2018 Cost of Insider Threats: Global

Sponsored by ObserveIT

Independently conducted by Ponemon Institute LLC
Publication Date: April 2018

2018 Cost of Insider Threats: Global

Ponemon Institute: April 2018

Part 1. Introduction

Companies throughout the globe share the risk of having a serious data breach or security exploit caused by an insider or credential thief. The *2018 Cost of Insider Threats: Global* study, sponsored by ObserveIT, is the second 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 are defined as:

- A careless or negligent employee or contractor,
- A criminal or malicious insider or
- A credential thief.

We interviewed 717 IT and IT security practitioners in 159 organizations in North America (United States and Canada), Europe, Middle East & Africa and Asia-Pacific. Interviews were completed in January 2018. Each organization experienced one or more material events caused by an insider. These organizations experienced a total of 3,269 insider incidents over the past 12 months. Our targeted organizations were business organizations with a global headcount of 1,000 or more employees.

Imposter risk is the most costly

The cost ranges significantly based on the type of incident. If it involves a negligent employee or contractor, each incident can average $283,281. The average cost more than doubles if the incident involves an imposter or thief who steals credentials ($648,845). Hackers cost the organizations represented in this research an average of $607,745 per incident. The activities that drive costs are: 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:

- Total number of benchmarked organizations = 159
- Total number of insider incidents = 3,269
- Total average cost = $8.76 million
- Incidents relating to negligence = 64%
- Incidents relating to criminal insider = 23%
- Incidents relating to user credential theft = 13%
- Annualized cost for negligence = $3.81 million
- Annualized cost for criminal insider = $2.99 million
- Annualized cost for credential theft = $1.96 million

The negligent insider is the root cause of most incidents

Most incidents in this research were caused by insider negligence. Specifically, the careless employee or contractor was the root cause of almost 2,081 of the 3,269 incidents reported. The most expensive incidents are due to imposters stealing credentials and were the least reported. There were a total of 440 incidents involving stolen credentials.

Organizational size and industry affects the cost per incident

The cost of incidents varies according to organizational size. Large organizations with a headcount of more than 75,000 spent an average of $2,081 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 $1.80 million. Companies in financial services, energy & utilities and industrial & manufacturing incurred average costs of $12.05 million, $10.23 million and $8.86 million, respectively.

All types of threat of insider risks are increasing. Since 2016 the average number of incidents involving employee or contractor negligence has increased from 10.5 to 13.4. The average number of credential theft incidents has tripled over the past two years, from 1.0 to 2.9.

Employee or contractor negligence costs companies the most. 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.

It takes an average of more than two months to contain an insider incident. It took an average of 73 days to contain the incident. Only 16 percent of incidents were contained in less than 30 days.

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 January 2018. Our final benchmark sample consisted of 159 separate organizations. A total of 717 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 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 159 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:

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

Part 2. Benchmarked Sample

The following 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 1. Industry distribution for participating organizations
n = 159 companies

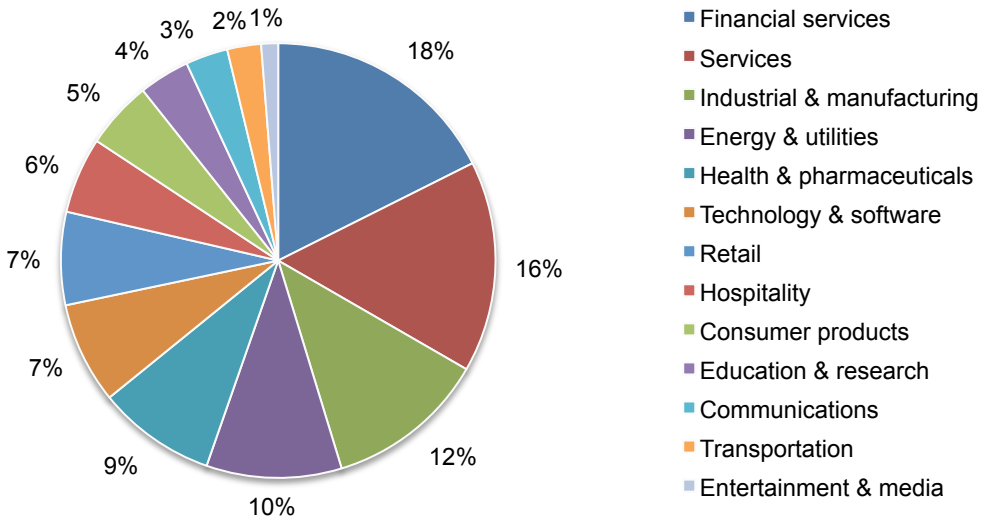
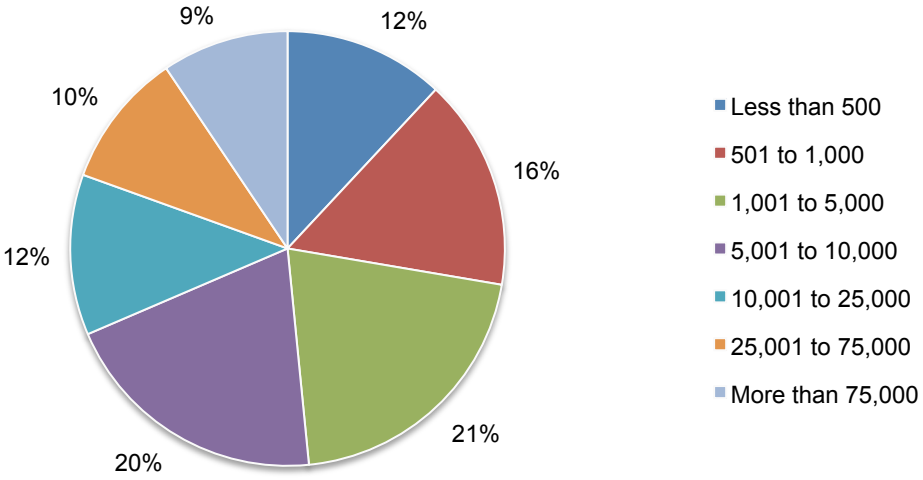


Figure 2 shows the percentage distribution of companies according to global headcount, which is a surrogate for organizational size. As can be seen, 51 percent of the sample includes larger-sized companies with more than 5,000 full-time equivalent employees.

