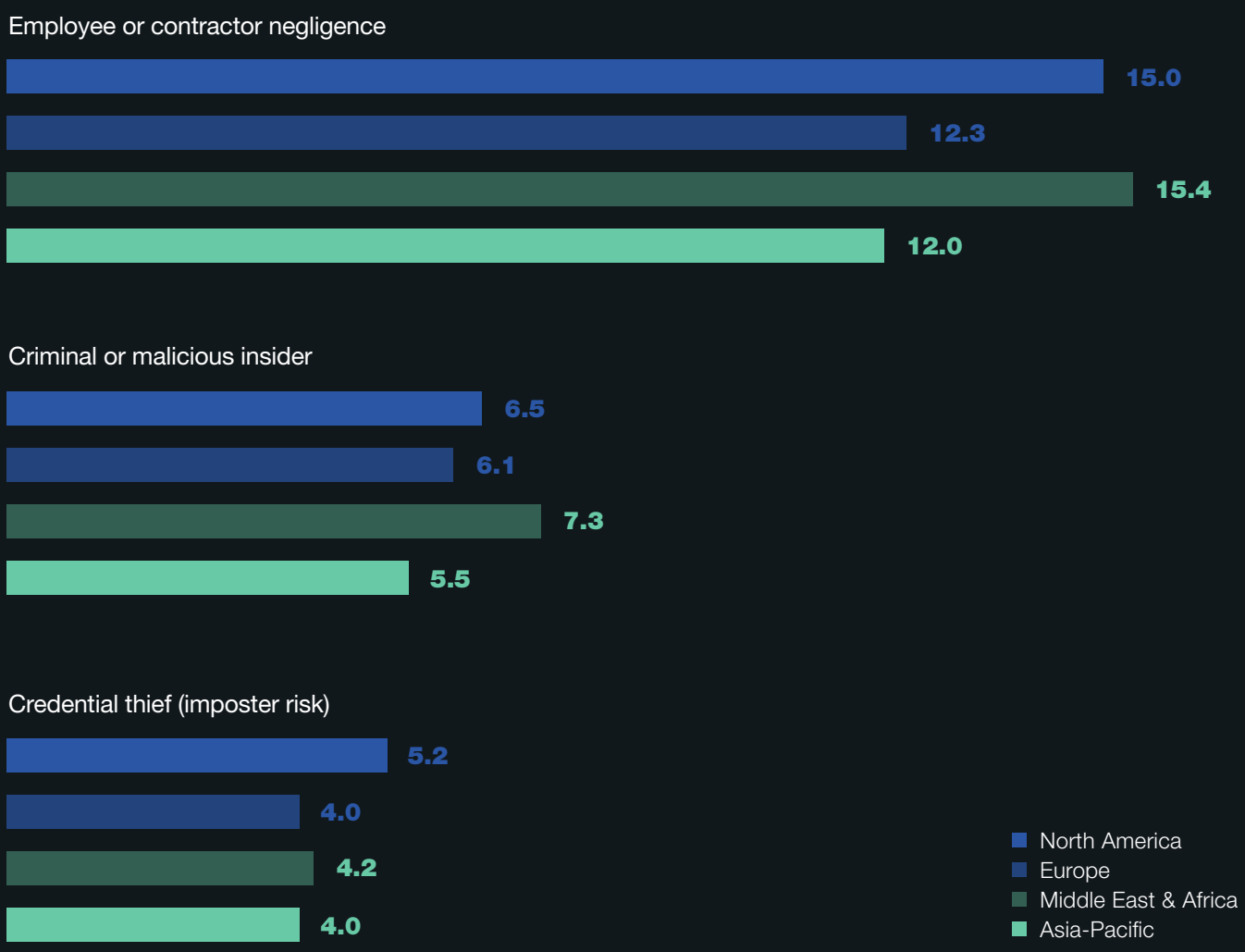


FIGURE 9.

Scattergram of insider-related incidents by company

Figure 9 shows a scattergram of insider incidents per company. Of the 278 participating companies, 152 companies (55 percent) of companies had an average total cost at or below the mean of $15.4 million over the past 12 months. The remaining 125 companies (45 percent) are above the average of $15.4 million. This finding suggests that the distribution is slightly skewed.

n = 278 companies

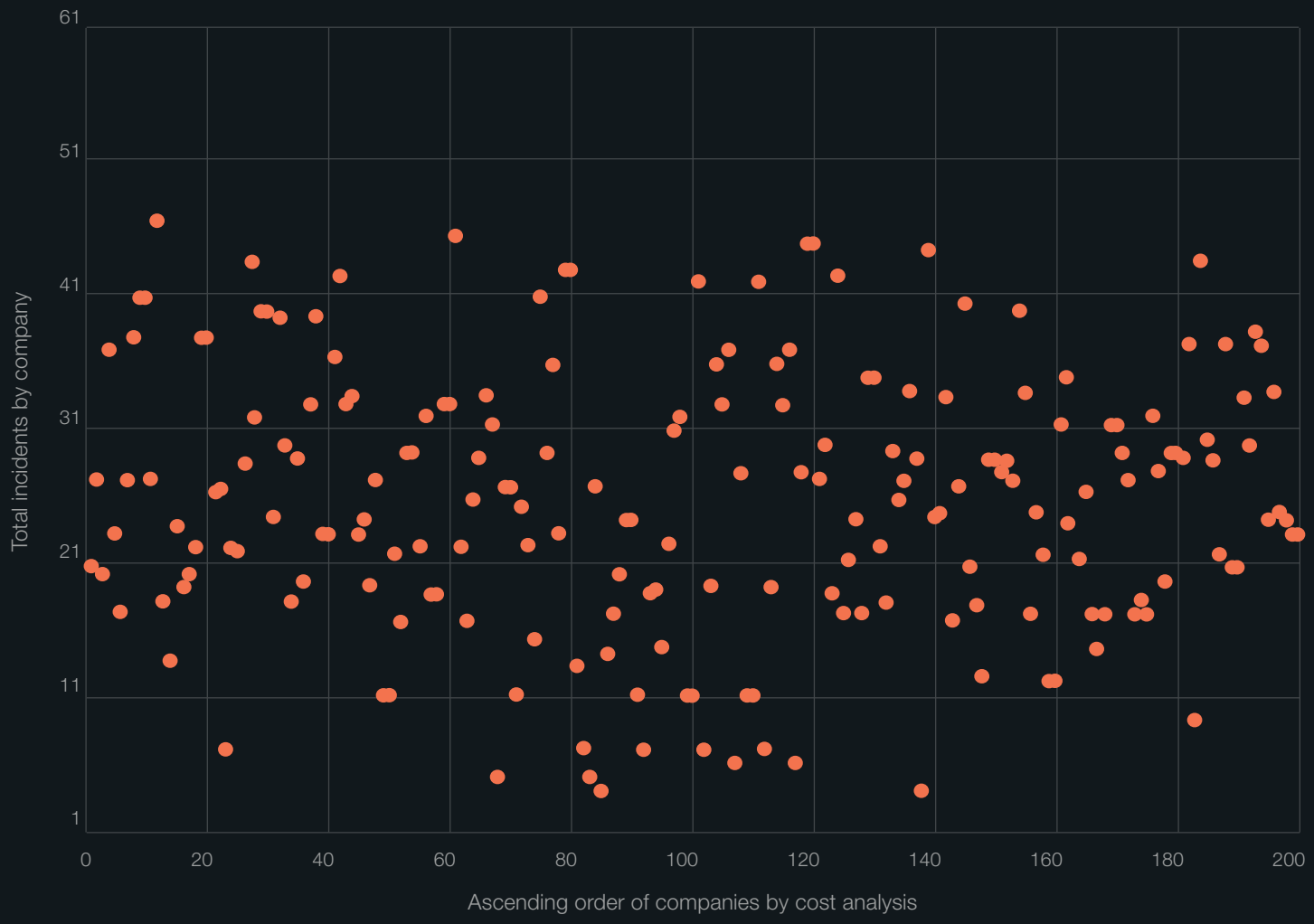


FIGURE 10.

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

Companies are spending an average of 85 days to contain one insider security incident. According to Figure 10, the time to contain insider-related incidents in our benchmark sample took an average of 85 days to contain the incident. Only 12 percent of incidents were contained in less than 30 days.

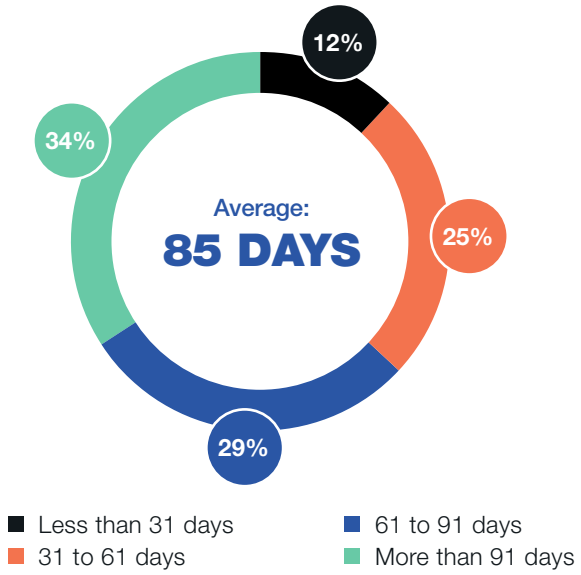


TABLE 1.

