IBM Security

Cost of Insider Threats: Global Report 2020

Independently conducted by

Ponemon Institute

Sponsored by

observe it IBM

Table of Contents

Introduction	3
About the study	7
Benchmarked sample	9
Analysis of the incidents	13
Cost analysis	21
Framework	36
Benchmarking	39
Limitations	40
Next steps	41

Introduction

Ponemon Institute is pleased to present the findings of the 2020 Cost of Insider Threats: Global study. Sponsored by ObserveIT and IBM, this is the third benchmark study conducted to understand the direct and indirect costs that result from insider threats. The first study was conducted in 2016 and focused exclusively on companies in the United States. Represented in this study are companies located in North America, Europe, the Middle East and the Asia-Pacific region.

In the context of this research, insider threats occur because of the following:

— A negligent or inadvertent employee or contractor,

— A criminal or malicious insider or

— A credential thief.

The key takeaway is that the costliest insider threat per incident is theft of credentials. These incidents have increased significantly in frequency and cost. In fact, the frequency of incidents per company has tripled since 2016 from an average of 1 to 3.2 and the average cost has increased from USD $493,093 to USD $871,686 in 2019. On an annual basis, organizations are spending more to deal with insider negligence but the per incident cost is much lower.

We interviewed 964 IT and IT security practitioners in 204 organizations in North America (United States and Canada), Europe, Middle East & Africa and Asia-Pacific. Interviews were completed in September 2019.

204
organizations

964
individuals

Each organization experienced one or more material events caused by an insider. These organizations experienced a total of 4,716 insider incidents over the past 12 months. Our targeted organizations were business organizations with a global headcount of 1,000 or more employees.

Cost of an insider breach highlights

Global Average

The average cost for theft of credentials

from $493,093 to $871,686

in 2019

Frequency

The frequency of incidents per company has tripled

from 1 to 3.2

since 2016

Remediation of each incident of credential theft is the most costly

The cost of insider threat varies significantly based on the type of incident.

If it involves a negligent employee or contractor, each incident can average

$307,111

The average cost almost triples if the incident involves an imposter or thief who steals credentials

$871,686

The costliest type of credential theft involves the theft of privileged users' credentials.

Criminal and malicious insiders cost the organizations represented in this research an average of

$756,760 per incident

The activities that drive costs are: monitoring & surveillance, investigation, escalation, incident response, containment, ex-post analysis and remediation.

The negligent insider is the root cause of most incidents

Most incidents in this research were caused by insider negligence.

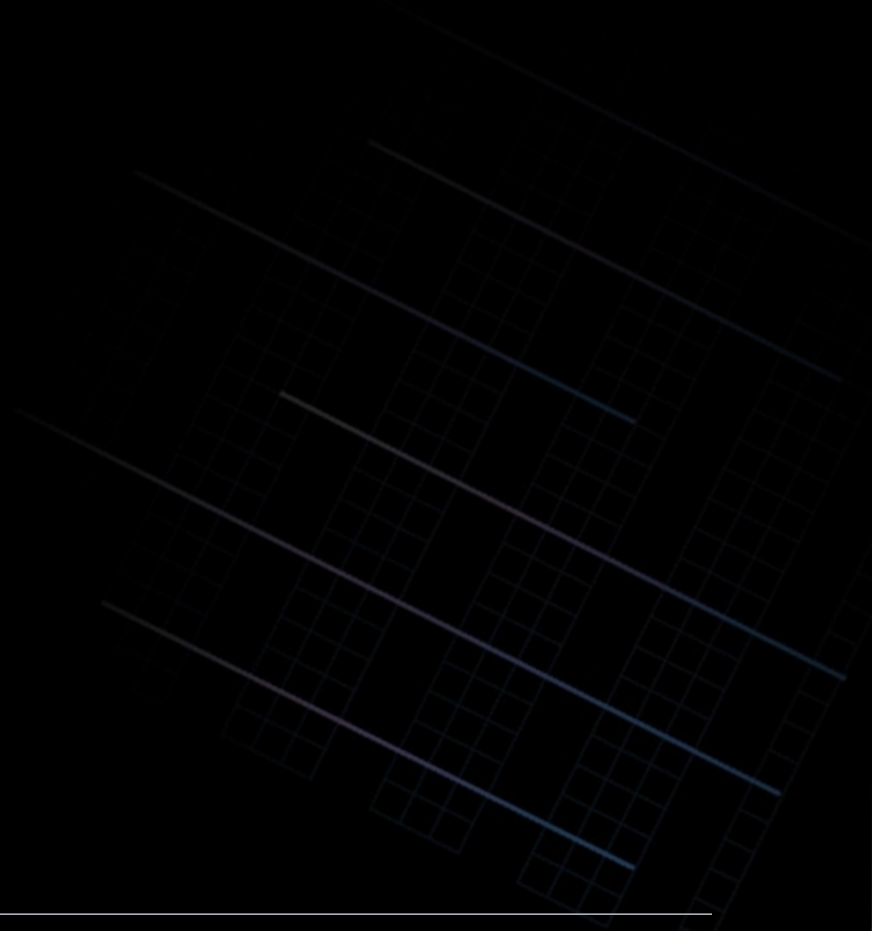
Specifically, of the 4,716 incidents reported

2,962 were due to negligent or inadvertent employees or contractors

1,105 were caused by criminal and malicious insiders

649 involved stolen credentials

191 involved the theft of privileged users' credentials



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

204
Total number of benchmarked organizations

14%
Incidents relating to user credential theft

4,716
Total number of insider incidents

$4.58M
Annualized cost for negligence

$11.45M
Total average cost

$4.08M
Annualized cost for criminal insiders

63%
Incidents relating to negligence

$2.79M
Annualized cost for credential theft

23%
Incidents relating to criminal insiders

Organizational size and industry affect the cost per incident

The cost of incidents varies according to organizational size. To deal with the consequences of an insider incident, smaller-sized organizations with a headcount below 500 spent an average of USD $7.68 million. Companies in financial services, services and technology and software incurred average costs of USD $14.05 million, USD $12.31 million and USD $12.30 million, respectively.

$17.92M

Large organizations with a headcount of more than 75,000 spent an average of USD $17.92 million over the past year to resolve insider-related incidents.

All types of insider risk threats are increasing

Since 2016 the average number of incidents involving employee or contractor negligence has increased from 10.5 to 14.5. The average number of credential theft incidents has tripled over the past two years, from 1.0 to 3.2. Sixty percent of organizations had more than 20 incidents per year.

60%

Sixty percent of organizations had more than 20 incidents per year.

On an annual basis, employee or contractor negligence incidents cost companies the most

In terms of total annual costs, employee or contractor negligence represents the most expensive insider profile.

On a per incident basis, credential theft is the most expensive

Each incident costs USD $871,686 to remediate.

29%

Twenty-nine percent of all credential thefts involve the theft of privileged users' credentials.

It takes an average of more than two months to contain an insider incident

Only 13 percent of incidents were contained in less than 30 days.

77 days

It took an average of 77 days to contain an incident.

About the study

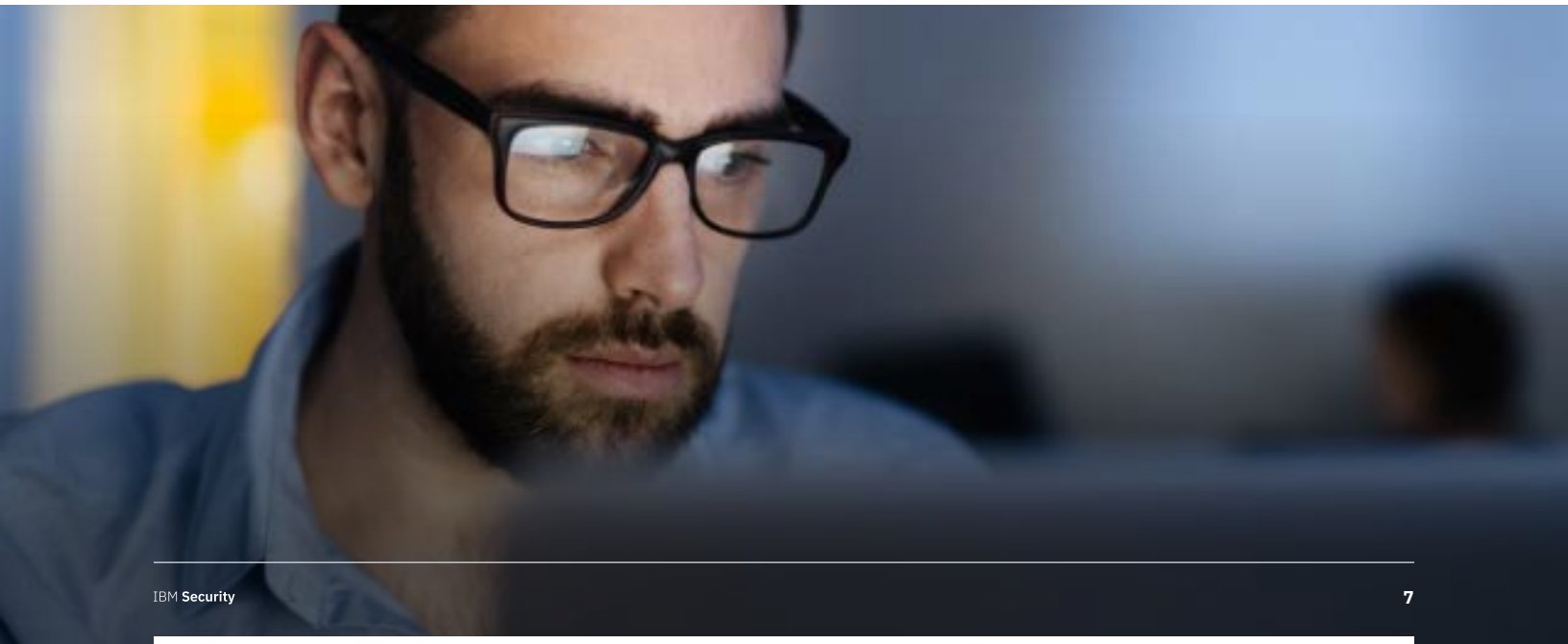
Our research focuses on actual insider-related events or incidents that impact organizational costs over the past 12 months.

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
- Deterioration 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 2019. Our final benchmark sample consisted of 204 separate organizations. A total of 964 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 & Africa and Asia-Pacific
- Central IT function with control over on-premise and/or cloud environmentbusiness processes
- Experienced one or more material incidents caused by careless, malicious or criminal insiders



About the study

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 204 organizations:

- Negligent or inadvertent 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:

- Working sessions with ObserveIT and IBM 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

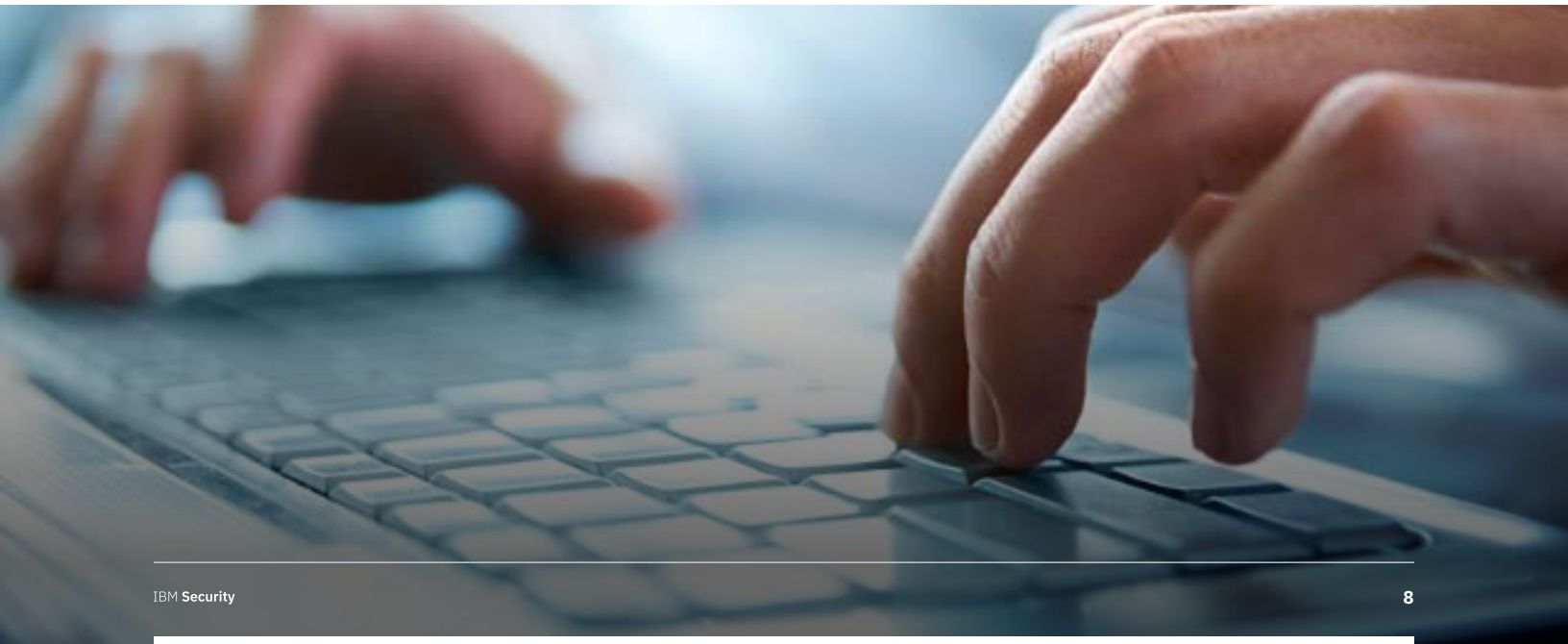


Figure 1:

Industry sectors of participating organizations

n = 204 companies

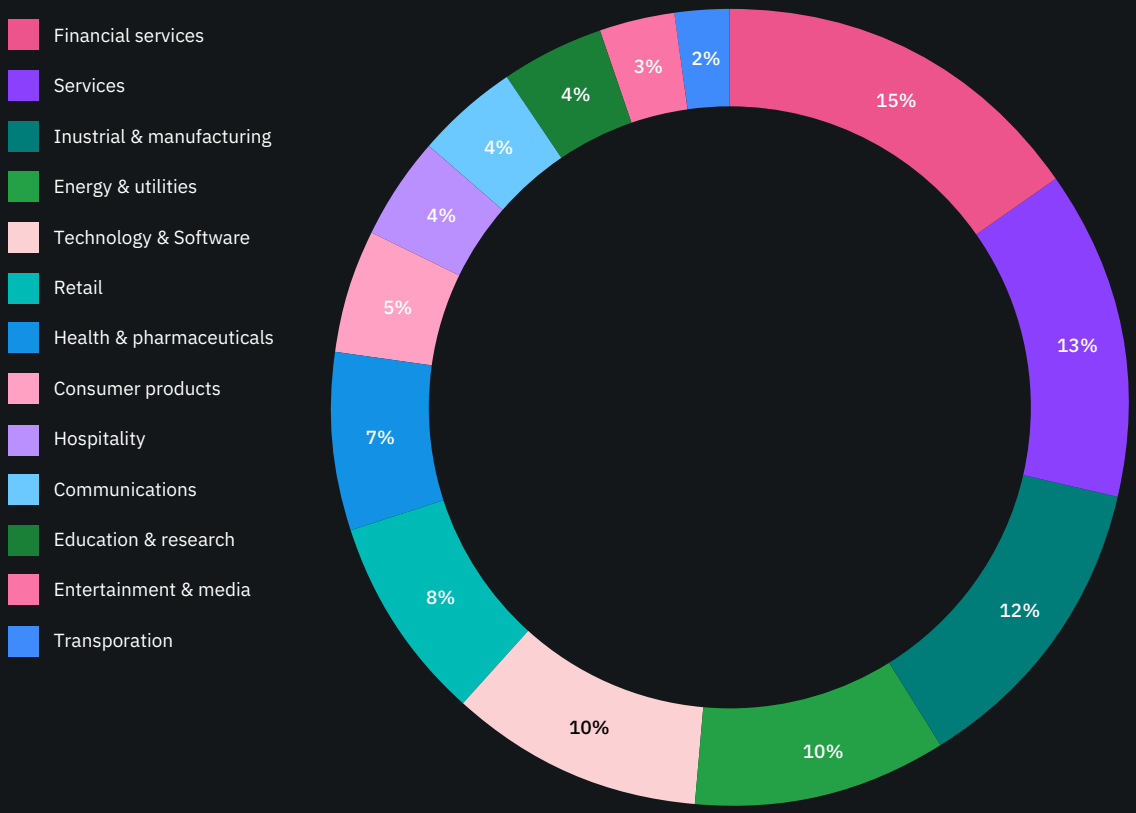


Figure 1 In benchmark research, the unit of analysis is the organization. The above pie chart shows the percentage distribution of companies across 13 industry segments. The three largest segments are financial services, services and industrial & manufacturing. Financial service organizations include banking, insurance, investment management and brokerage. Service organizations represent a wide range of companies, including professional service firms.

Figure 2:

Headcount (size) for participating organizations

n = 204 companies

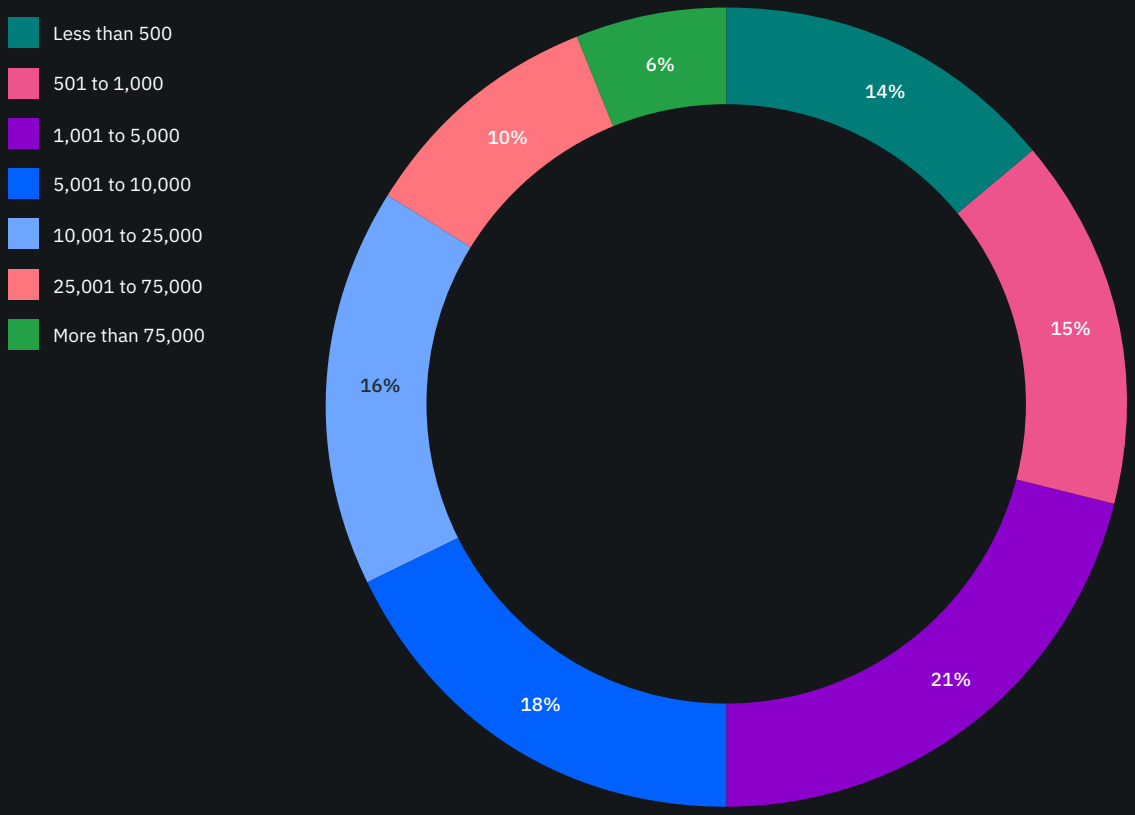


Figure 2 shows the percentage distribution of companies according to global headcount, which is a surrogate for organizational size. As can be seen, 50 percent of the sample includes larger-sized companies with more than 5,000 full-time equivalent employees.

Figure 3:

Interviewees by position level or function

n = 964 respondents

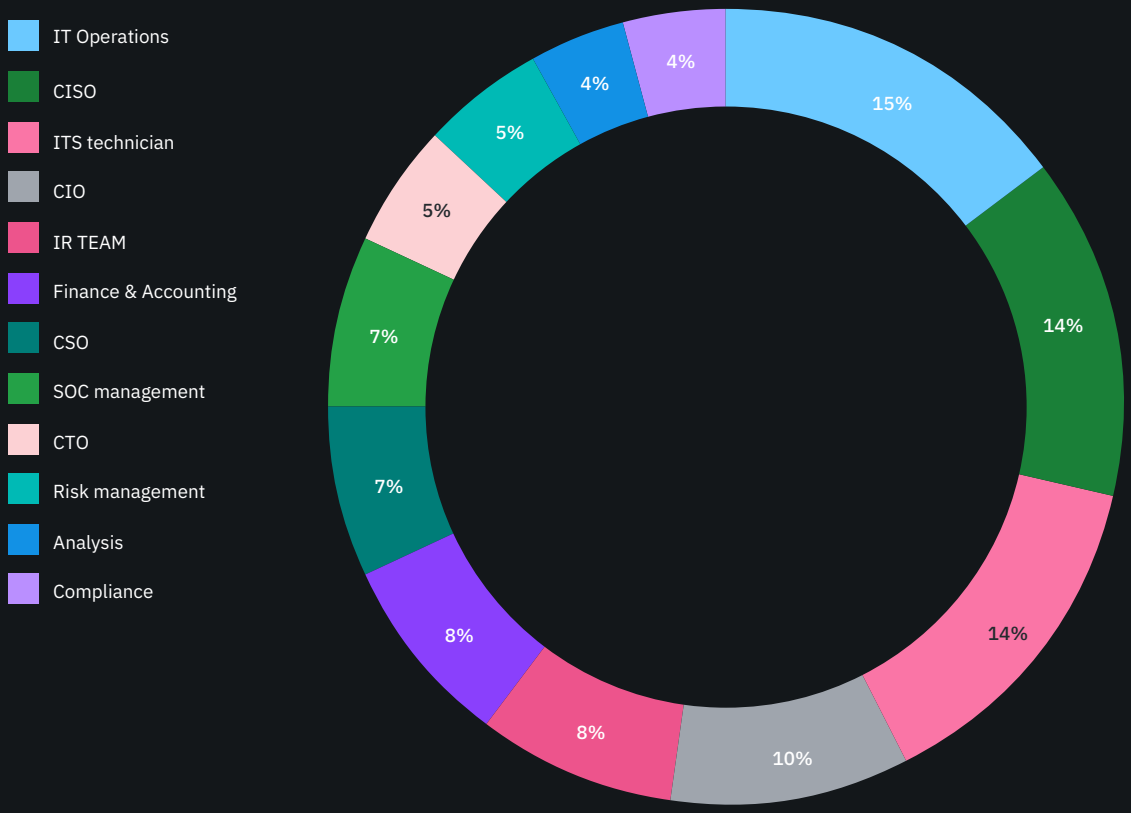


Figure 3 According to Figure 3, 964 individuals participated in field-based interviews. Each case study involved an average of 4.7 individuals. The three largest segments include: IT operations (15 percent), CISOs (14 percent) and IT technicians (14 percent).

Figure 4:

Regional distribution of global organizations

n = 204 companies

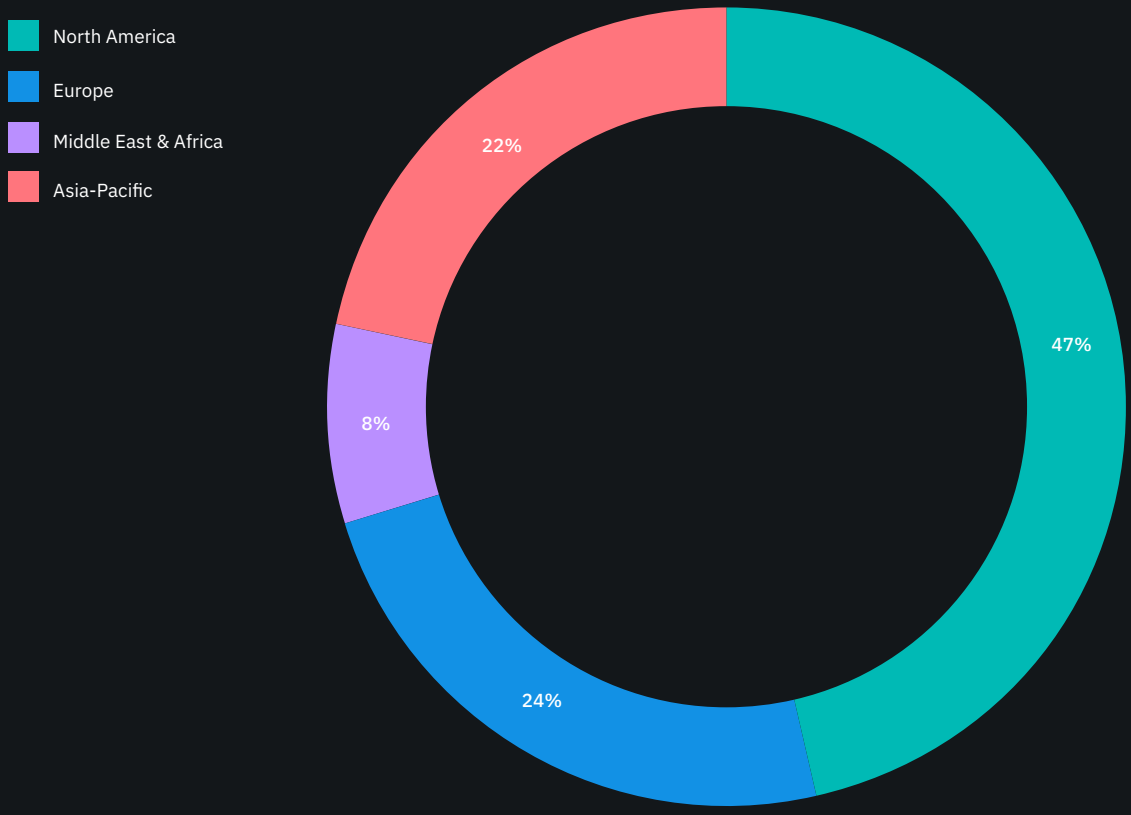


Figure 4 shows the global regions participating in this research. North America represents the largest segment (47 percent of companies) and the Middle East is the smallest segment (8 percent of companies). Because of small sample size, we combined Europe and the Middle East to form the EMEA segment.