Figure 2. Headcount of participating organizations
n = 159 companies



According to Figure 3, the three largest segments of individuals who participated in field-based interviews include CISOs, IT operations practitioners and IT technicians.

Figure 3. Distribution of interviewees by position or function
n = 717 respondents

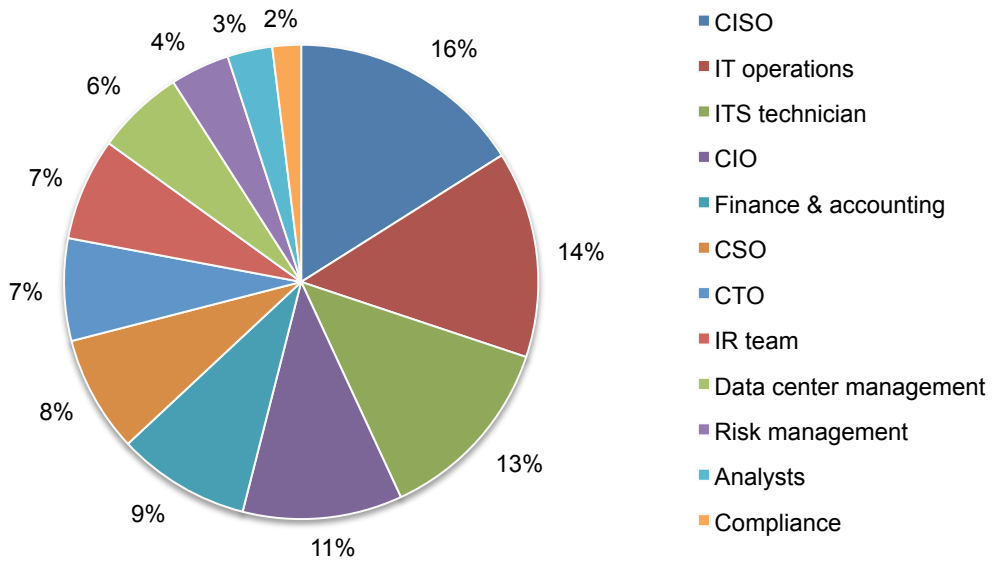
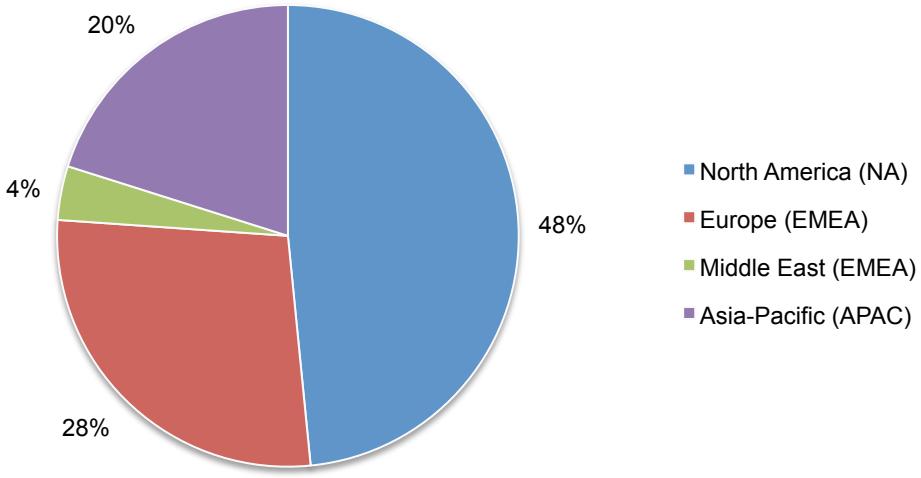


Figure 4 shows the global regions participating in this research. North America represents the largest segment (77 companies) and Asia-Pac is the smallest segment (32 companies). Because of small sample size, we combined 44 European and 6 Middle Eastern companies to form the EMEA segment.

Figure 4. Regional distribution of global organizations
n = 159 companies



Part 3. Analysis of Insider Incidents

Figure 5 shows the distribution of 3,269 reported attacks analyzed in our sample. A total of 2,081 attacks (or 64 percent) pertained to employee or contractor negligence. Criminal or malicious insiders caused another 748 attacks (or 23 percent). Only 430 attacks (or 13 percent) involved credential theft (a.k.a. imposter risk). The largest number of reported incidents for a given company is 60 and the smallest number of incidents is 1.

Figure 5. Frequency of 3,269 incidents for three insider profiles

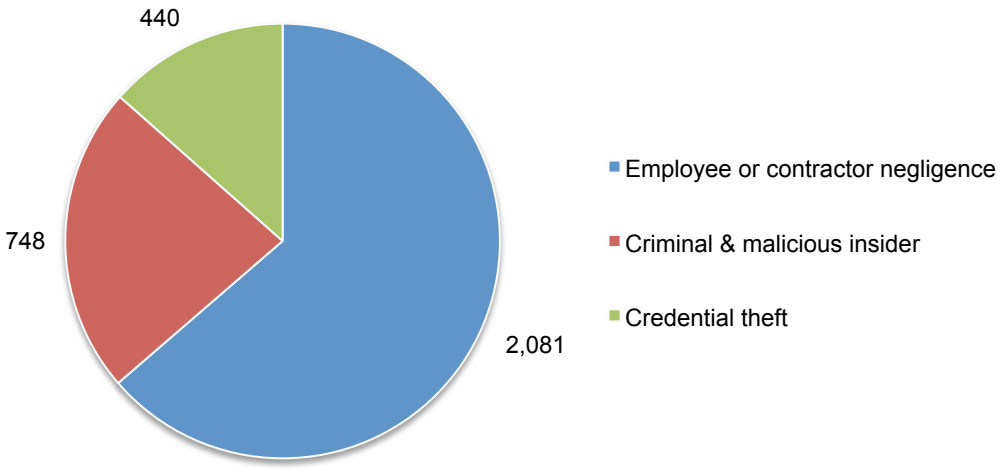
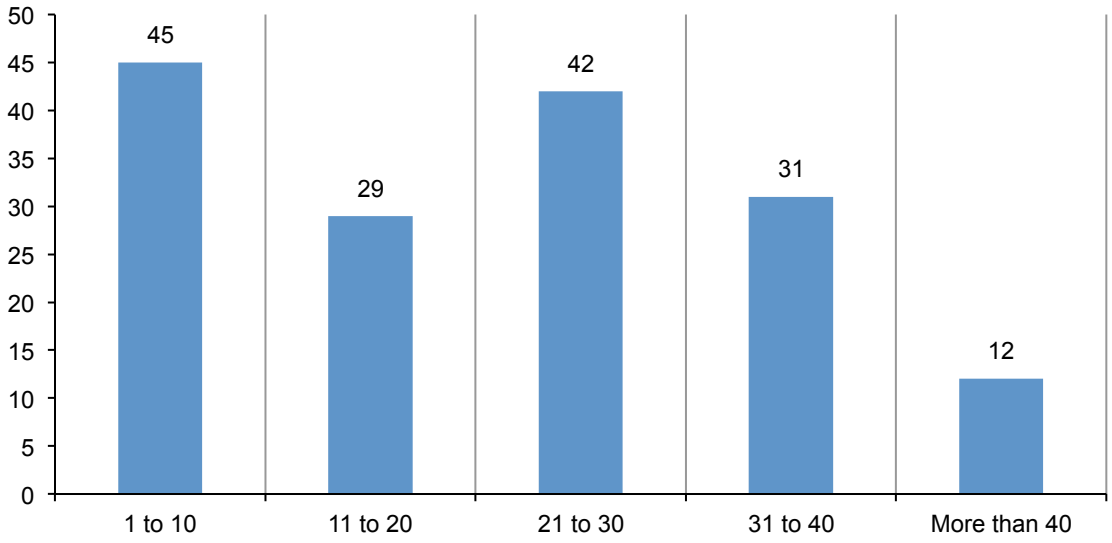