Tools and activities that reduce insider threats

Based on our interviews, the top three technologies that result in the greatest cost reductions are data loss prevention, privileged access management and user and entity behavior analytics as shown in Table 1.

More than one response permitted

TECHNOLOGIES USED TO REDUCE THE COST OF THE THREE ROOT CAUSES OF INSIDER RISK	PCT%
Data Loss Prevention (DLP)	64%
Privileged Access Management (PAM)	60%
User and Entity Behavior Analytics (UEBA)	57%
Security Information and Event Management (SIEM)	53%
Endpoint Detection and Response (EDR)	50%
Insider Threat Management (ITM)	41%
Other (please specify)	3%
Total	**328%**

FIGURE 11.

Percentage of insider cost by consequence to business organization

Disruption or downtime and technologies represent the most significant costs when dealing with insider incidents. Figure 11 reports the percentage of insider cost for careless or negligent employees, criminal insiders and credential theft according to seven cost categories. The two largest cost categories are the impact of business disruption due to diminished employee/user productivity (23 percent of total cost) and technology, which includes the amortized value and the licensing for software and hardware that are deployed in response to insider-related incidents (21 percent).

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

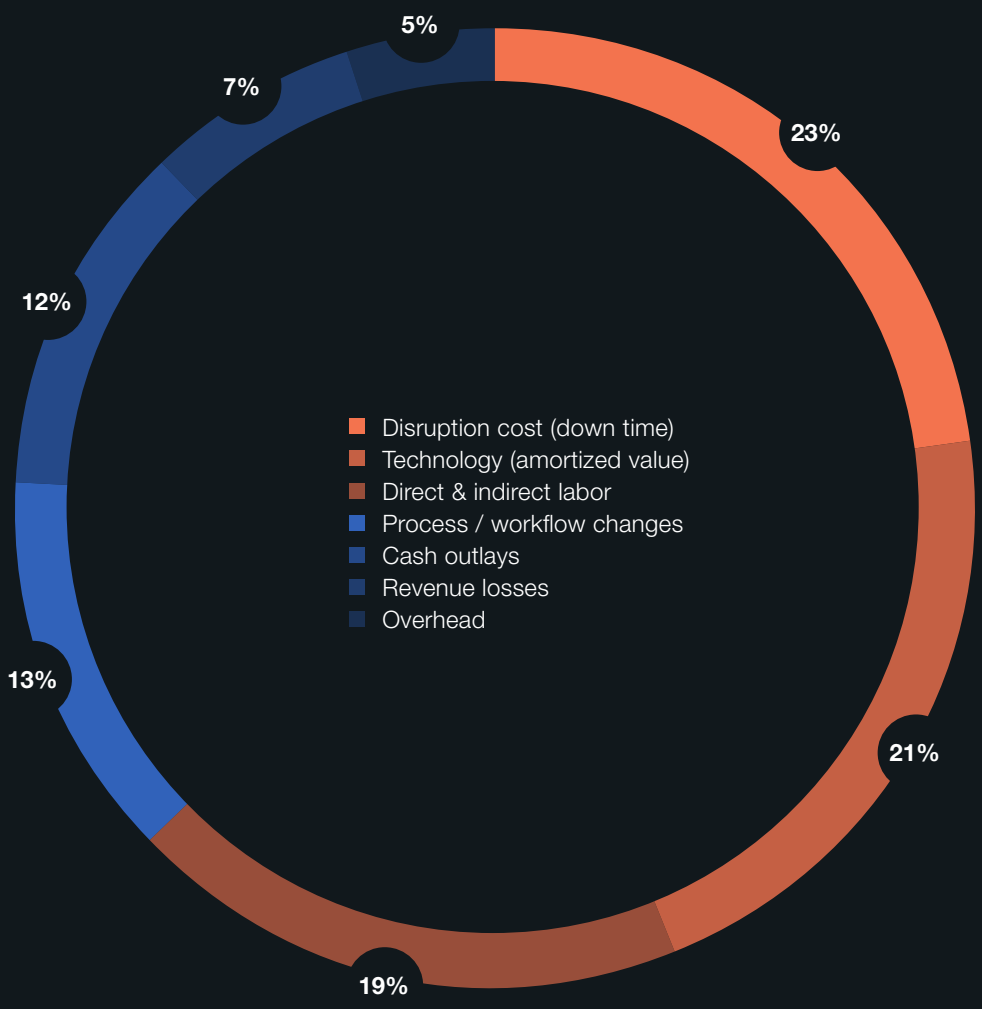


FIGURE 12.

Insider incidents in ascending order by headcount (size)

THE LARGER THE ORGANIZATION, THE MORE INSIDER INCIDENTS.

Figure 12 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.

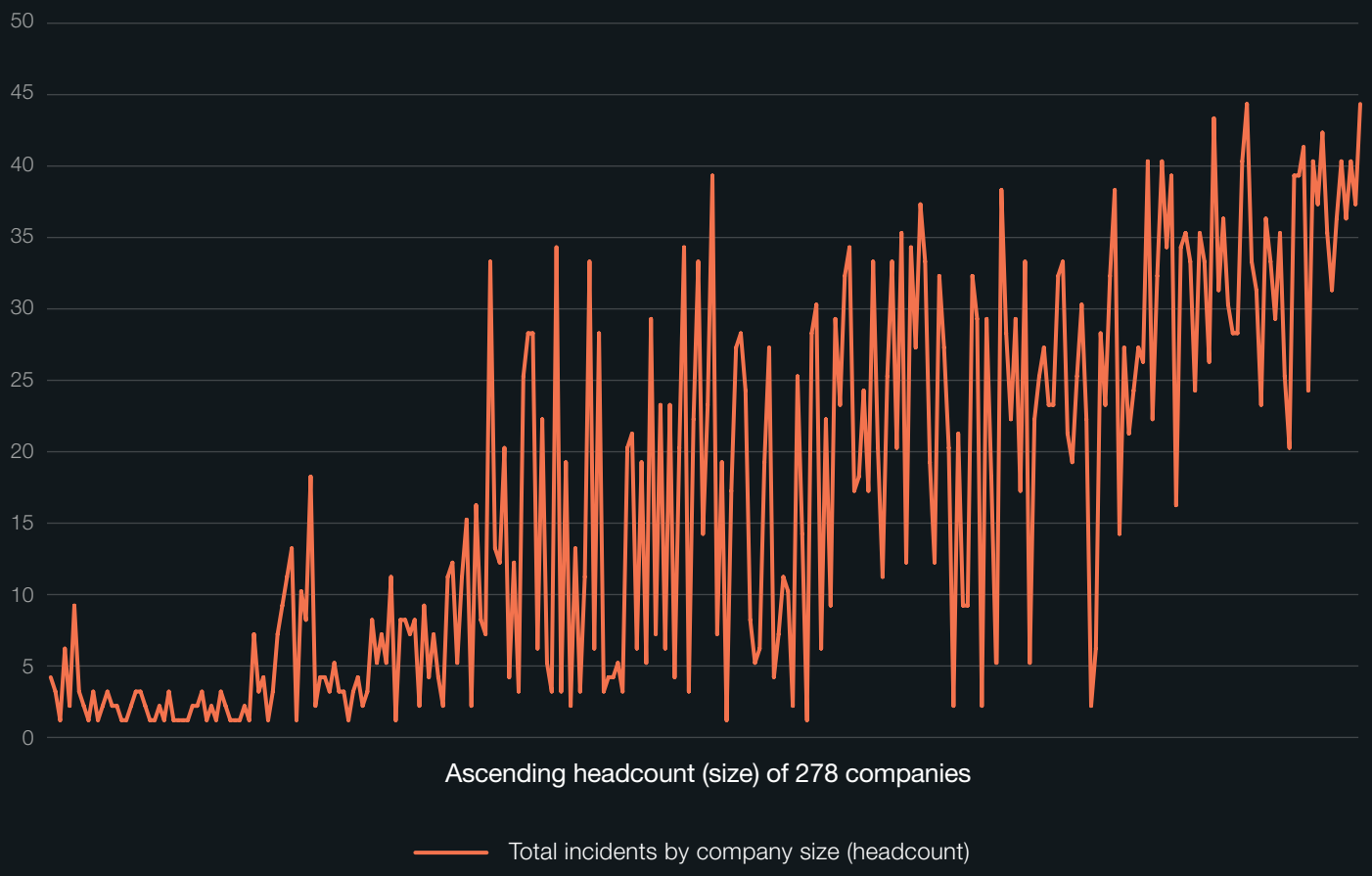


TABLE 2.