Figure 5:

Frequency of 4,716 incidents for three insider profiles

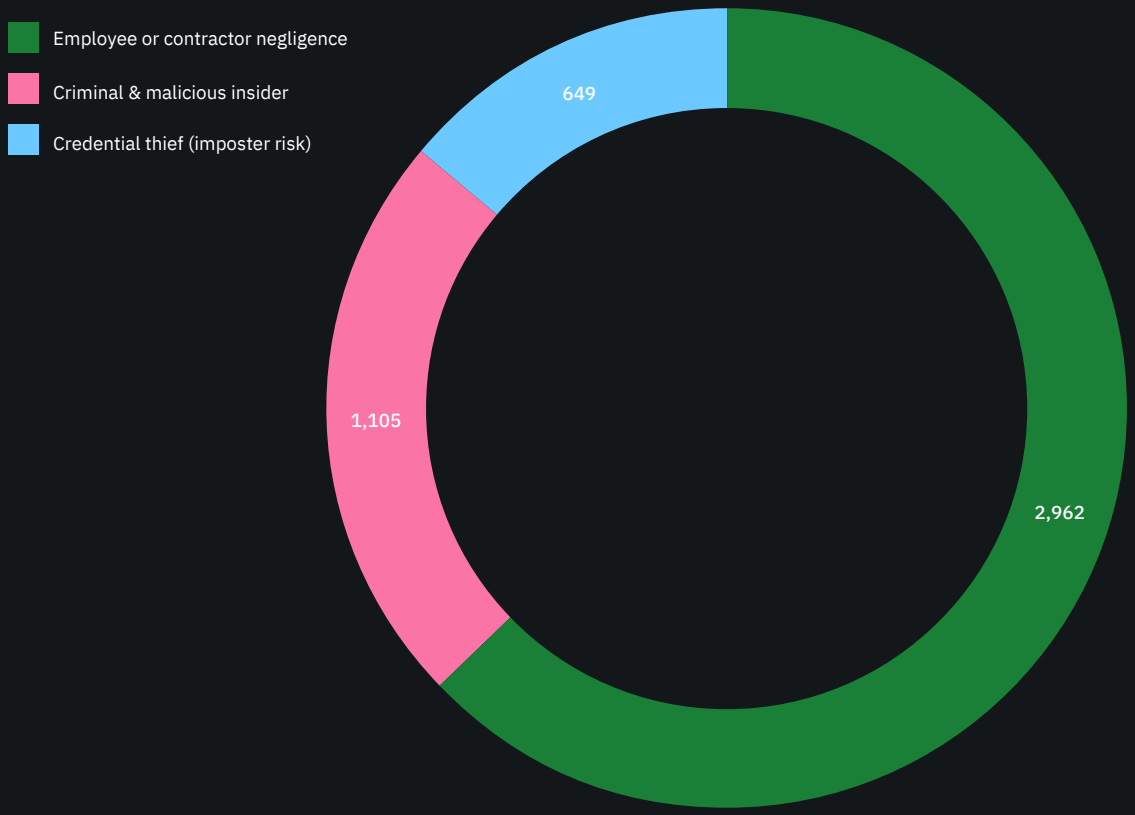


Figure 5 shows the distribution of 4,716 reported attacks analyzed in our sample. A total of 2,962 attacks (or 63 percent) pertained to employee or contractor negligence. Criminal or malicious insiders caused another 1,105 attacks (or 23 percent).

There were 649 attacks (or 14 percent) that involved credential theft (a.k.a. imposter risk). Of these, 191 involved privileged user credential theft. The largest number of reported incidents for a given company is 45 and the smallest number of incidents is one per participating company.

Figure 6:

Percentage frequency of insider-related incidents per company

Consolidated for three profiles

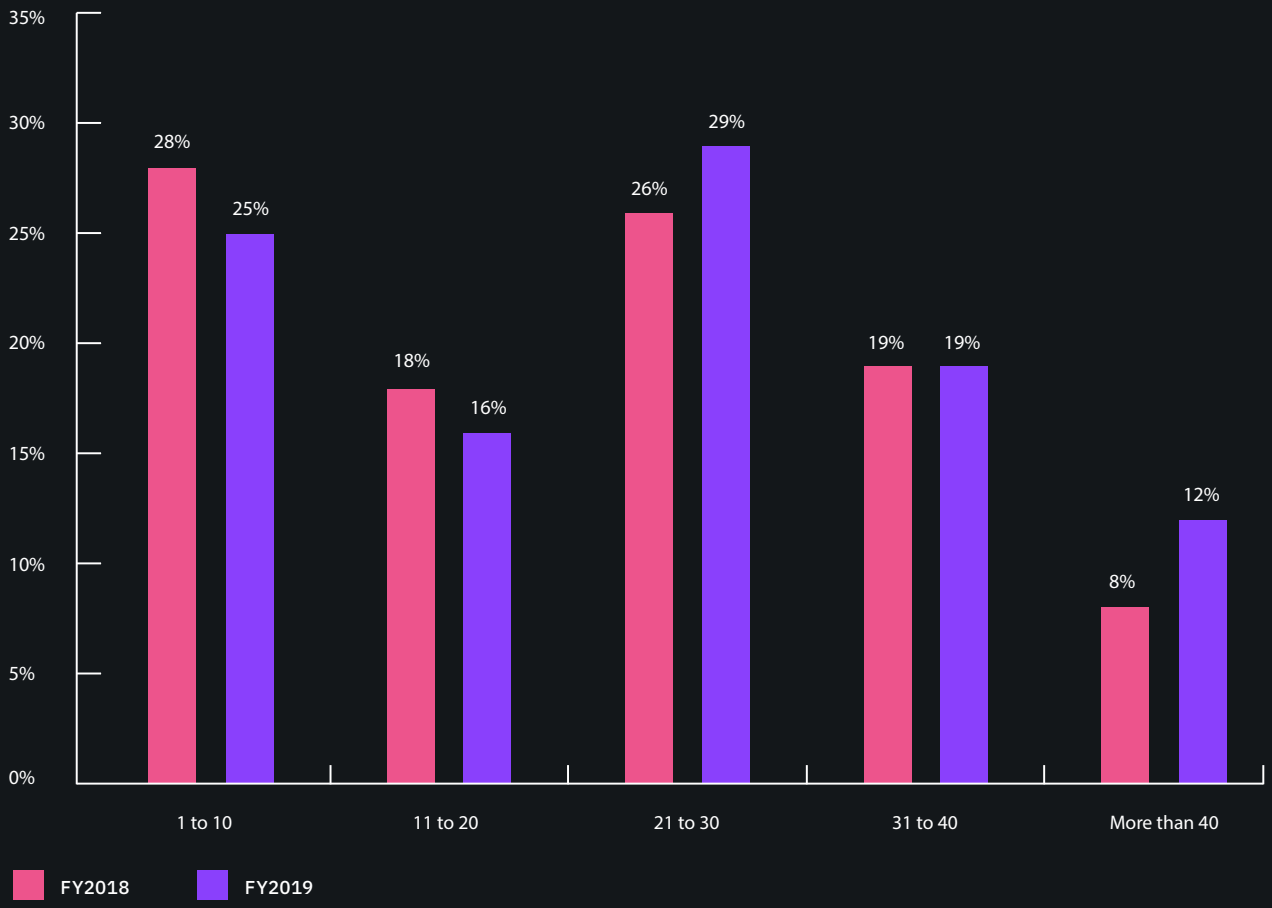


Figure 6 provides a graph that shows a histogram of insider incidents for our sample of 204 companies over the past 12 months. As shown, 60 percent of companies experienced an average of more than 20 incidents per year.

Figure 7:

Frequency for three profiles of insider incidents

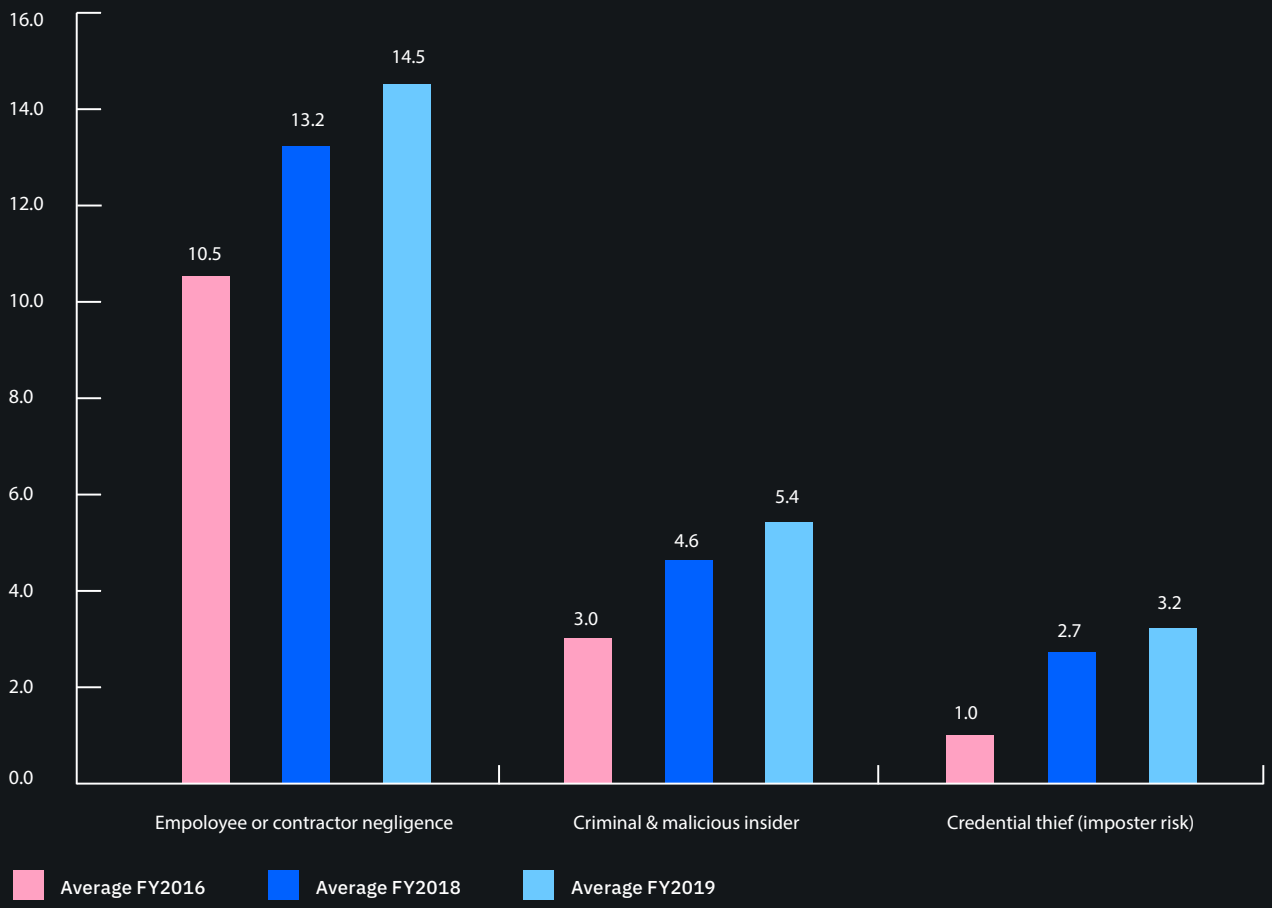


Figure 7 All types of insider threats are steadily increasing. As shown in Figure 7, since 2016 the average number of incidents involving employee or contractor negligence has increased from 10.5 to 14.5 in 2019. The average number of credential theft incidents per company have tripled over the past three years, from 1.0 to 3.2.[1]

The 2016 data only pertains to US companies. The 2019 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 8:

Average incident frequency for three profiles

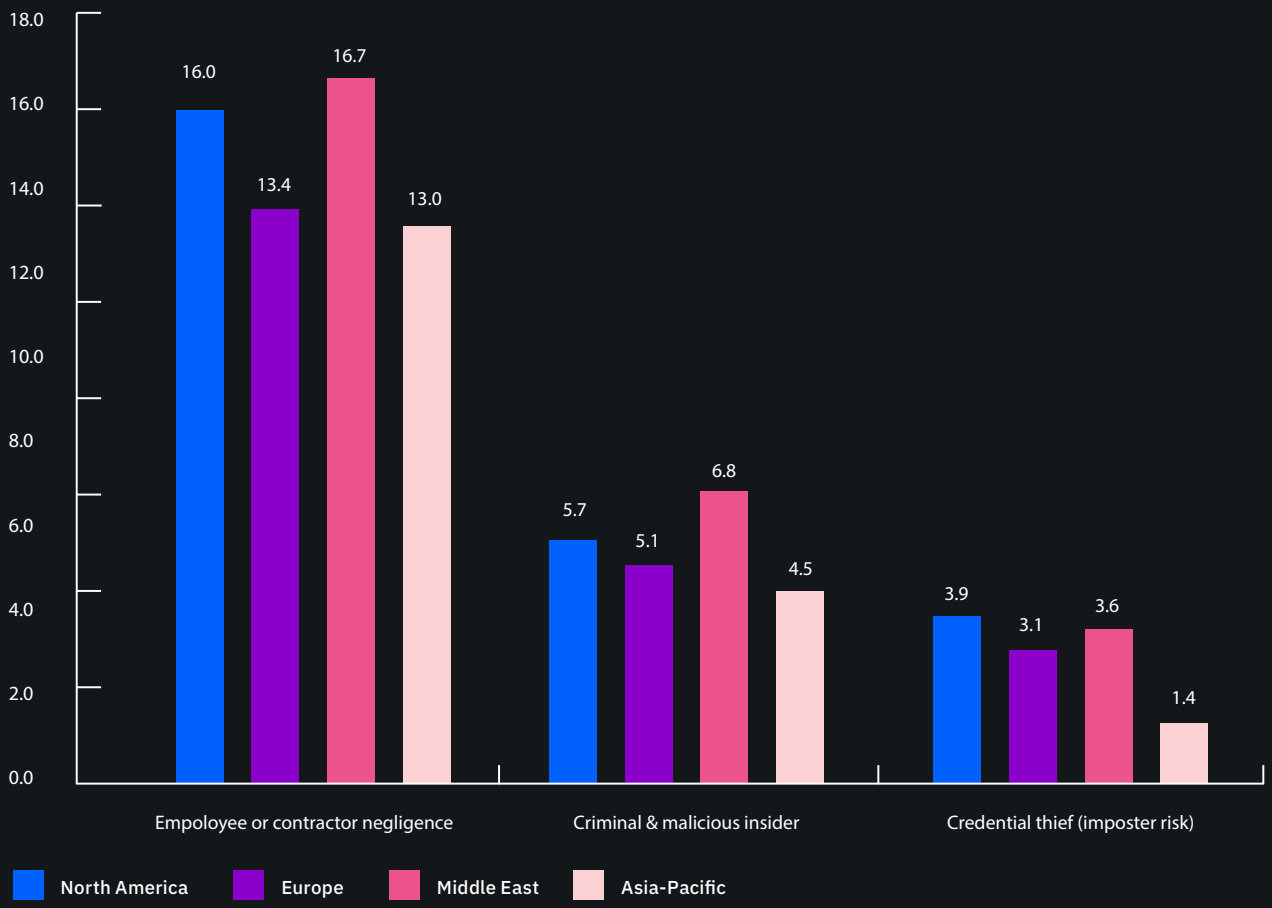


Figure 8 Companies in the Middle East experiences the most insider incidents and Asia-Pacific had the least incidents. Figure 8 presents the frequency of insider incidents in the four regions represented in the research. In all regions, employee or contractor negligence occur most frequently. North America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

Figure 9:

Frequency for three profiles of insider incidents by global region

Figure 9 The frequency of insider threats varies across global regions. As shown in Figure 9, North American and Middle Eastern companies experienced the highest number of insider-related incidents over the past 12 months. In contrast, APAC companies had the lowest number of insider-related incidents.

Figure 10:

Average activity cost by global region

Mean = $11.45 (US$ millions)

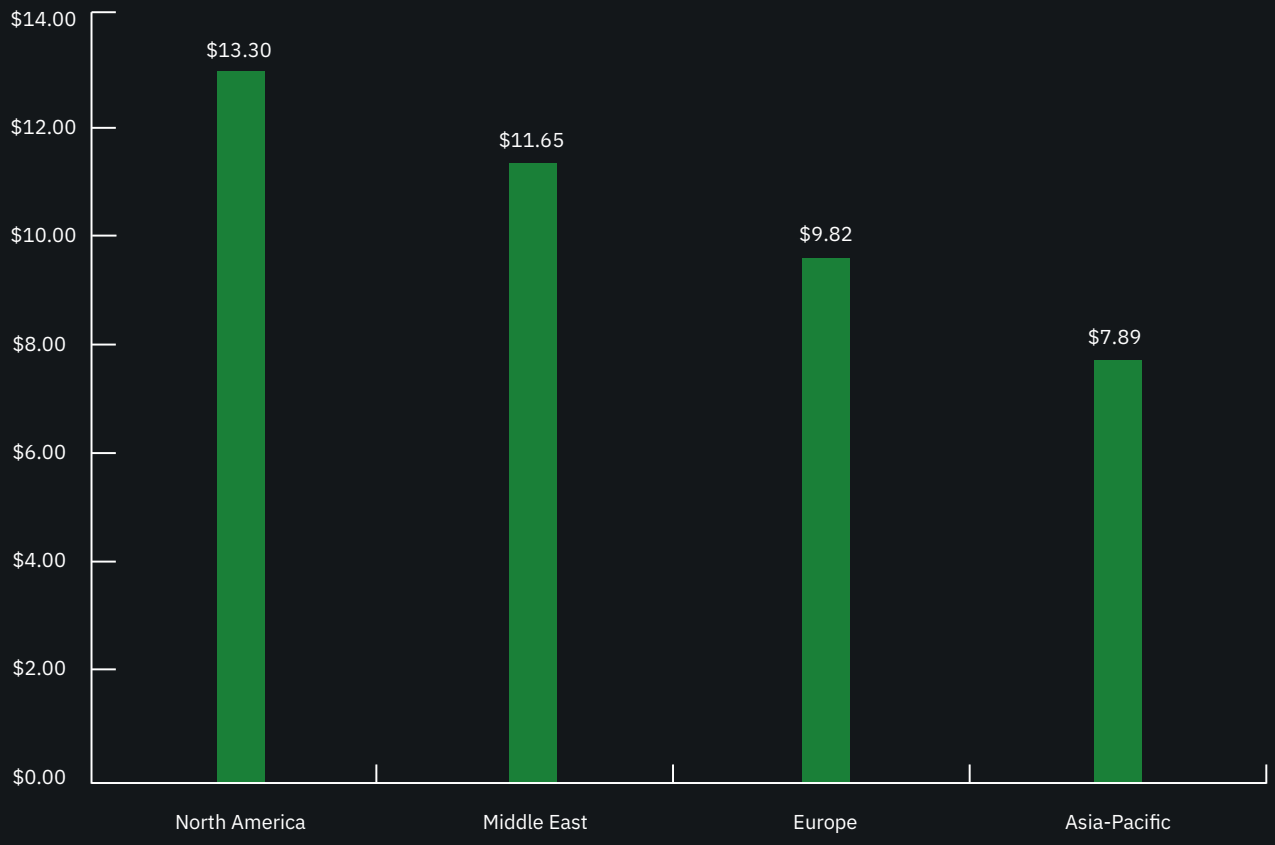


Figure 10 North American companies had an average annual cost higher than the average cost. Total annualized cost for three global regions is reported in Figure 10. Companies in North America experienced the highest total cost at USD $13.3 million. Middle East companies had the next highest cost at USD $11.65 million. Europe and Asia-Pacific had an average cost much lower than average total cost for all 204 companies.

Figure 11:

Insider incidents in ascending order by headcount (size)

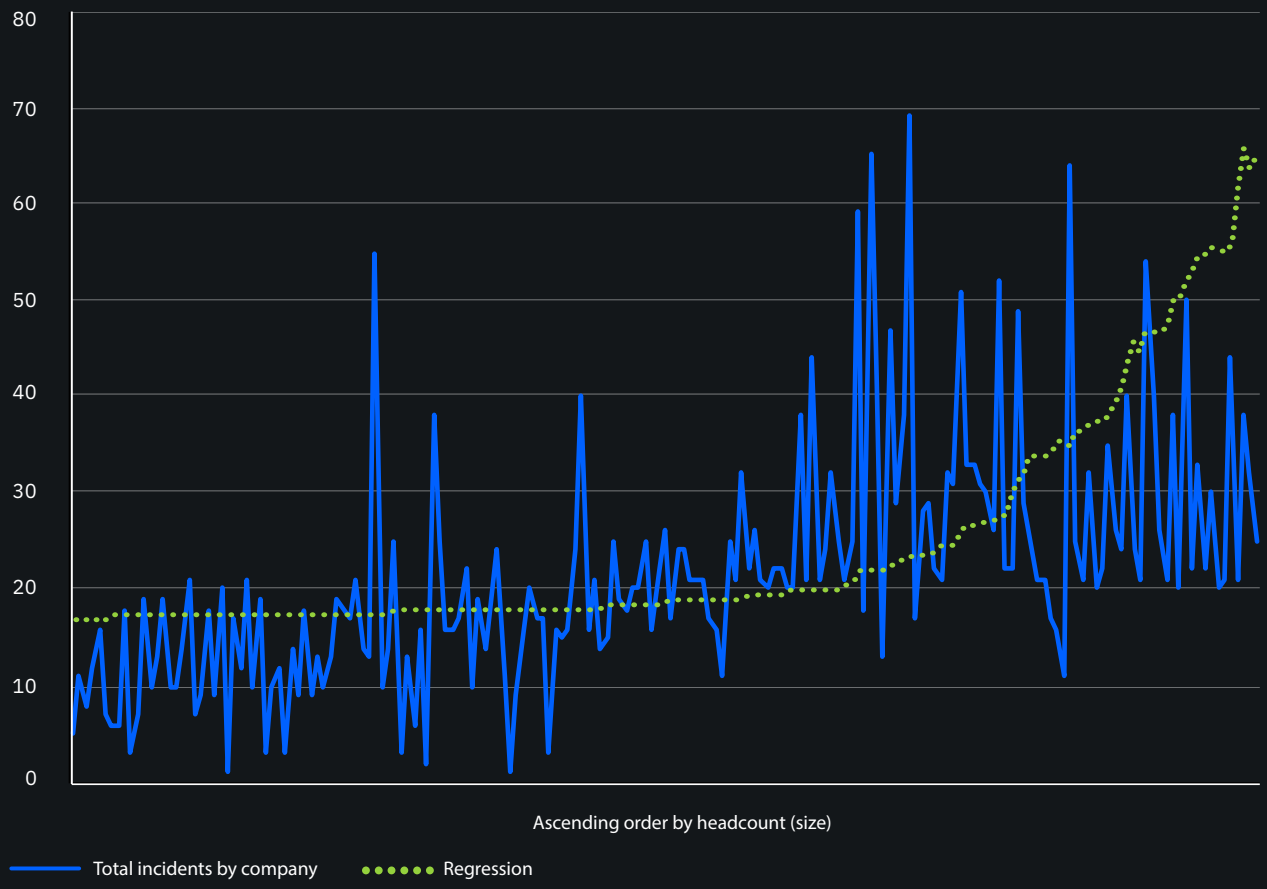


Figure 11 A simple linear regression model was used and from the data an R2 value of .21 was calculated. The larger the organization, the more insider incidents. Figure 11 shows the distribution of insider incidents in ascending order by headcount or size of the participating companies. As can be seen, 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.