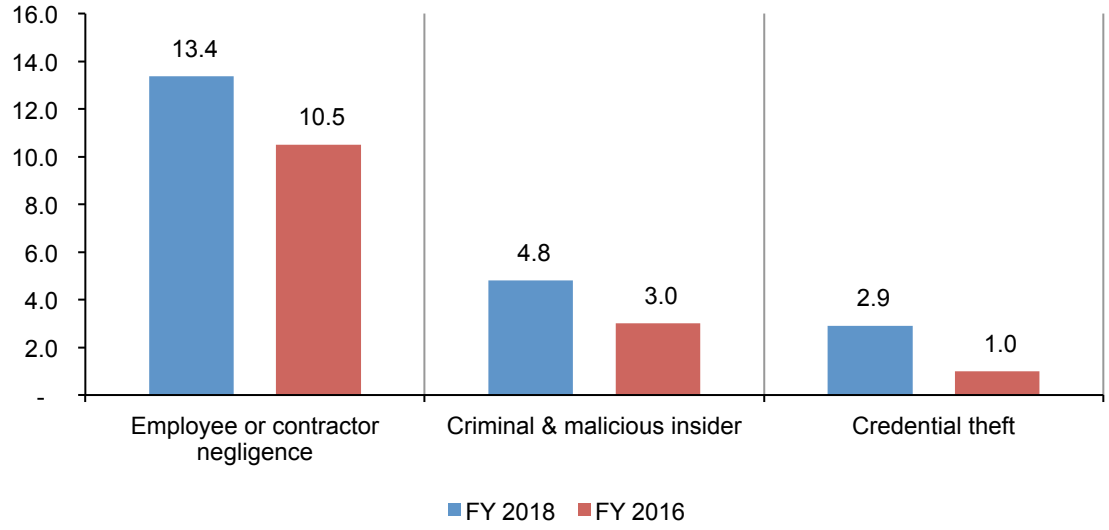
Figure 6 provides a graph that shows a histogram of insider incidents for our sample of 159 companies over the past 12 months. As can be seen, 45 companies experienced between 1 and 10 incidents, while only 12 companies experienced more than 40 incidents.

Figure 6. Frequency of insider-related incidents per company
Consolidated for three profiles



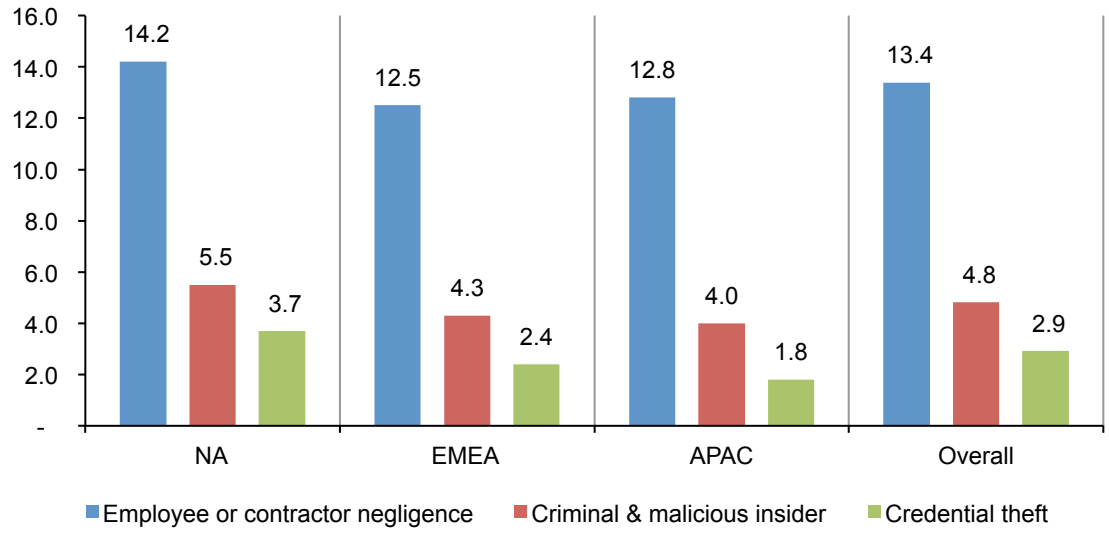
All types of threat of insider risks are increasing. As shown in Figure 7, since 2016 the average number of incidents involving employee or contractor negligence has increased from 10.5 to 13.4. The average number of credential theft incidents has almost tripled over the past two years, from 1.0 to 2.9.[1]

Figure 7. Frequency for three profiles of insider incidents



The frequency of insider threats varies across global regions. As shown in Figure 8, North American 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.