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

Credential theft continues to be the costliest insider security incident. 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. However, the average cost per this type of incident is far less than credential theft and malicious insider incidents.

The cost of criminal insider incidents steadily increased between 2018 and 2020 from $614,192 to $755,761 but declined to $648,062 in this year's research. The average number of credential thefts has increased significantly since 2018 and the average cost for remediating these incidents is $804,997 in this year's research.

FY 2018 CASE PROFILES	AVERAGE COST PER INCIDENT	MEAN NUMBER OF INCIDENTS PER YEAR	AVERAGE ANNUALIZED COST
Employee or contractor negligence	$277,557	13.2	$3,663,752
Criminal & malicious insider	$614,192	4.6	$2,825,283
Credential thief (imposter risk)	$672,112	2.7	$1,814,702
			$8,303,737
FY 2020 CASE PROFILES			
Employee or contractor negligence	$317,111	14.9	$4,724,954
Criminal & malicious insider	$755,761	5.4	$4,081,109
Credential thief (imposter risk)	$871,686	3.2	$2,789,395
			$11,595,458
FY 2022 CASE PROFILES			
Employee or contractor negligence	$484,931	13.7	$6,643,555
Criminal & malicious insider	$648,062	6.4	$4,147,597
Credential thief (imposter risk)	$804,997	5.7	$4,588,483
			$15,378,635

US$ millions

COST ANALYSIS

THIS STUDY ADDRESSES THE CORE PROCESS-RELATED ACTIVITIES THAT DRIVE A RANGE OF EXPENDITURES AND COSTS ASSOCIATED WITH A COMPANY'S RESPONSE TO INSIDER-RELATED INCIDENTS.

The seven cost activity centers in our framework are defined as follows:[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.

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 multiyear investments in technologies.

TABLE 3.

Average trend in activity cost per incident for 7 activity centers.

Companies spend the most on containment of the insider security incident. As discussed, the average time to contain an incident has increased from 77 days to 85 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 reported, containment and investigation of the incident represent the most expensive activity centers. Least expensive are ex-post analysis and escalation. The activity costs have increased 80 percent since 2016.

ACTIVITY COST CENTERS	FY 2016	FY 2018	FY 2020	FY 2022
Monitoring & surveillance	$9,620	$12,634	$22,124	$35,080
Investigation	$41,461	$78,398	$103,798	$128,056
Escalation	$8,919	$12,542	$21,805	$32,228
Incident response	$66,371	$91,263	$118,317	$120,391
Containment	$122,796	$173,161	$211,553	$184,548
Ex-post analysis	$8,498	$11,491	$19,480	$26,563
Remediation	$91,397	$138,532	$147,776	$119,131
Overall	**$349,152**	**$517,921**	**$644,853**	**$645,997**

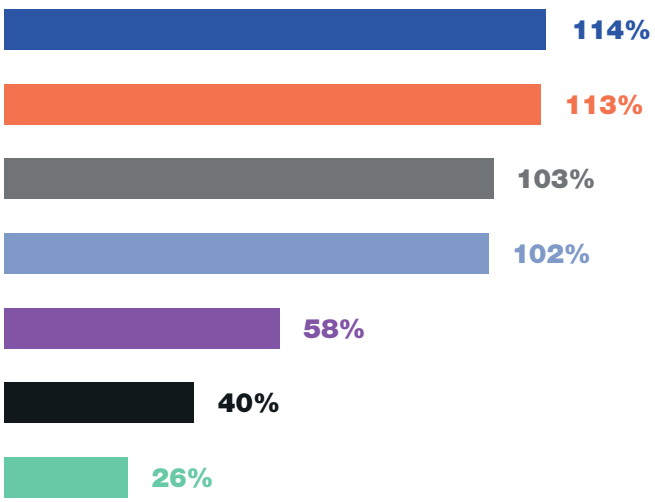


FIGURE 13.

Percentage net increase in average annual cost from FY 2016 to FY 2022

Since 2016, it has become far more costly to respond to an insider threat incident. As shown in Figure 13, monitoring and surveillance and escalation have increased the most since 2016, 114% and 113%, respectively. The average annual increase in activity costs is 80 percent since 2016.

TABLE 4.

2022 cost of seven activities by the type of incident

Containing the insider incident is most costly as a % of total cost for credential theft (imposter risk) and negligent insider incidents. Table 4 presents the average annualized cost for the seven activities according to the type of incident.

FY 2022 ACTIVITY COST CENTERS	EMPLOYEE OR CONTRACTOR NEGLIGENCE	CRIMINAL & MALICIOUS INSIDER	CREDENTIAL THIEF (IMPOSTER RISK)	AVERAGE COST
Monitoring & surveillance	$34,517	$34,511	$36,213	$35,080
Investigation	$121,511	$126,545	$136,111	$128,056
Escalation	$29,121	$31,112	$36,451	$32,228
Incident response	$112,345	$119,711	$129,118	$120,391
Containment	$151,311	$149,814	$252,518	$184,548
Ex-post analysis	$23,515	$26,733	$29,441	$26,563
Remediation	$12,611	$159,636	$185,145	$119,131
Total	**$484,931**	**$648,062**	**$804,997**	**$645,997**

FIGURE 14.

2022 average activity cost per incident for the three types of incidents

The average activity cost is highest for credential theft. Figure 14 demonstrates the significant difference in activity cost between employee or contractor negligence and credential theft.

US$

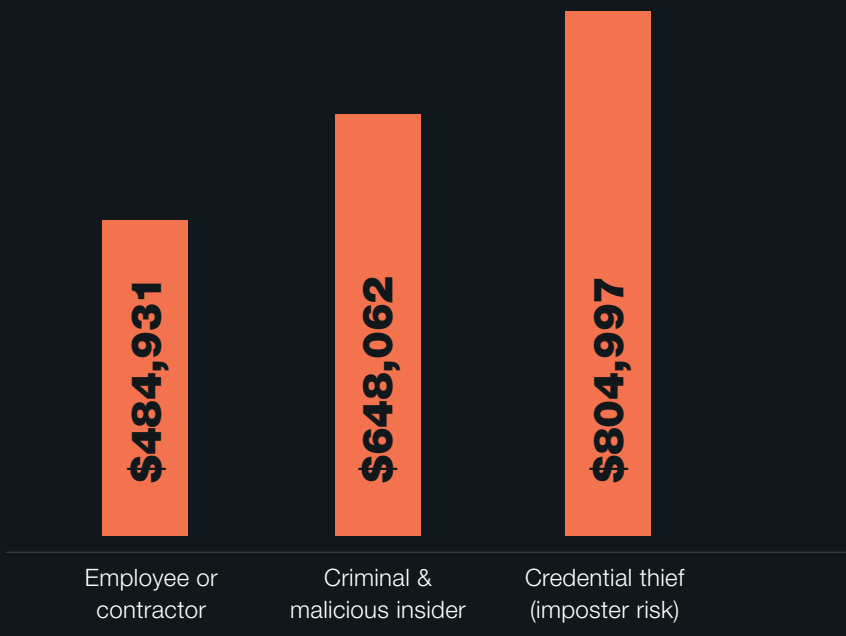


FIGURE 15.

Average activity cost by global region

NORTH AMERICAN COMPANIES ARE SPENDING MORE THAN THE AVERAGE COST ON ACTIVITIES THAT DEAL WITH INSIDER THREATS.

The total average cost of activities to resolve insider threats over a 12-month period is $15.4 million. As shown in Figure 15, companies in North America experienced the highest total cost at $17.53 million. European companies had the next highest cost at $15.44 million. Asia-Pacific had an average cost much lower than average total cost for all 278 companies at $11.90 million.

Mean = $15.38 (US$ Millions)

FIGURE 16.

Average activity cost by headcount

Larger organizations spend the most on the activities to resolve an insider threat incident. As shown in Figure 16, 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 $23.00 million.