Figure 12:

Average activity cost by global region

Mean = $11.45 (US$ millions)

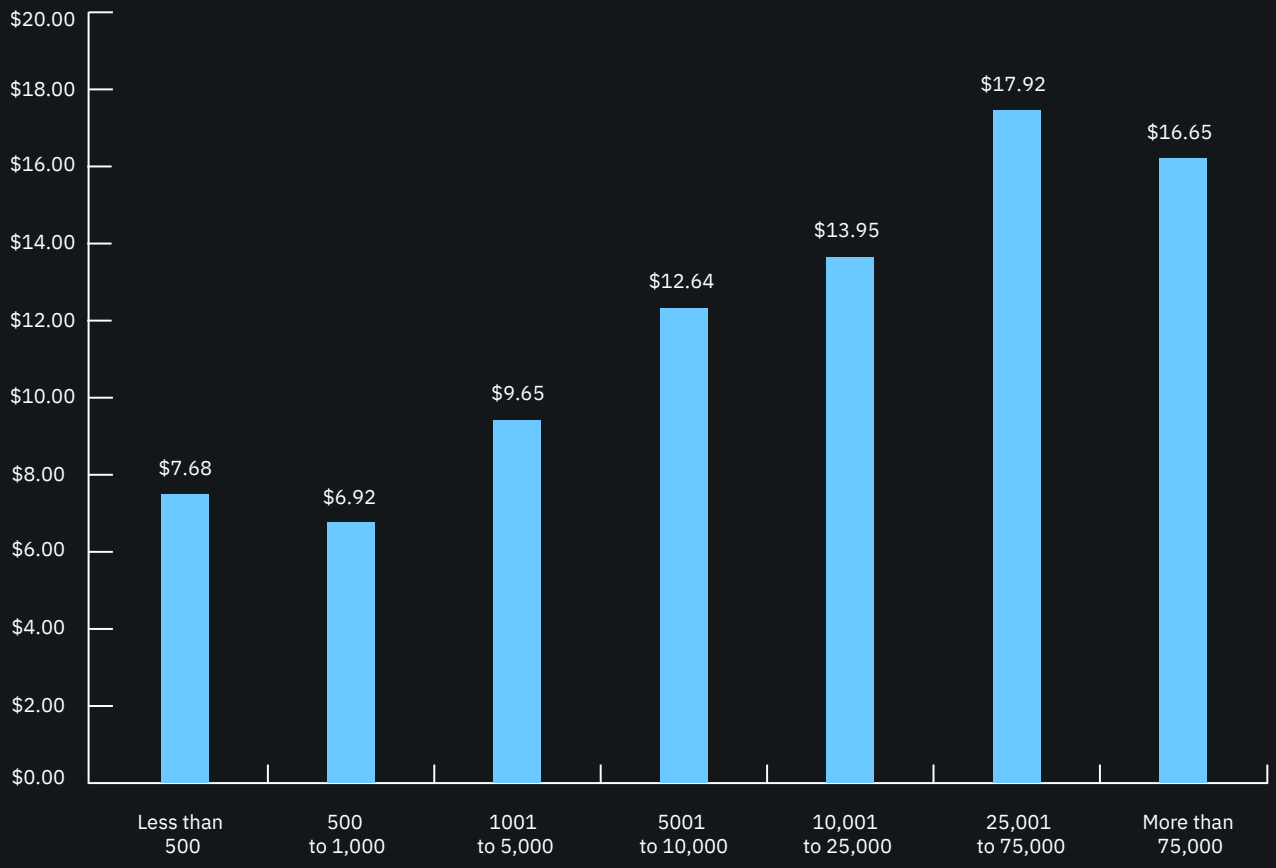


Figure 12 Total annualized cost adjusted for companies' worldwide headcount is reported in Figure 12. Companies with between 25,001 and 75,000 employees experienced the highest total cost at USD $17.92 million, while those with 500 to 1,000 employees had the lowest annualized cost at USD $6.92 million.

Cost Analysis

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 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 1:

Cost Activity Centers (per incident)

(US$ millions)

Cost Activity Centers (per incident)	Employee or contractor negligence	Criminal & malicious insider	Credential theft	Average cost
Monitoring & surveillance	$21,538	$21,857	$22,977	$22,124
Investigation	$49,441	$114,524	$147,429	$103,798
Escalation	$9,282	$29,513	$26,619	$21,805
Incident response	$62,877	$159,398	$132,677	$118,317
Containment	$75,903	$175,962	$382,794	$211,553
Ex-post analysis	$21,035	$19,282	$18,121	$19,480
Remediation	$67,036	$235,223	$141,069	$147,776
Total	$307,111	$755,760	$871,686	$644,852

Table 1 Companies spend an average of USD $644,852 on each incident. Table 1 summarizes the average cost of insider-related incidents for the three types of incidents and seven activity centers. As reported, containment and remediation represent the most expensive activity centers. Least expensive are ex-post analysis and escalation.

Table 2:

Activity Cost Centers

(US$ millions)

Cost Activity Centers	FY 2016	FY 2018	FY 2019	Net Increase over 3 years
Monitoring & surveillance	$9,610	$12,634	$22,124	79%
Investigation	$41,461	$78,398	$103,798	86%
Escalation	$8,919	$12,542	$21,805	84%
Incident response	$66,370	$91,263	$118,317	56%
Containment	$122,796	$173,060	$211,553	53%
Ex-post analysis	$8,498	$11,491	$19,480	78%
Remediation	$91,397	$138,532	$147,776	47%
Total	$349,052	$517,920	$644,852	60%

Table 2 Companies are spending more on investigations and escalation. Table 2 shows the percentage increase in cost for each activity. The cost of remediation has not increased as sharply as the other activities.

Figure 13:

Average cost per incident for three profiles

US$ millions

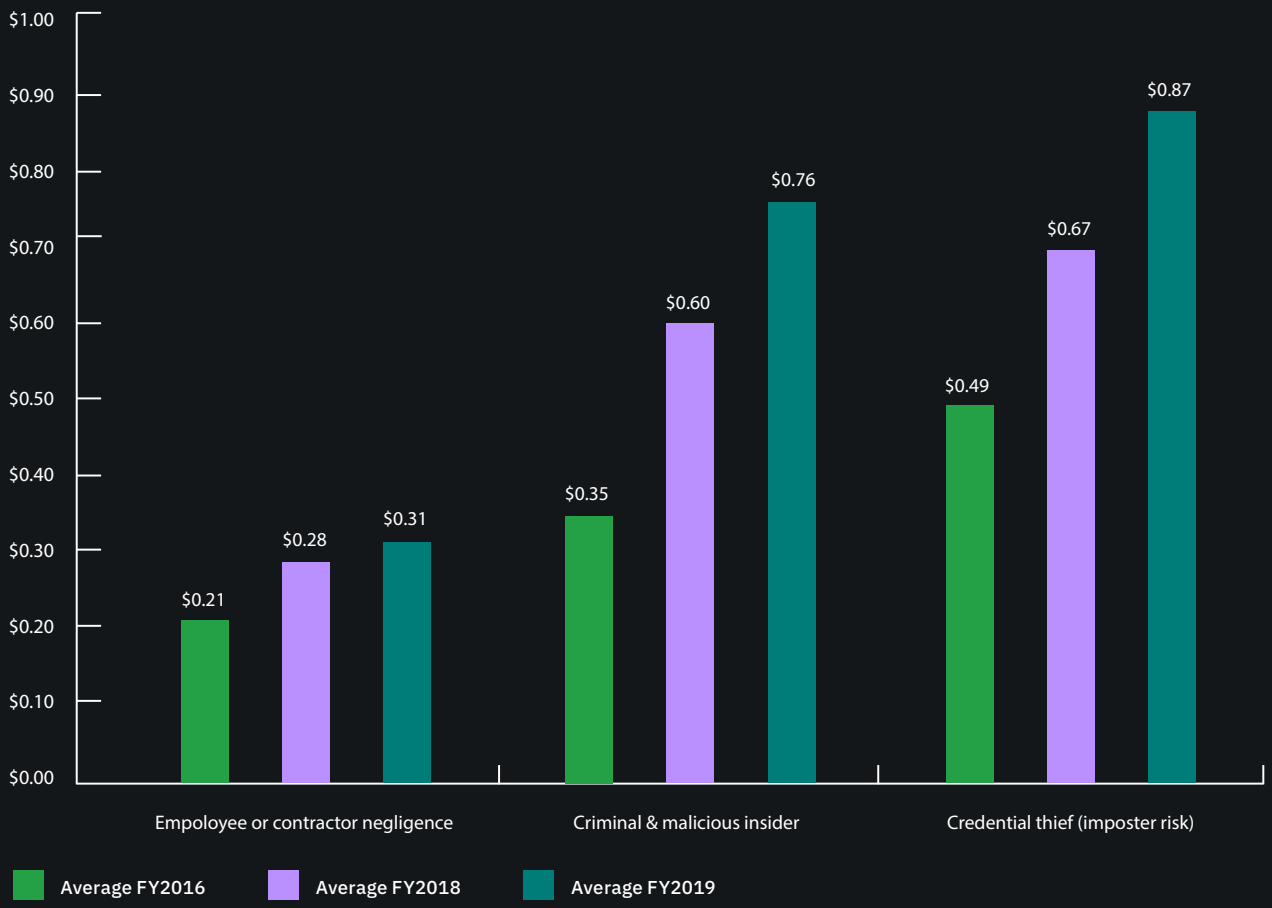


Figure 13 As shown in Figure 13, the costliest insider incidents involve credential theft – which is more than 2.5 times as expensive for incidents involving employee or contractor negligence.

Figure 14:

Average annualized cost for three profiles

US$ millions

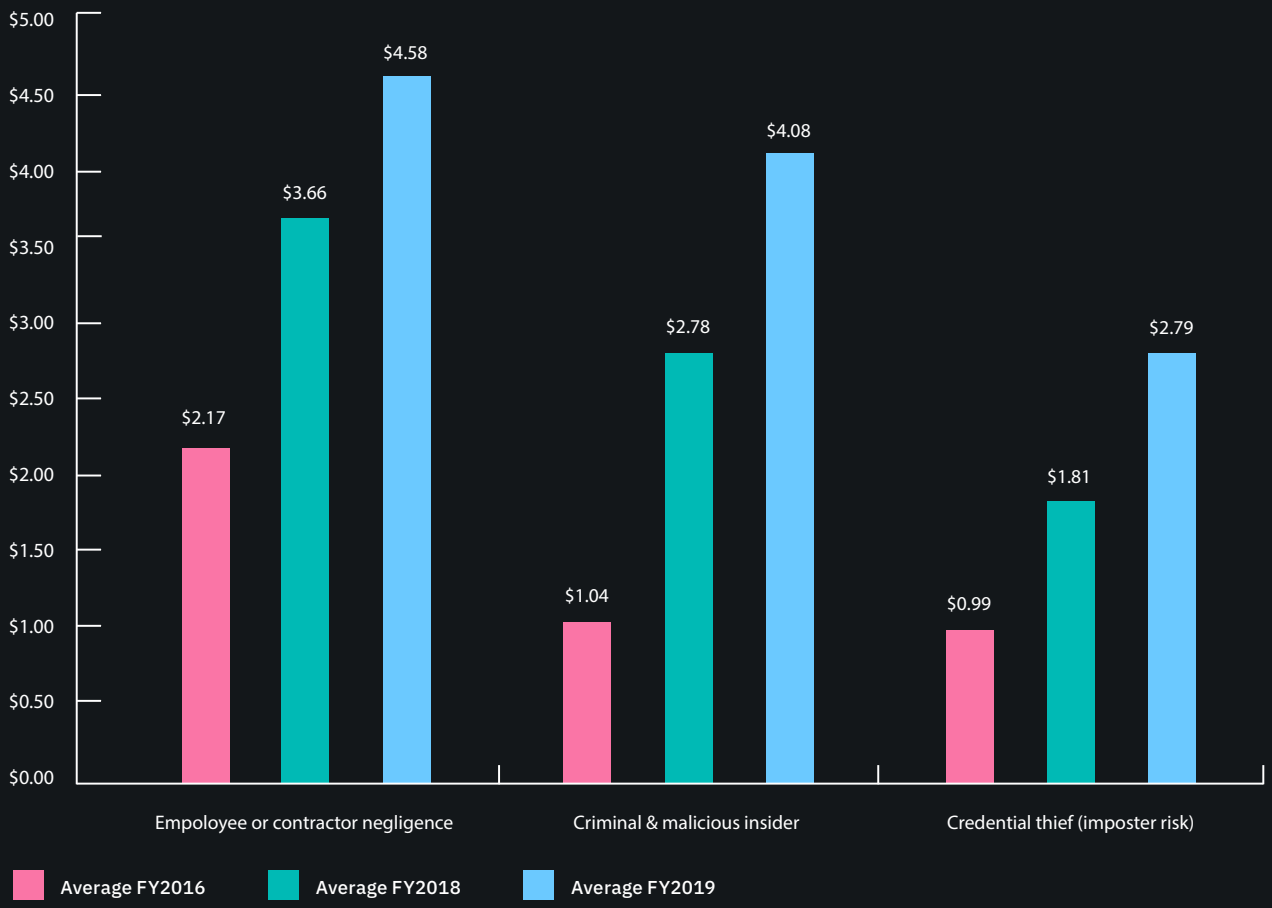


Figure 14 On an annual basis, employee or contractor negligence costs companies the most. Figure 14 reports the extrapolated annualized insider-related costs for three profiles. In terms of total annual costs, it is clear that employee or contractor negligence represents the most expensive insider profile. While credential theft is the most expensive on a unit cost basis, it represents the least expensive profile on an annualized basis.