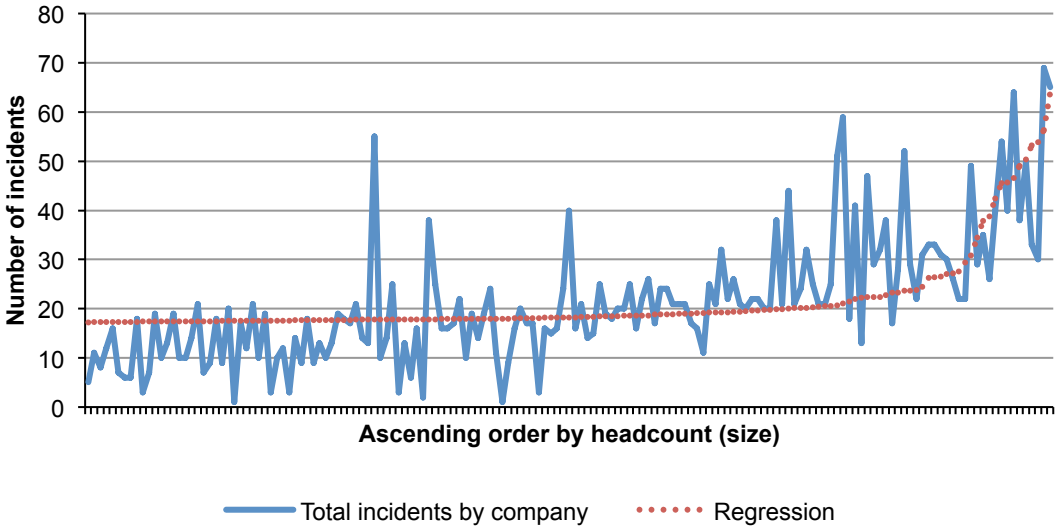
Figure 8. Frequency for three profiles of insider incidents by global region



[1] The 2016 data only pertains to US companies. The 2018 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 9 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 9. Insider incidents in ascending order by headcount (size)



Part 4. Cost Analysis

Table 1 summarizes the average cost of insider-related incidents for three profiles (or personas) and seven activity centers. As reported, remediation, containment and incident response represent the most expensive activity centers.

Table 1. Cost Activity Centers (per incident)	Employee or contractor negligence	Criminal & malicious insider	Credential theft	Average cost
Monitoring & surveillance	$15,116	$10,902	$9,544	$11,854
Investigation	$37,972	$88,982	$98,987	$75,314
Escalation	$7,650	$18,734	$13,107	$13,164
Incident response	$42,267	$109,300	$101,938	$84,501
Containment	$49,980	$196,891	$270,218	$172,363
Ex-post analysis	$17,859	$11,443	$13,372	$14,225
Remediation	$112,436	$171,494	$141,679	$141,869
Total	$283,281	$607,745	$648,845	$513,290

As shown in Figure 10, the most costly insider incidents involve credential theft – which is more than 2.5 times as expensive for incidents involving employee or contractor negligence.

Figure 10. Average cost per incident for three profiles
US$

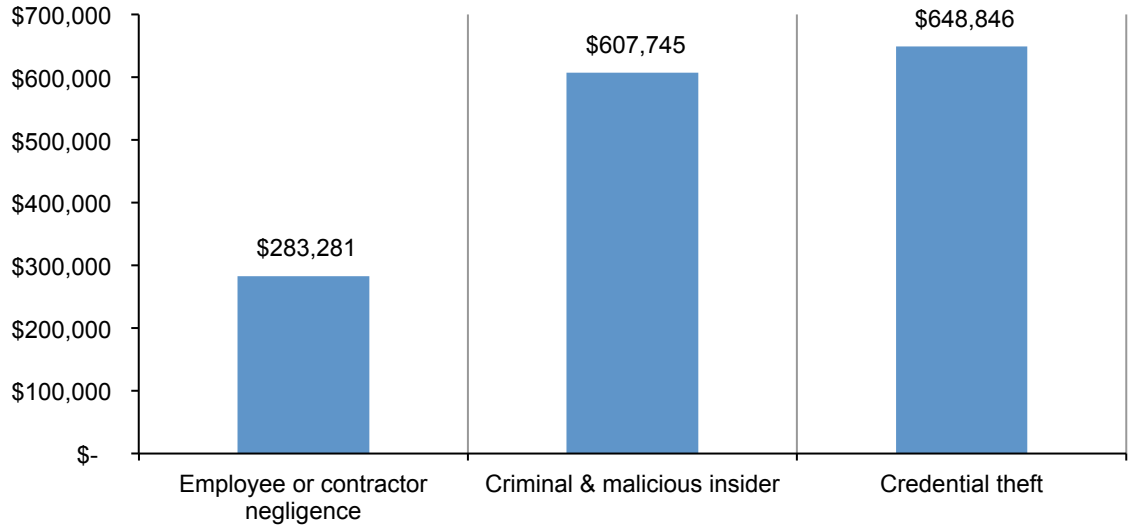


Figure 11 reports the extrapolated annualized insider-related costs for three profiles. In terms of total annual costs, it is clear that employee or contractor negligence represents the most expensive insider profile. While credential theft is the most expensive on a unit cost basis, it represents the least expensive profile on an annualized basis.