Mean = $15.38 (US$ millions)

Consolidated for three profiles

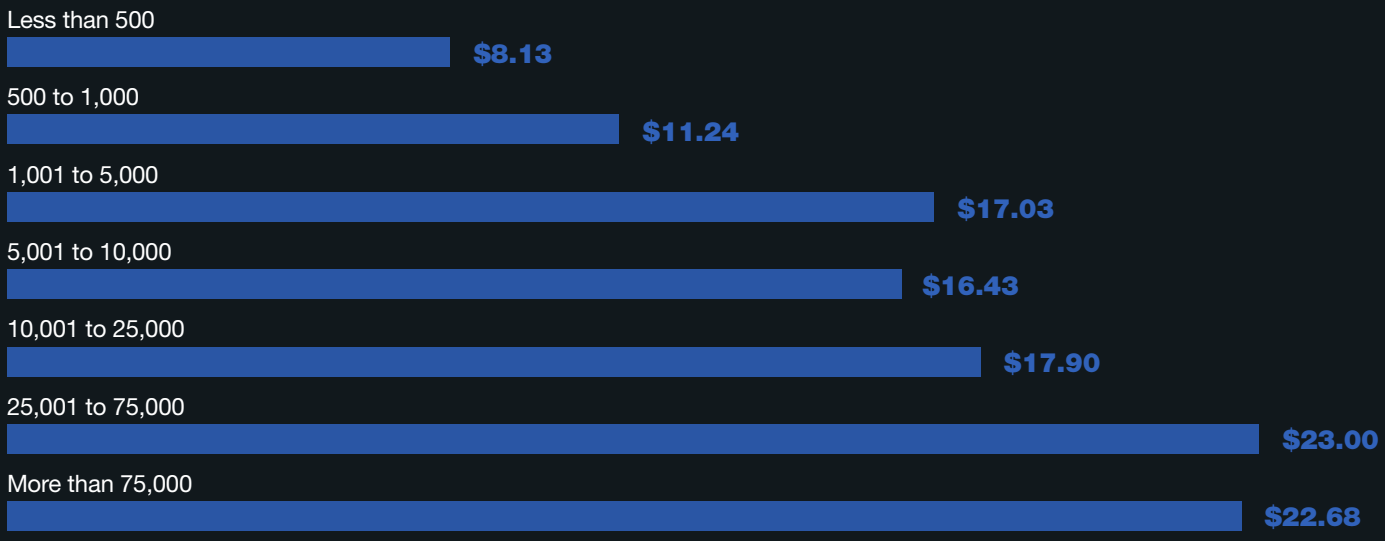


FIGURE 17.

Average activity cost by days to contain the incidents

The faster containment occurs, the lower the activity cost. Total annualized cost appears to be positively correlated with the time to contain insider-related incidents. As shown in Figure 17, incidents that took more than 90 days to contain had the highest average total cost per year ($17.19 million). In contrast, incidents that took less than 30 days to contain had the lowest total cost. ($11.23 million). The average annual cost is $15.38 million.

Mean = $15.38 (US$ millions)

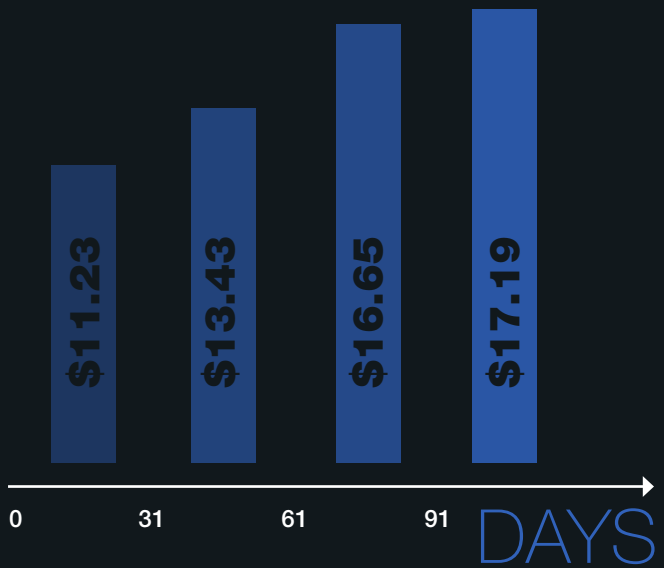


FIGURE 18.

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 18, containment represents 29 percent of total annualized insider-related activity costs. Activities relating to investigation and incident response represent 20 percent and 19 percent of total cost, respectively.

n = 278 companies

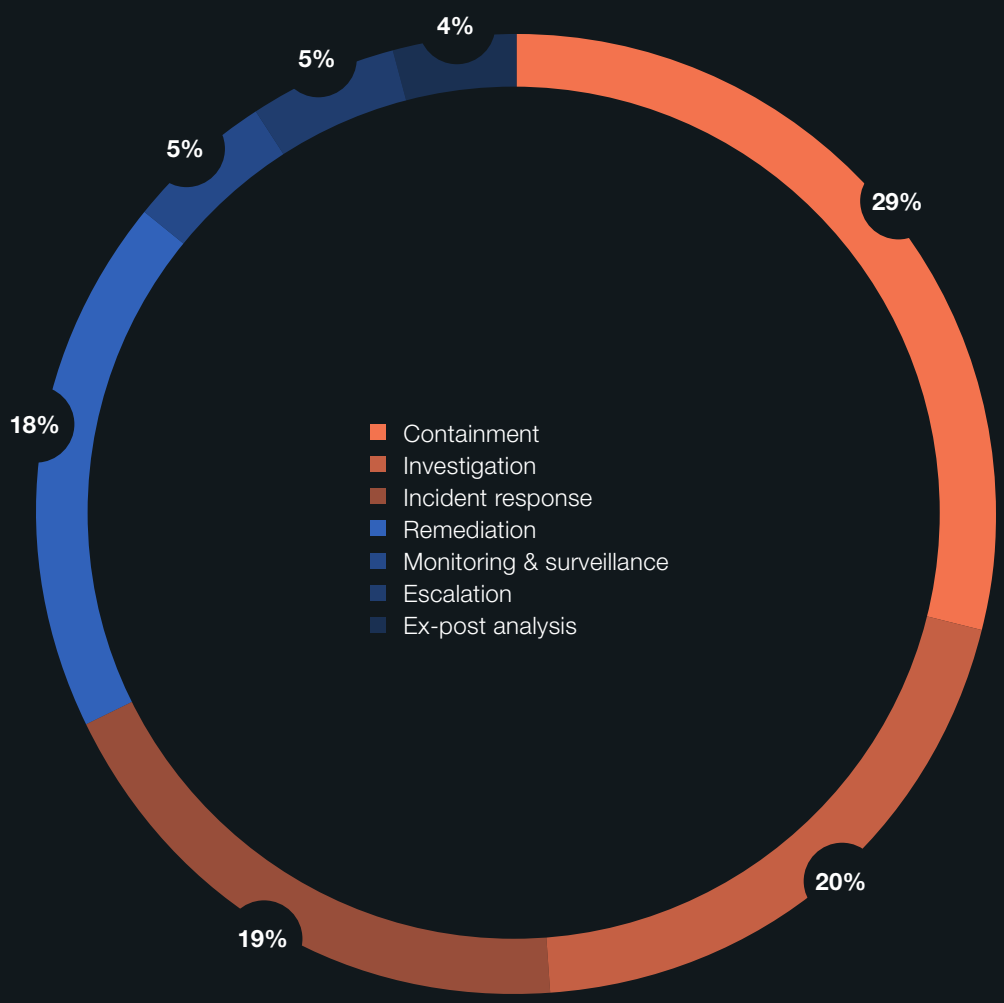


FIGURE 19.

Annualized activity cost by industry

ACTIVITY COSTS ARE HIGHER FOR FINANCIAL SERVICES AND SERVICES.

According to Figure 19, the average activity cost for financial services is $21.25 million and services is $18.65 million, much higher than the average of $15.4 million. Services includes such companies as law, consulting and accounting firms.