Figure 15:

Sample statistics on the cost of insider incidents over the past 12 months

Consolidated for three profiles
US$ millions

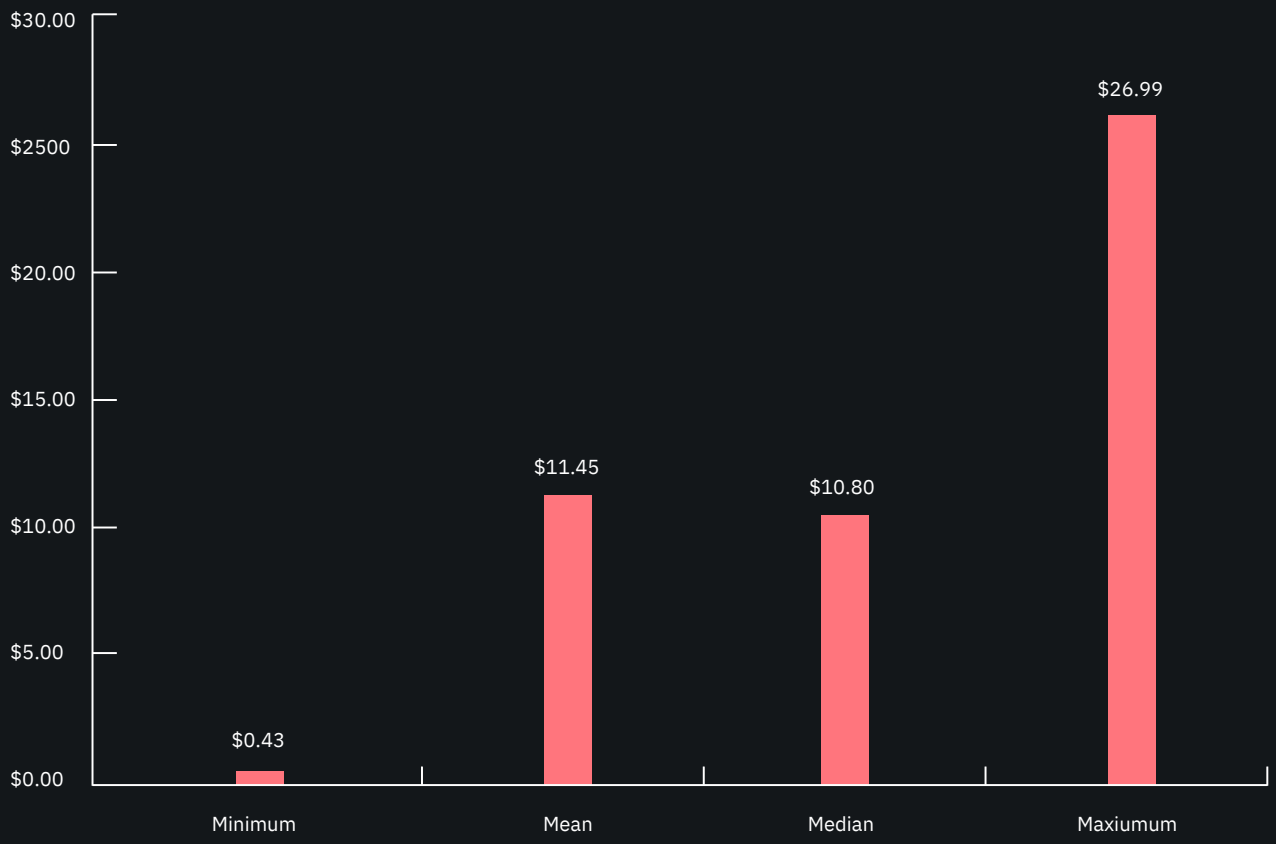


Figure 15 reports the median, mean, minimum and maximum values for insider cost (combining three profiles) over the past 12 months. The mean and median are USD $11.45 and USD $10.80 million, respectively. The minimum cost value is USD $.43 million and the maximum cost value is USD $26.99 million.

Figure 16:

Percentage cost of insider incidents by activity center

n = 204 companies

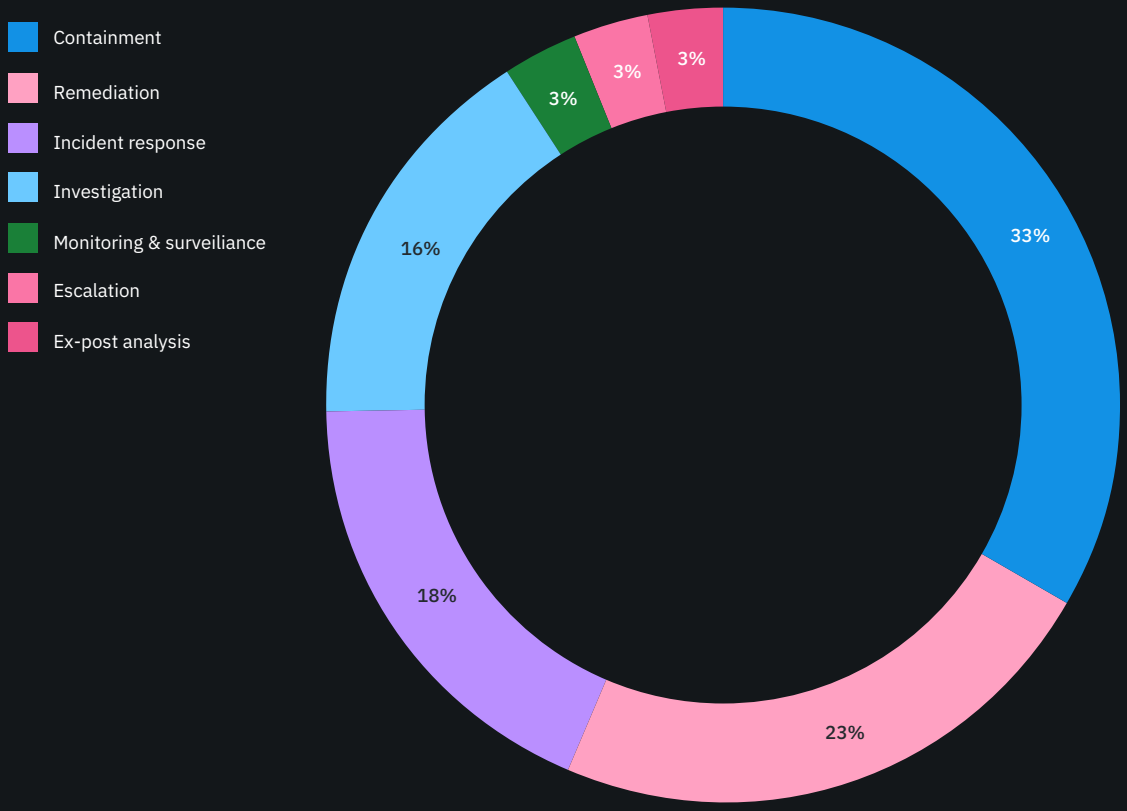


Figure 16 Containment accounts for one-third of all costs. The above pie chart shows the percentage cost for seven activity centers. According to Figure 16, containment represents 33 percent of total annualized insider-related costs. Activities relating to remediation and incident response represent 23 percent and 18 percent of total cost, respectively.

Figure 17:

Percentage of insider cost by standard categories

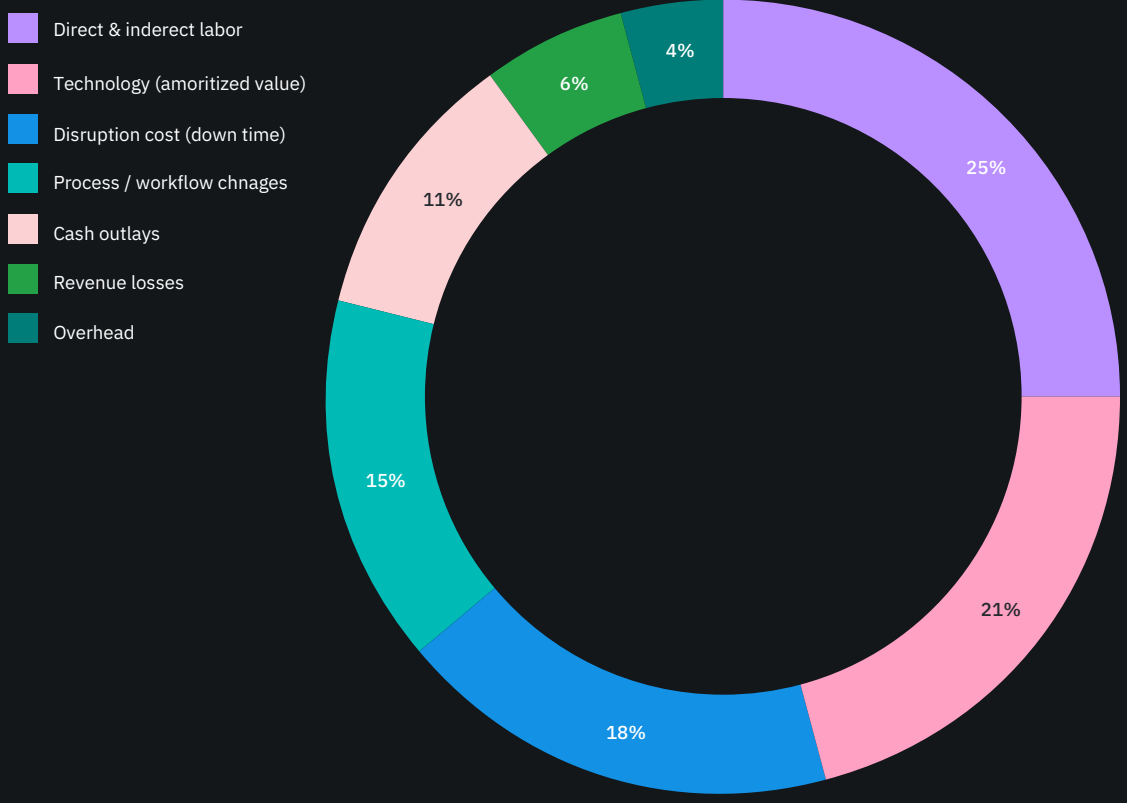


Figure 17 Companies are spending the most on personnel and technology to resolve insider incidents. Figure 17 reports the percentage of insider cost for careless or negligent employees, criminal insiders and credential theft according to seven cost categories. The two largest cost categories (direct & indirect labor) include both direct and indirect costs associated with in-house personnel and temporary and contract workers. This is followed by technology, which includes the amortized value and the licensing for software and hardware that are deployed in response to insider-related incidents (18 percent).

Process costs include governance and control system activities in response to threats and attacks. The cost of disruption includes diminished employee/user productivity as a result of insider incidents. Overhead includes a wide array of miscellaneous costs incurred to support personnel as well as the IT security infrastructure.

Figure 18:

Percentage of direct vs. indirect costs for activity centers

Consolidated for three profiles

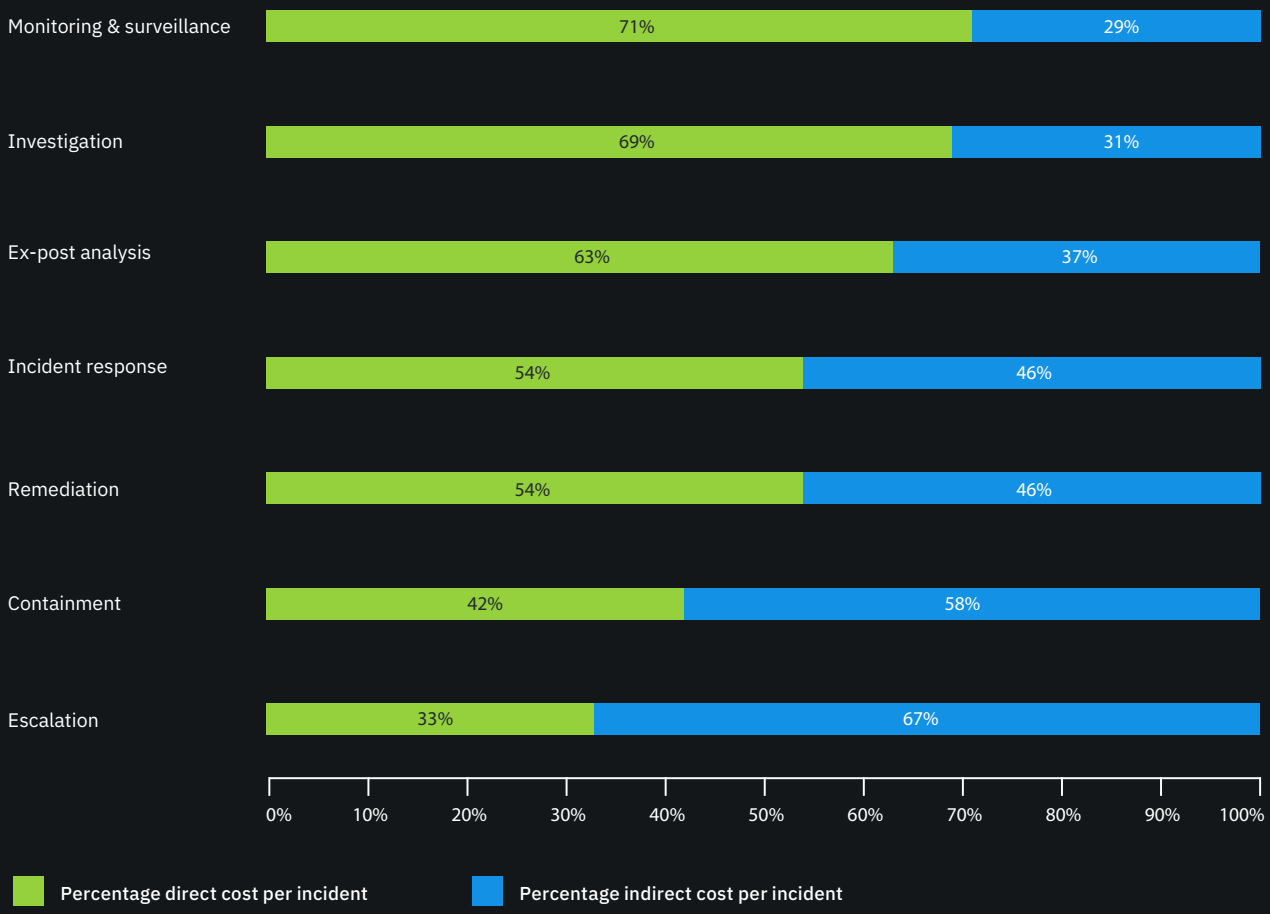


Figure 18 Companies were asked to estimate the direct costs spent to accomplish a given activity and the amount of time, effort and other resources spent, but not as a direct cash outlay (i.e. indirect costs). Figure 18 shows the proportion of direct and indirect costs for seven internal activity cost centers. As can be seen, the cost related to monitoring and surveillance has the highest direct cost percentage. In contrast, escalation has the highest percentage of indirect cost.