Figure 11. Average annualized cost for three profiles
US$

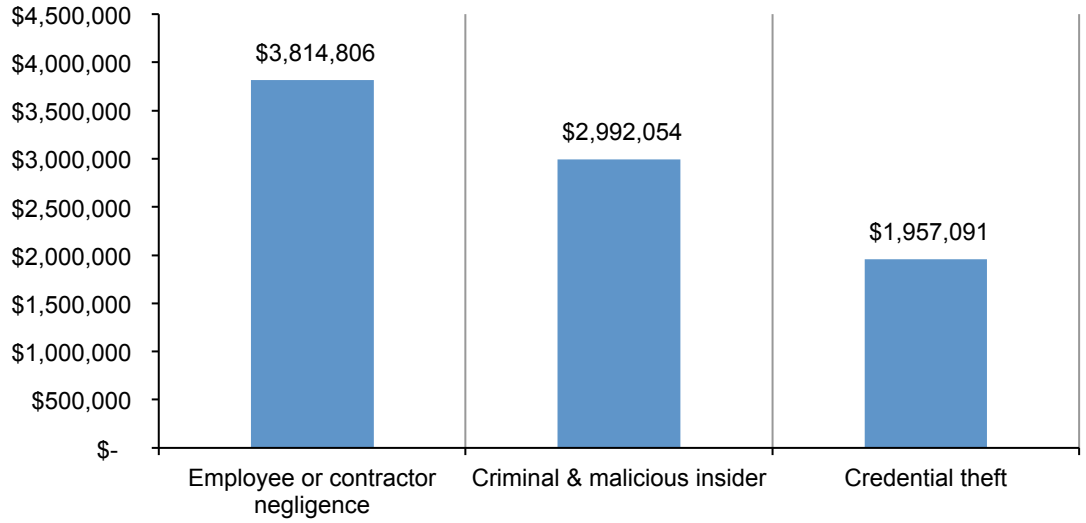
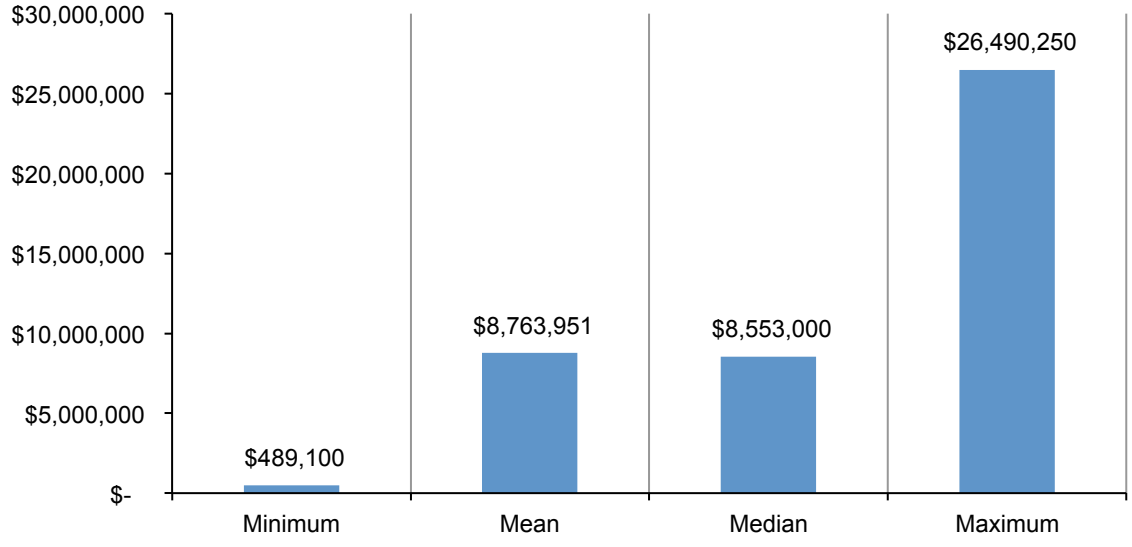


Figure 12 reports the median, mean, minimum and maximum values for insider cost (combining three profiles) over the past 12 months. The mean and median are $8.76 and $8.55 million, respectively. The minimum cost value is $489,100 and the maximum cost value is $26.5 million.

Figure 12. Sample statistics on the cost of insider incidents over the past 12 months
Consolidated for three profiles
US$



The following pie chart shows the percentage cost for seven activity centers. As can be seen in Figure 13, containment represents 34 percent of total annualized insider-related costs. Activities relating to remediation and incident response represent 28 percent and 16 percent of total cost, respectively.

Figure 13. Percentage cost of insider incidents by activity center
n = 159

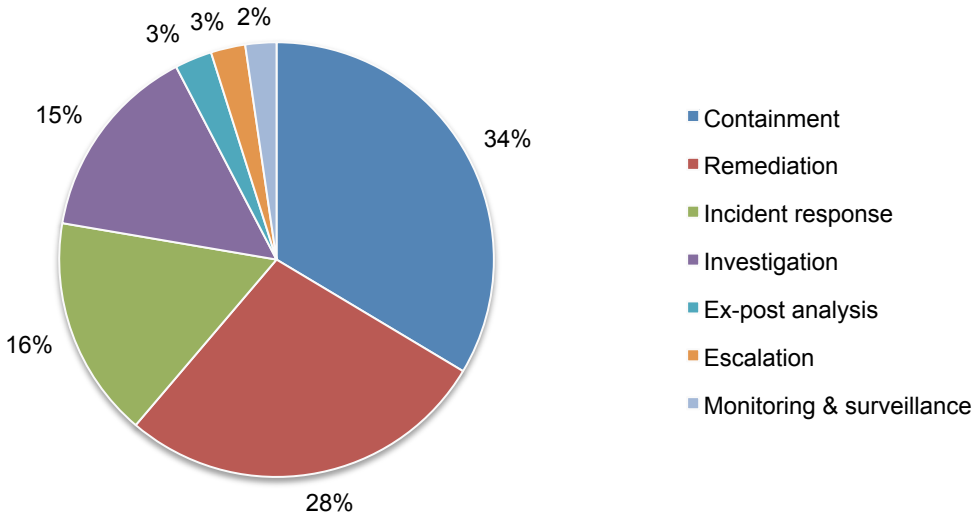


Figure 14 reports the percentage of insider cost for careless or negligent employees, criminal insiders and credential theft according to seven cost categories. The two largest cost categories (direct & indirect labor) include both direct and indirect costs associated with in-house personnel and temporary and contract workers. 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.

Technology costs include the amortized value plus licensing fees for software and hardware that are deployed in response to insider-related incidents. Overhead includes a wide array of miscellaneous costs incurred to support personnel as well as the IT security infrastructure.