US$ millions

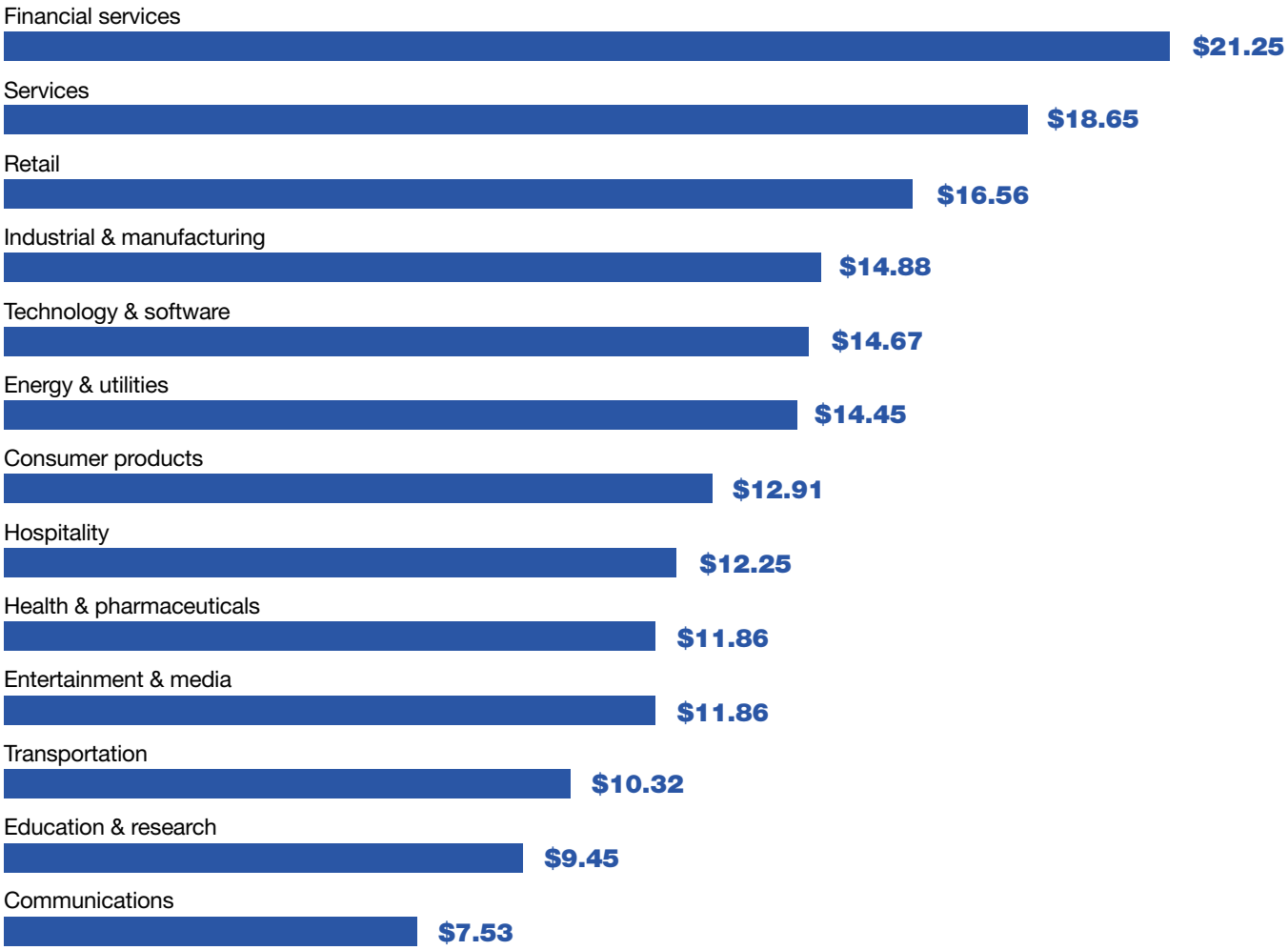
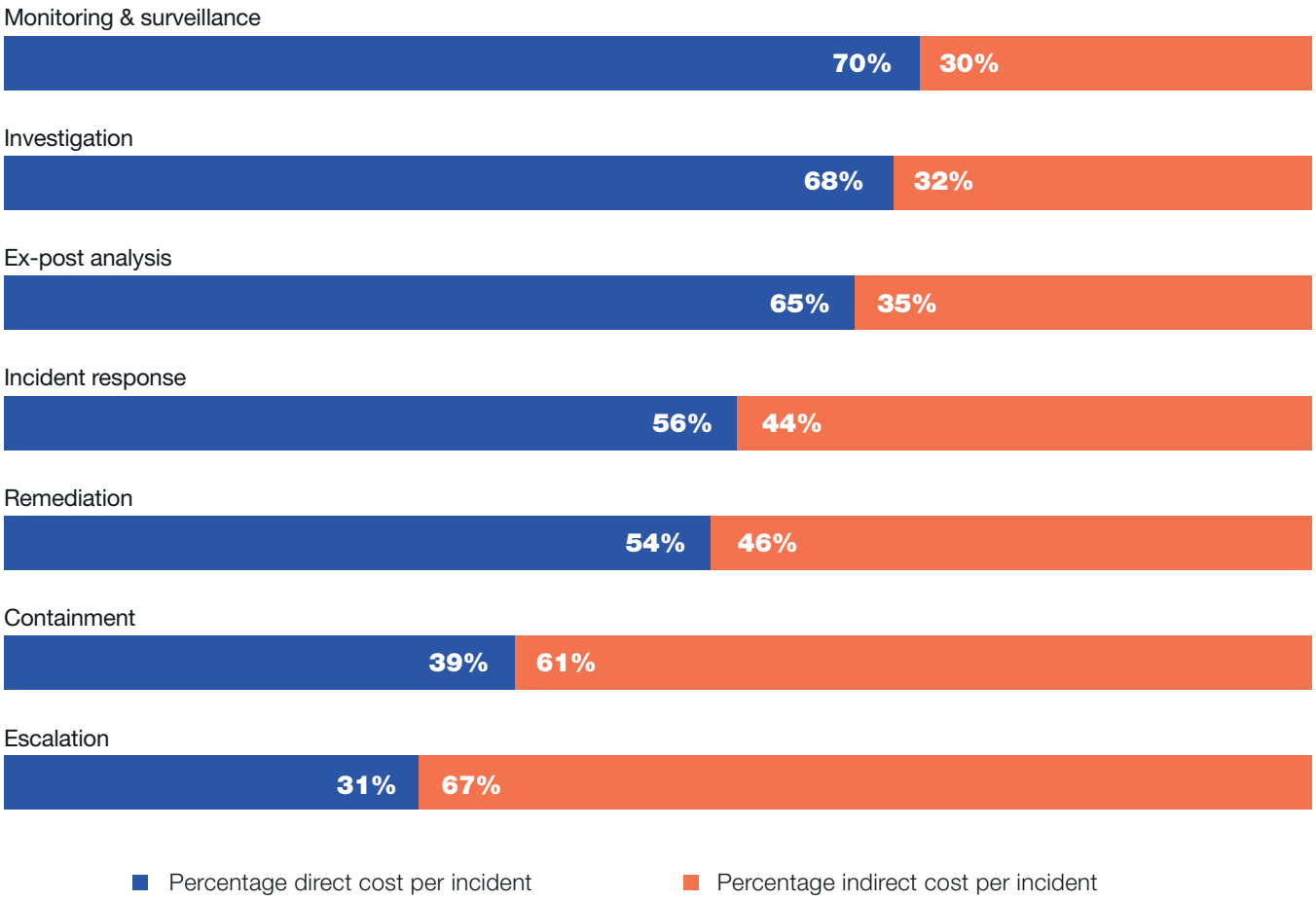


FIGURE 20.

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. Figure 20 shows the proportion of direct and indirect costs[3] for seven internal activity cost centers. As can be seen, the cost for monitoring and surveillance and investigation have the highest percentage of direct cost (70 percent and 68 percent, respectively). The highest percentage of indirect cost for activities are for containment (61 percent) and escalation (67 percent).

Consolidated for three profiles



3 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.

IN ADDITION TO DETERMINING THE COST OF INSIDER THREATS FOR COMPANIES IN THIS RESEARCH, WE INTERVIEWED PARTICIPANTS ABOUT THEIR EXPERIENCES WITH THE THREAT AND WHAT THEY ARE DOING TO REDUCE RISKS.

FIGURE 21.

Which insider incidents are you most concerned about?

Of all the types of insider threat in this research, organizations are most concerned about credential theft. As discussed previously, credential thefts have almost doubled since the last study and cost the most to remediate. Fifty-five percent of respondents say they are most concerned about a hacker stealing the valid credentials of an employee. Far fewer respondents (21 percent) are concerned about the negligent insider.

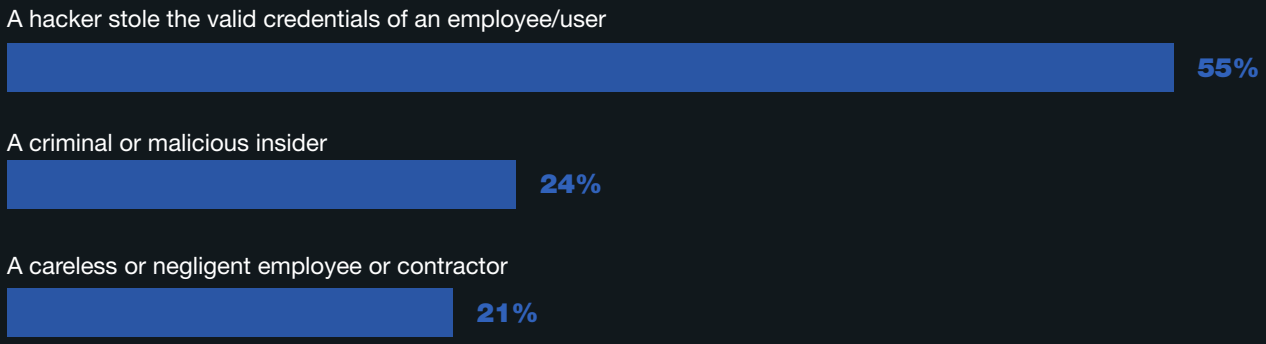


FIGURE 22.

Did any of the incidents involve the following?

Negligent employees and credential thieves are the root causes of most insider incidents. As shown in Figure 22, 57 percent of respondents say the insider incidents involved employee negligence and 51 percent say a malicious outsider stole data by compromising insider credentials or accounts.