Figure 19:

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

Average = 77 days

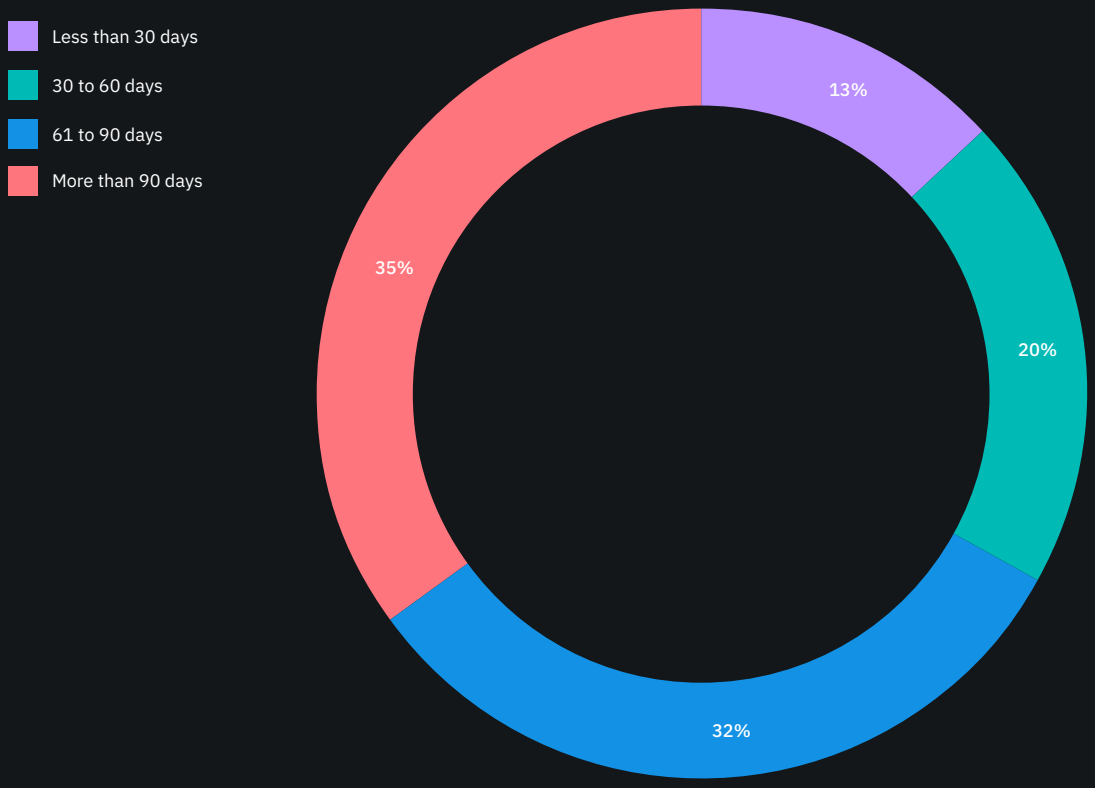


Figure 19 Companies are spending an average of more than two months to contain an incident. According to Figure 19, the time to contain insider-related incidents in our benchmark sample took an average of 77 days to contain the incident. Only 13 percent of incidents were contained in less than 30 days.

Figure 20:

Average activity cost by days to contain the incidents

Mean = $11.45 (US$ millions)

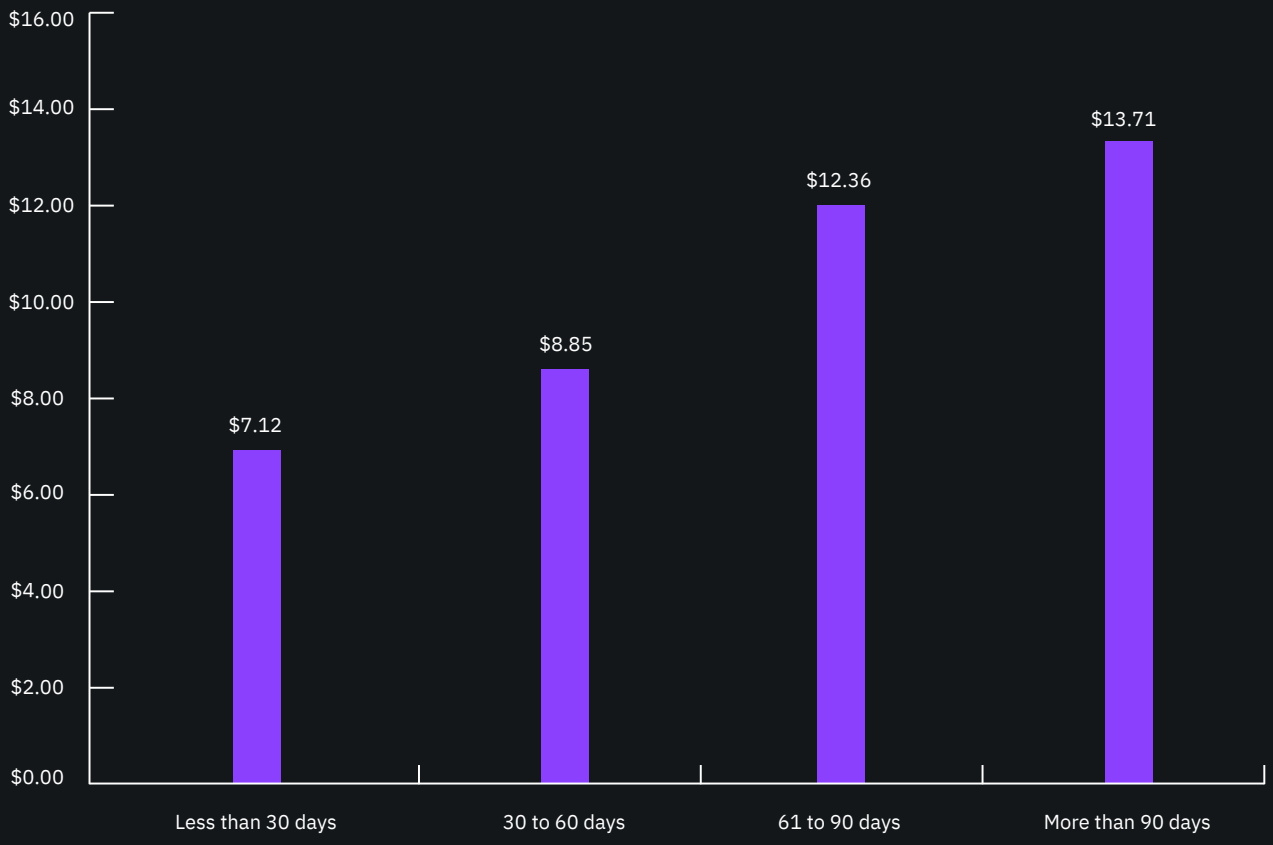


Figure 20 The faster containment occurs, the lower the cost. Total annualized cost appears to be positively correlated with the time to contain insider-related incidents. As shown in Figure 20, incidents that took more than 90 days to contain had the highest average total cost per year (USD $13.71 million). In contrast, incidents that took less than 30 days to contain had the lowest total cost (USD $7.12 million). The average annual cost is USD $11.45 million.

Figure 21:

Annualized activity cost by industrial sector

Mean = $11.45 (US$ millions)

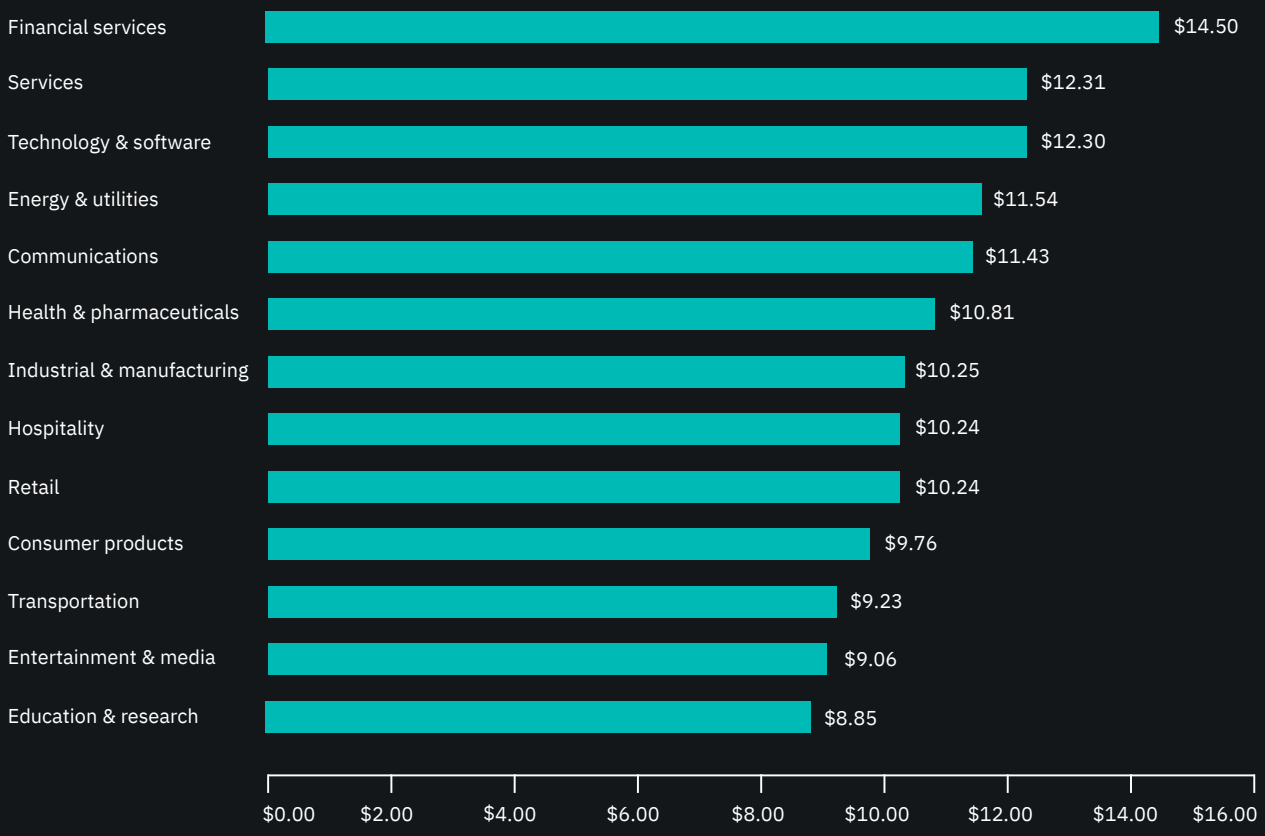


Figure 21 Total annualized cost for 13 industry sectors is reported in Figure 21.[3] At USD $14.50 million, companies in financial services experienced the highest total cost. Services and technology & software had the next highest costs at USD $12.31 million and USD $12.30 million, respectively. In contrast, companies in education and research had the lowest total annualized cost at USD $8.85 million.

[3]Care should be taken when reviewing industry sector differences because of small subsample sizes.