Figure 14. Percentage of insider cost by standard categories

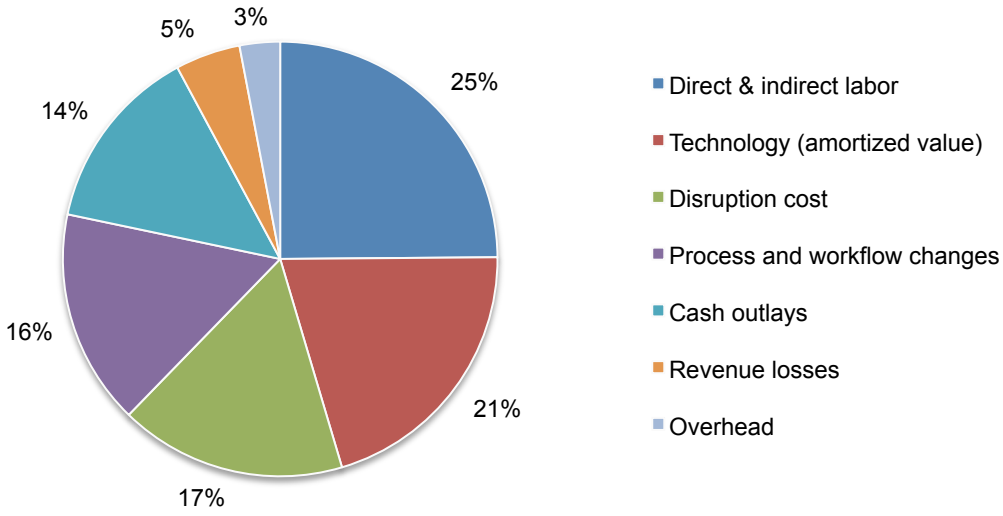


Figure 15 shows the proportion of direct and indirect costs for seven internal activity cost centers. As can be seen, the cost relating to monitoring and surveillance has the highest direct cost percentage. In contrast, escalation has the highest percentage of indirect cost.

Figure 15. Percentage of direct vs. indirect costs for activity centers

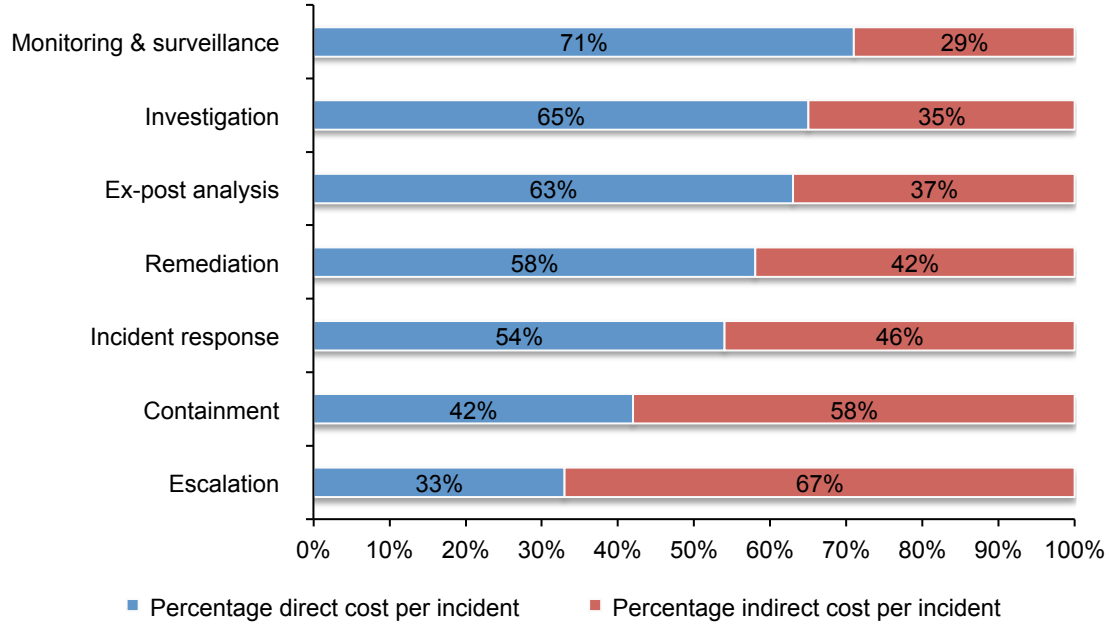
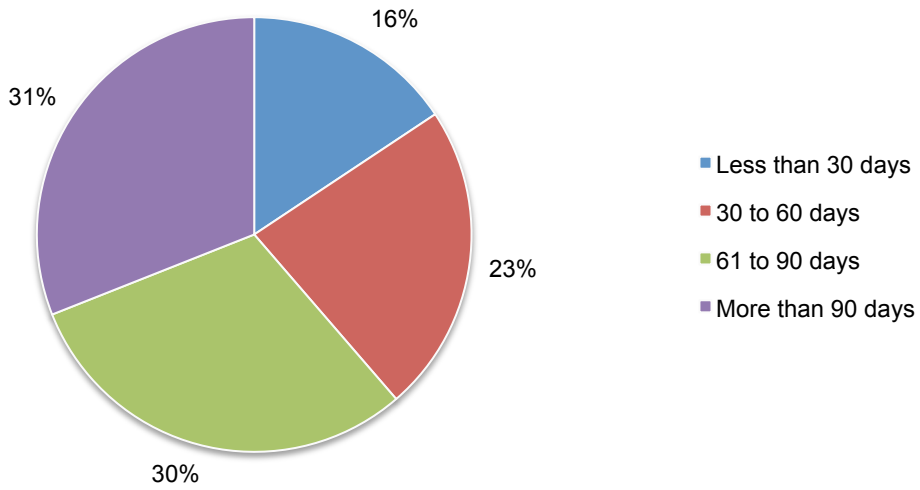