More than one response permitted

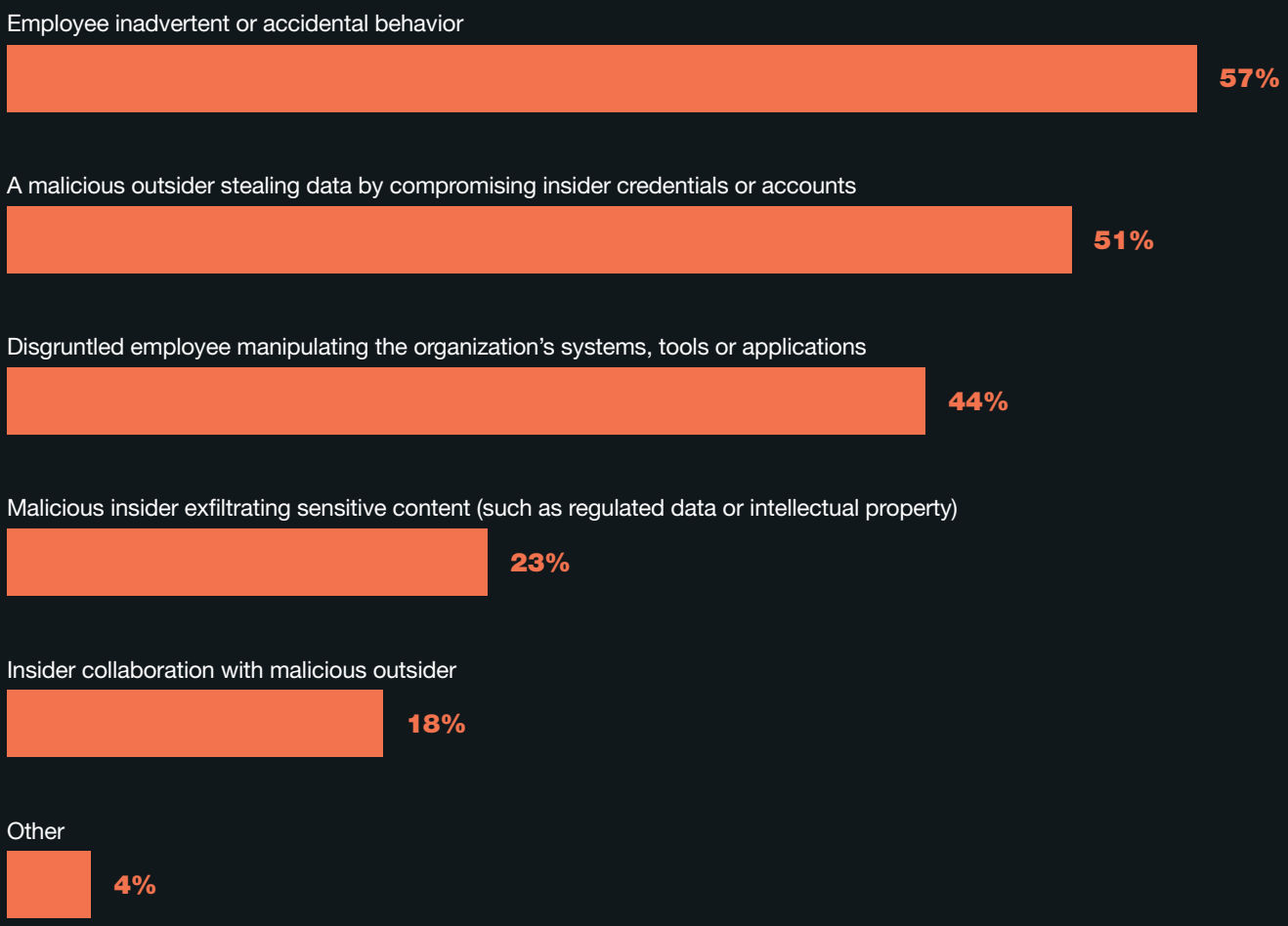


FIGURE 23.

Which channels of insider-driven data loss are you most worried about?

Vulnerable IoT devices are of greatest risk to data loss. The plethora of IoT devices in organizations is increasing insider risk. Sixty-three percent of respondents say they are worried about unmanaged IoT devices resulting in the loss of sensitive data. This is followed by the cloud (52 percent of respondents) and network (51 percent of respondents) as shown in Figure 23.

More than one response permitted

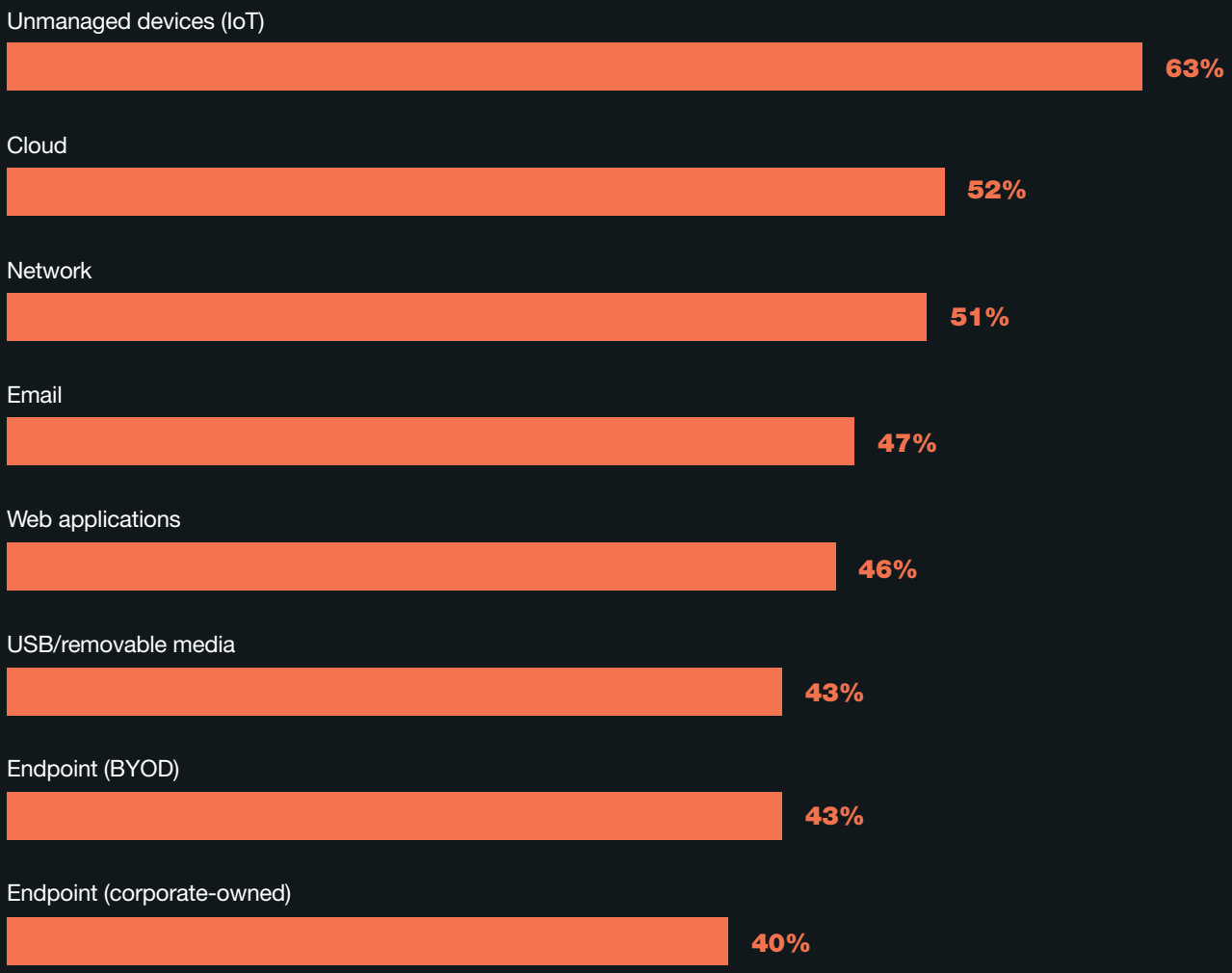


FIGURE 24.

Where do your users store your organization's sensitive data, such as PII, IP and other critical business information?

Most sensitive data is in employees' email. According to Figure 24, 65 percent of respondents email is where employees store their organizations most sensitive data such as personally identifiable information (PII), intellectual property (IP) and other critical business information. Training and awareness programs are critical to reducing employees' negligence in how they are sending and receiving sensitive information.