Figure 22:

Scattergram of insider-related incidents by company

n = 204 companies

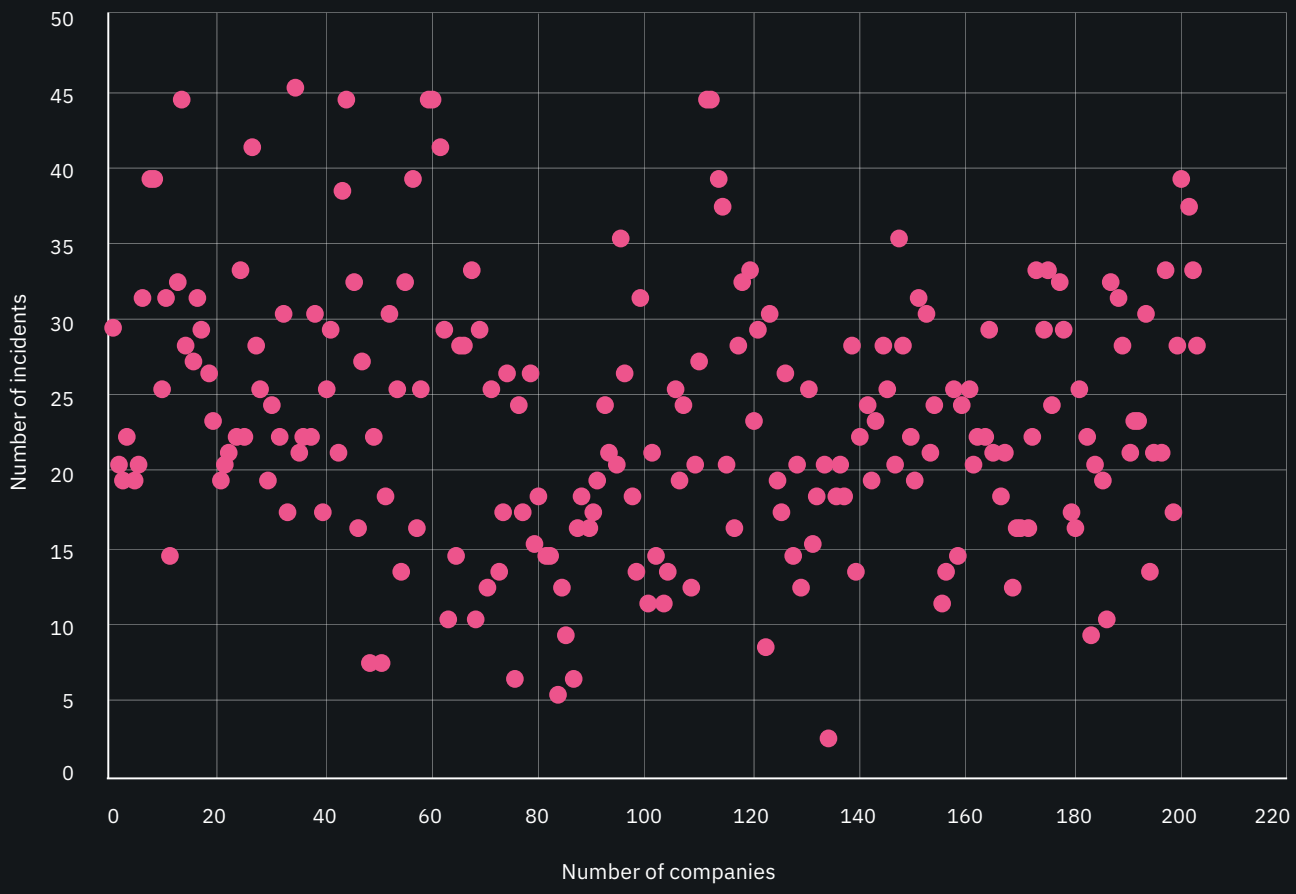


Figure 22 shows a scattergram on the total annualized cost of insider incidents per company. Of the 204 participating companies, 124 companies (61 percent) of companies had an average total cost at or below the mean of USD $11.45 million over the past 12 months. The remaining 80 companies (39 percent) are above the average of USD $11.45 million. This finding suggests that the distribution is skewed.

[3]Care should be taken when reviewing industry sector differences because of small subsample sizes.

Table 3:

Tools and activities that reduce insider threats

Security tools & activities	Frequency of companies	Percentage of companies
User training & awareness	112	55%
Data loss prevention (DLP)	110	54%
User behavior analytics (UBA)	102	50%
Employee monitoring & surveillance	96	47%
Security incident & event management (SIEM)	91	45%
Incident response management (IRM)	89	44%
Strict third-party vetting procedures	87	43%
Threat intelligence sharing	85	42%
Privileged access management (PAM)	80	39%
Network traffic intelligence	77	38%

Table 3 The majority of companies are deploying user training awareness (55 percent), data loss prevention (54 percent) and user behavior analytics (50 percent) to prevent insider threats, as shown in Table 3.

Figure 23:

Cost savings resulting in the deployment of cyber risk reducing tools and activities

Mean = $11.45 (US$ millions)

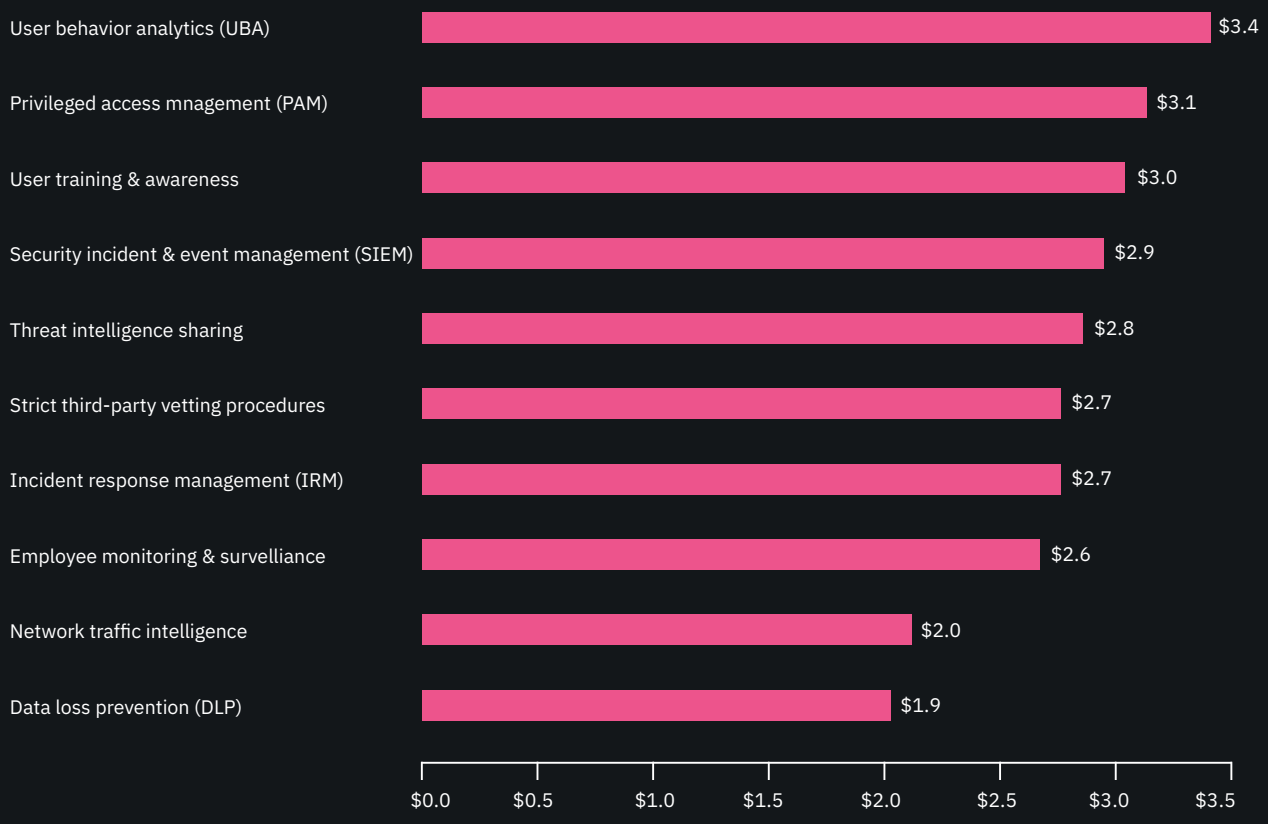


Figure 23 UBA, PAM and user training awareness are the most cost effective tools and activities. According to Figure 24, companies can save an average of USD $3.4 million and USD $3.1 million when deploying UBA and a privileged access management (PAM) solution. The most frequently deployed tools and activities are shown in Table 3. Accordingly, 112 companies conduct training programs to raise employee awareness about insider threats. The number of companies that utilize data loss prevention is 110 and 102 companies deploy user behavior analytics (UBA) to spot suspicious network activities.

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:

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]

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]

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.

[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.

[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.

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:

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.processes. These include the restoration of damaged information assets and IT infrastructure.

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.

Currency conversions for non US-currencies are current as of this field of research timeframe. Field Research was launched in March 2019. 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).

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 global study, 507 companies completed the benchmark process. Non-response bias was not tested so it is possible that 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 omitted 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, it is always possible 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.

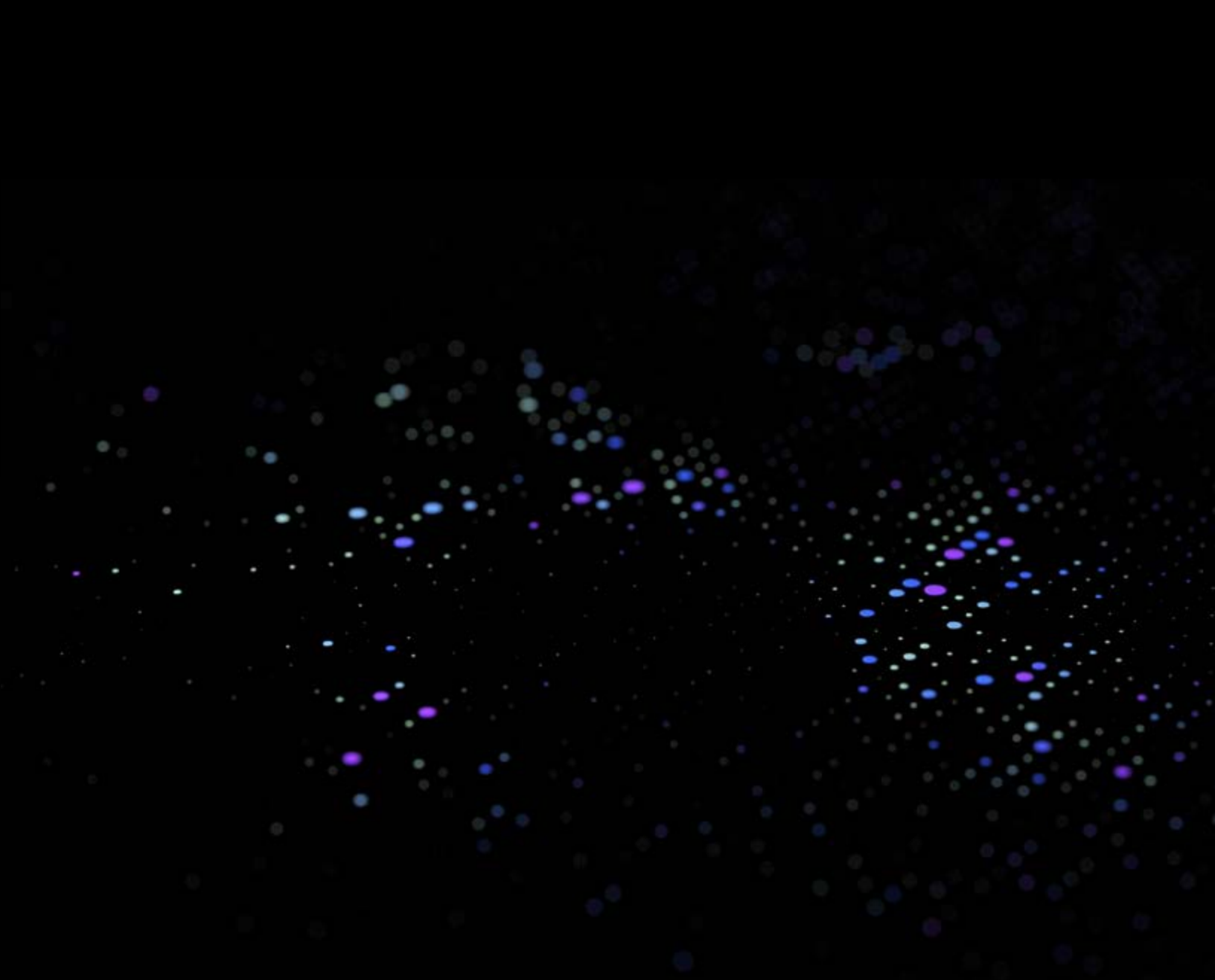
Next steps

Deliver Digital Trust
Grow business and protect your organization from insider threats with a seamless user experience.

Protect Assets
Ensure the secure flow of data through apps and endpoints.

Identify Threats
Automate threat detection and response across the enterprise.

Remediate and Respond
Analyze and respond to advanced persistent threats and advanced attacks.



If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

The Cost of Insider Threats report is sponsored by IBM Security and Observe IT. Previous years' Cost of a Data Breach Reports are available at ibm.com/security/data-breach

Ponemon Institute LLC
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.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security solutions to help organizations stop threats, prove compliance, and grow securely.

IBM operates one of the broadest and deepest security research, development and delivery organizations. It monitors more than two trillion events per month in more than 130 countries and holds more than 3,000 security patents. To learn more, visit ibm.com/security.

IBM **Security**