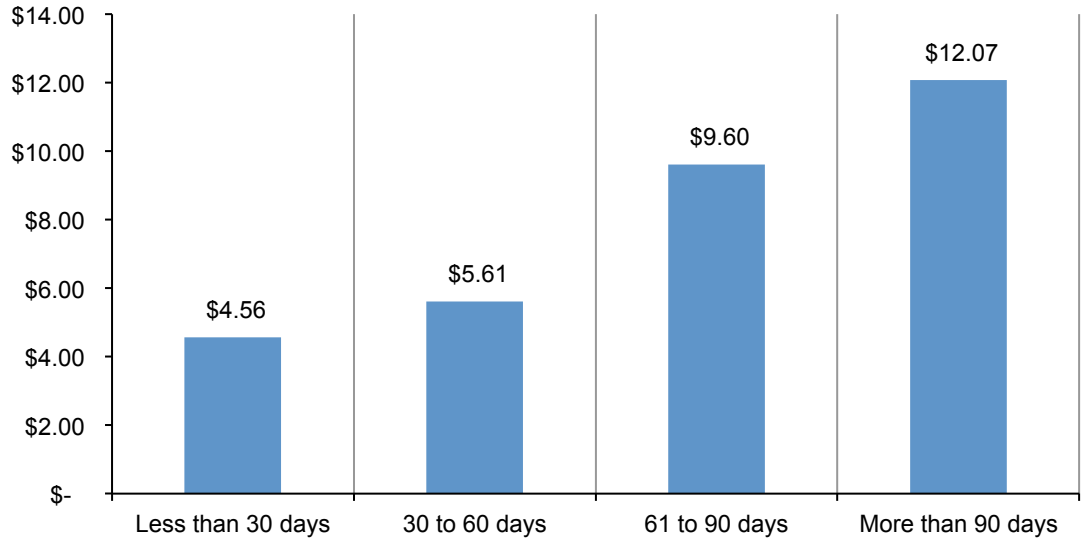
Figure 16 shows the time to contain insider-related incidents in our benchmark sample. As can be seen, it took an average of 72 days to contain the incident. Only 16 percent of incidents were contained in less than 30 days.

Figure 16. Percentage distribution of insider-related incidents based on the time to contain
Average = 72 days



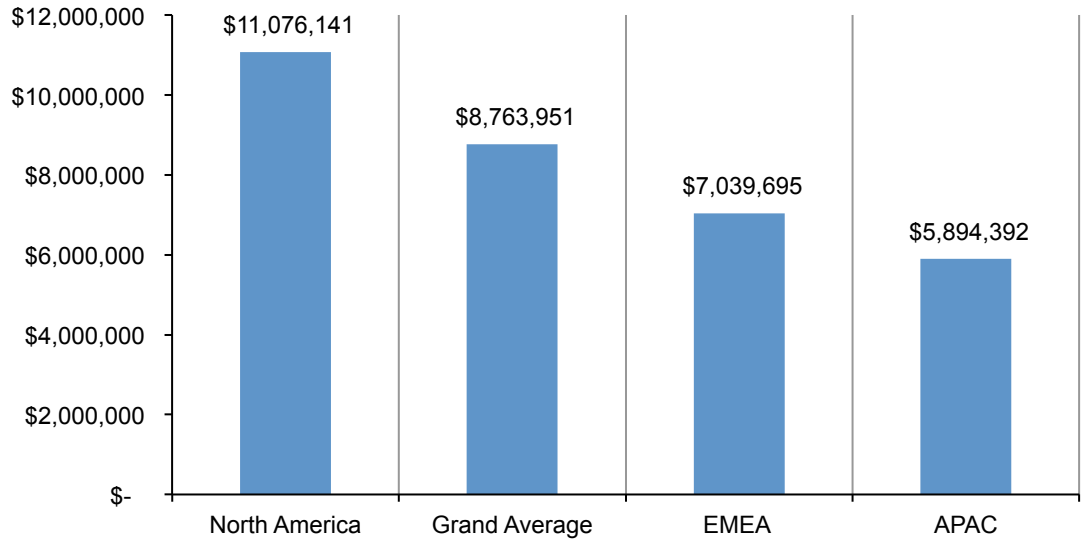
Total annualized cost appears to be positively correlated with the time to contain insider-related incidents. As shown in Figure 17, incidents that took more than 90 days to contain had the highest average total cost per year. In contrast, incidents that took less than 30 days to contain had the lowest total cost.

Figure 17. Total annualized cost by time (days) to contain the insider-related incident
US$ millions



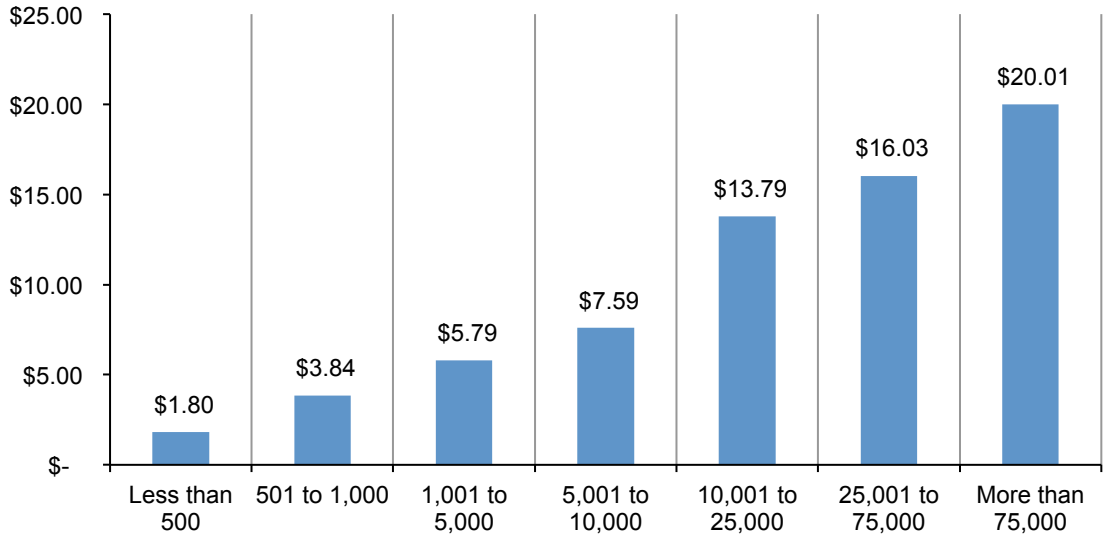
Total annualized cost for three global regions is reported in Figure 18. Companies in North America experienced the highest total cost at $11.1 million. EMEA companies had the next highest cost at $7.04 million. In contrast, APAC companies had lowest annualized costs at $5.88 million. The grand average total cost for all 159 companies is $8.76 million for insider-related incidents.