Three responses permitted

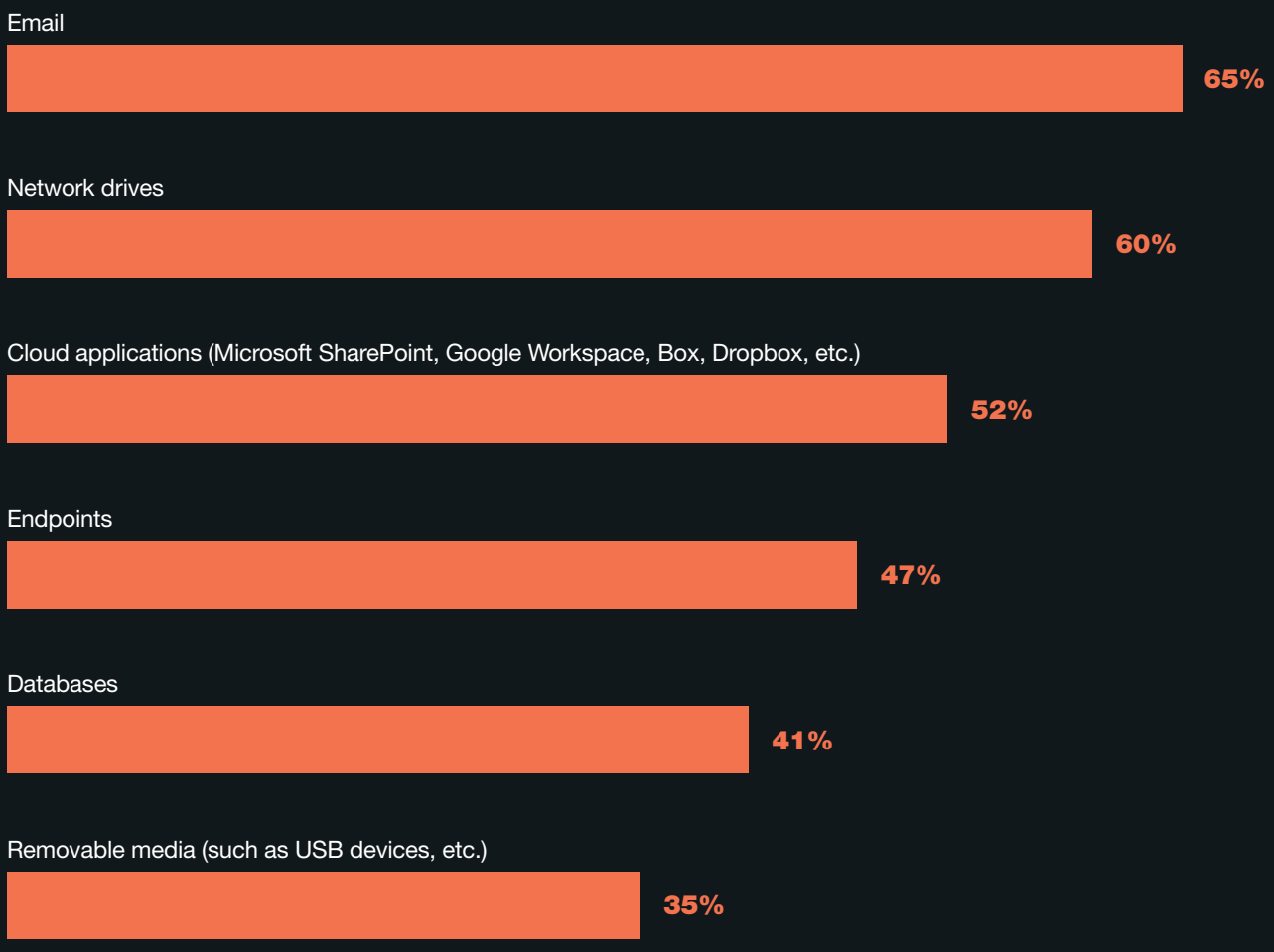


FIGURE 25.

How do your users communicate and collaborate with colleagues and third parties?

As shown in Figure 25, business chat tools and email are the top methods used to communicate and collaborate internally and with third parties according to 61 percent and 52 percent of respondents.

Three responses permitted

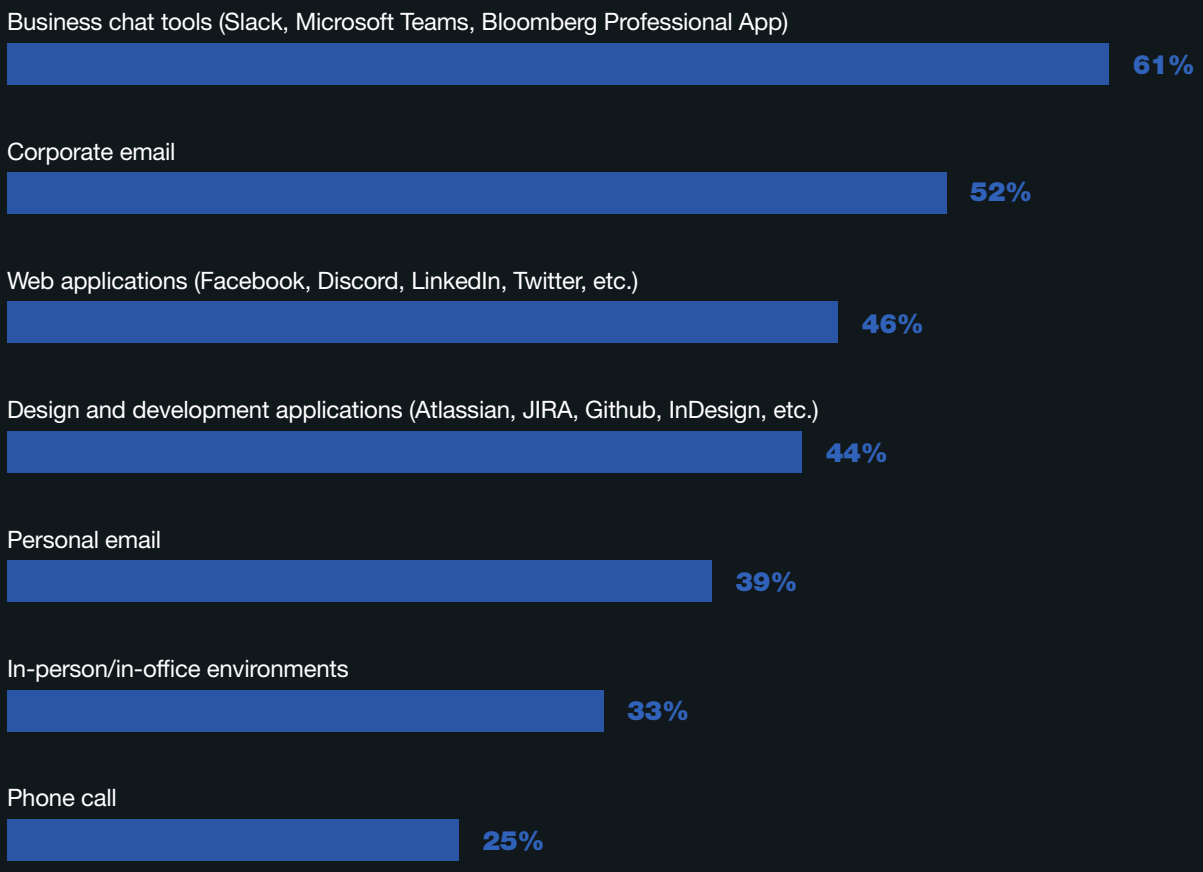


FIGURE 26.

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

Malicious insiders use corporate email to steal sensitive data. Figure 26 presents a list of malicious insiders' activities in organizations represented in this research. Seventy-four percent of respondents say malicious insiders emailed sensitive data to outside parties followed by scanning for open ports and vulnerabilities (62 percent of respondents) and accessing sensitive data not associated with the role or function (60 percent of respondents).

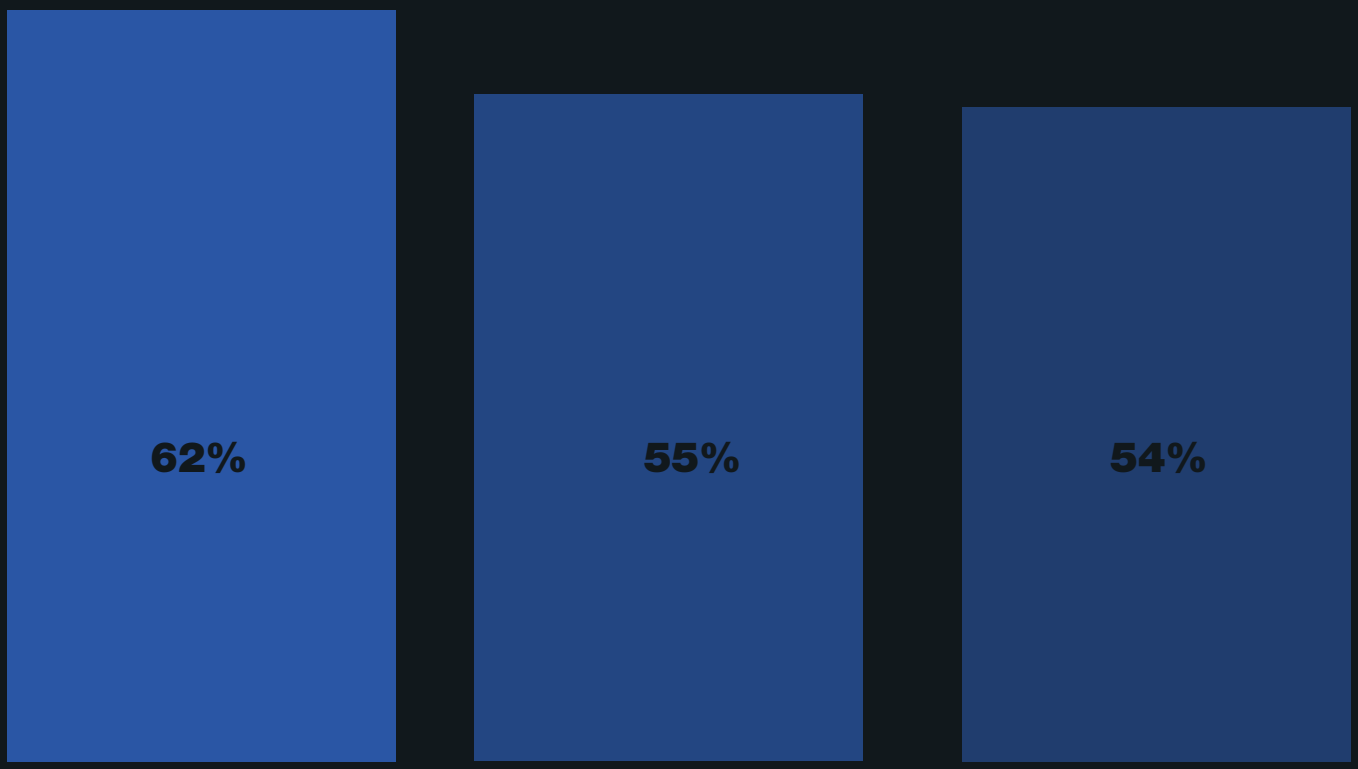
More than one response permitted

FIGURE 27.

How important are advanced technologies in reducing insider threats?

As more insider incidents occur and the time to contain increases, advanced technologies are important to reducing insider threats. According to Figure 27, user behavior-based tools to detect insider threat are considered essential or very important to reducing insider threats (62 percent of respondents). This is followed by automation for the prevention, investigation, escalation and containment and remediation of insider incidents (55 percent of respondents) and AI and machine learning to prevent, investigate, escalate, contain and remediate insider incidents (54 percent of respondents).

Essential and Very important responses combined



User behavior-based tools to detect insider threats

Automation for the prevention, investigation, escalation and containment and remediation of insider incidents

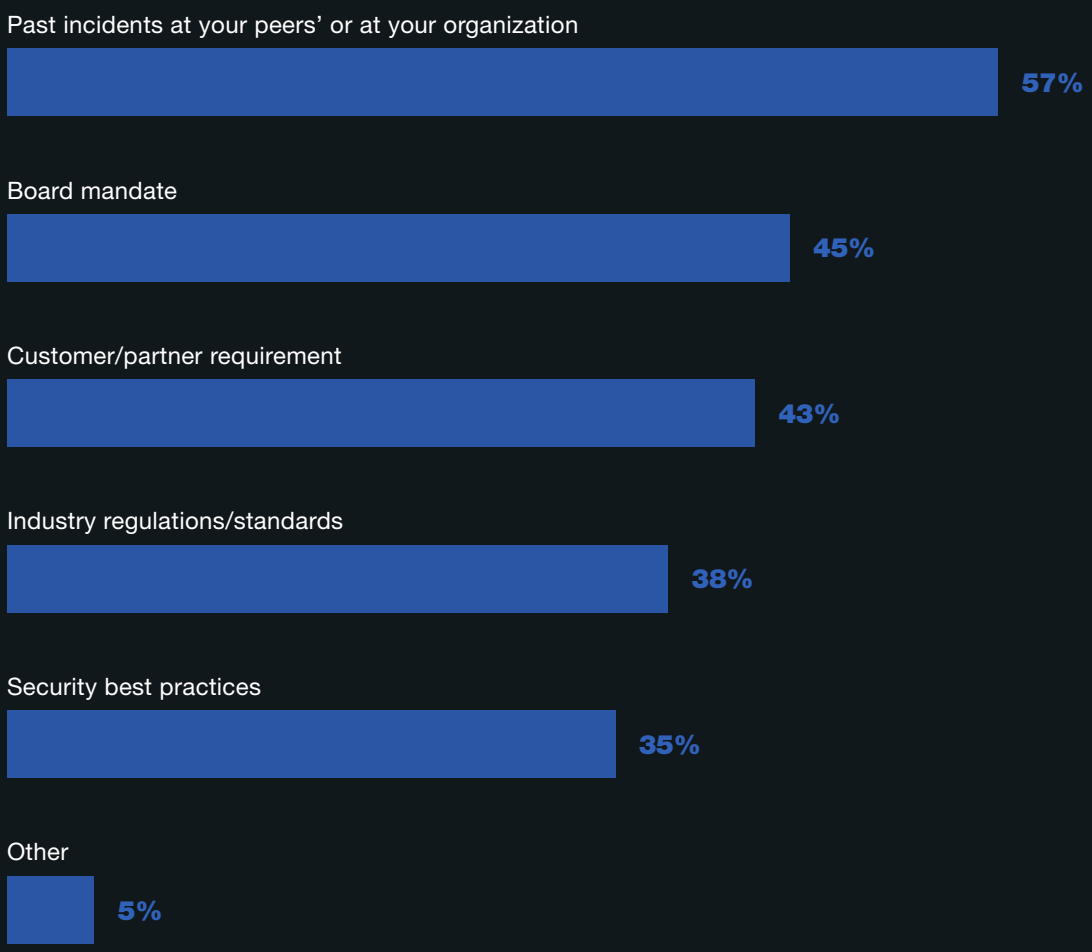
AI and machine learning to prevent, investigate, escalate, contain and remediate insider incidents

FIGURE 28.

What was the primary business driver behind your insider threat management program?

Past incidents motivate organizations to adopt an insider threat management program. Figure 28 presents reasons why organizations represented in this research are making efforts to mitigate insider threats. The primary reason (57 percent) is past incidents directed at other companies and their organization. Only 38 percent of respondents say industry regulations and standards are drivers to have an insider threat management program.

More than one response permitted



CONCLUSIONS

The rapid digital transformation over the past two years unintentionally set the stage for insider threats to grow.

From the use of personal devices to increased use of the cloud, organizations are recognizing the traditional approach to securing data just won't cut it.

This illustrates the importance for organizations to implement a people-centric Insider Threat Management (ITM) program, one that is designed for today's modern work-from-anywhere world. An effective ITM program is built with cross-team collaboration, including IT, HR, compliance and legal, to name a few. Having both technical and non-technical representatives on the team ensures the organization can achieve the three successful elements of an ITM program:

Visibility

Implement an ITM platform that provides your organization with the visibility and context into data movement. Doing so grants you the opportunity to accelerate both your mean time to detect (MTTD) and your mean time to respond (MTTR). With a better understanding of why data is moving a certain way, you can effectively reduce the average number of days it takes to contain an insider threat incident.

Consistency

Evaluate the organization's risk, including any high-risk insiders, and develop a dedicated insider threat function within the organization. Part of this process should also include establishing a consistent and repeatable process to detect and respond to relevant insider threat alerts based on context. Leveraging a purpose-built insider risk solution ensures there is a consistent process in place to reduce the MTTD and MTTR.

Transparency

Understanding what could work better next time requires an element of continuous improvement. Being open to lessons learned can enhance an organization's efforts to evolve with the changing risk environment more effectively.

As more insider incidents occur and the time to contain them increases, advanced technologies are important to reducing insider threats. Establishing an ITM program that empowers your organization to confidently identify and detect risky user behavior and data interaction, and respond to the incident, is key when it comes to preventing data loss and mitigating insider risk.

FRAMEWORK

THE PURPOSE OF THIS RESEARCH IS TO PROVIDE GUIDANCE ON WHAT AN INSIDER THREAT 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 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 threats 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 threat 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.[4]

4 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:[5]

07

internal cost activity centers

01 **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.

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

03 **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.

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

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

06 **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.

07 **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:

04

general cost activities

01 **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.

02 **Cost of business disruption:** The economic impact of downtime or unplanned outages that prevent the organization from meeting its data processing requirements.

03 **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.

04 **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.

5 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.

Field research was launched in September 2021. To maintain consistency for all benchmark companies, information was 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 this past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to this 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.

proofpoint.

About Proofpoint

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. Proofpoint.com