Figure 18. Total annualized cost by global region
US$ millions



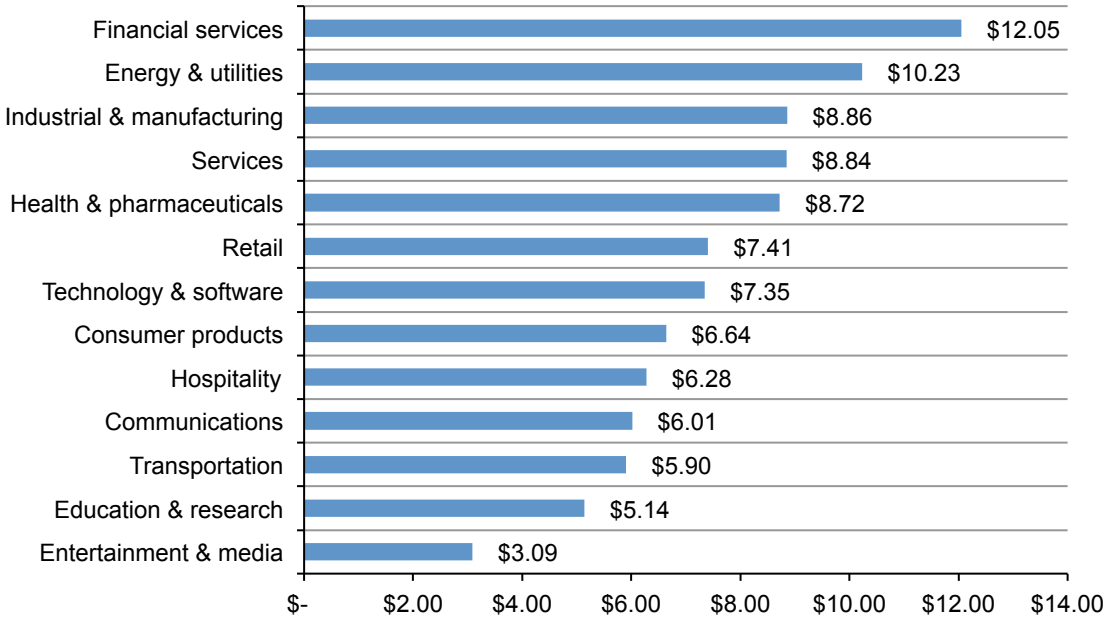
Total annualized cost adjusted for companies' worldwide headcount is reported in Figure 19. Companies with more than 75,000 employees experienced the highest total cost at $20.01 million, while those with fewer than 500 employees had the lowest annualized cost at $1.80 million.

Figure 19. Total annualized cost by global headcount (size)
US$ millions



Total annualized cost for 13 industry sectors is reported in Figure 20.[2] At $12.05 million, companies in financial services experienced the highest total cost. Energy & utilities and retail had the next highest costs at $10.23 million and $8.86 million, respectively. In contrast, companies in entertainment and media had the lowest total annualized cost at $3.09 million.

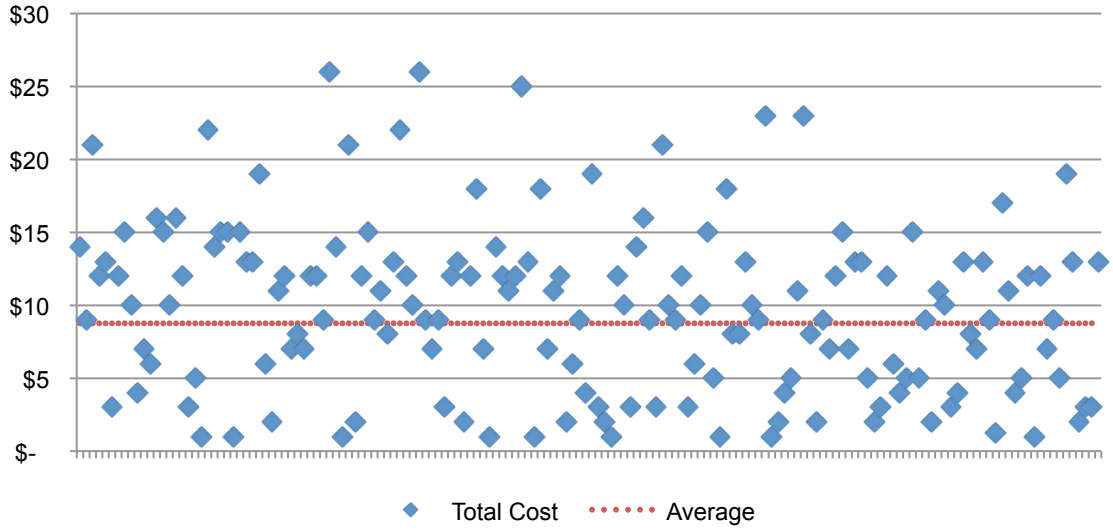
Figure 20. Total annualized cost by industrial sector
US$ millions



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

Figure 21 shows a scattergram on the total annualized cost of insider incidents per company. As can be seen, 86 companies (54 percent) at or below an average total cost of $8.76 over the past 12 months. The remaining 73 companies (46 percent) are above the average

Figure 21. Scattergram on the total cost of insider-related incidents for 159 companies
Consolidated for three profiles



Part 5. 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.[3]

This study addresses the core process-related activities that drive a range of expenditures associated with a company's response to insider-related incidents. The seven internal cost activity centers in our framework include:[4]

- **Monitoring and surveillance**: Activities that enable an organization to reasonably detect and possibly deter insider incidents or attacks. This includes allocated (overhead) costs of certain enabling technologies that enhance mitigation or early detection.
- **Investigation**: Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents.
- **Escalation**: Activities taken to raise awareness about actual incidents among key stakeholders within the company. The escalation activity also includes the steps taken to organize an initial management response.
- **Incident response**: Activities relating to the formation and engagement of the incident response team including the steps taken to formulate a final management response.

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

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

- **Containment**: Activities that focus on stopping or lessening the severity of insider incidents or attacks. These include shutting down vulnerable applications and endpoints.
- **Ex-post response**: Activities to help the organization minimize potential future insider-related incidents and attacks. It also includes steps taken to communicate with key stakeholders both within and outside the company, including the preparation of recommendations to minimize potential harm.
- **Remediation**: Activities associated with repairing and remediating the organization's systems and core business processes. These include the restoration of damaged information assets and IT infrastructure.

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

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

Part 6. Benchmarking

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

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

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

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

LL	_____|_____	UL

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

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

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

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

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

Field research was concluded in January 2018. 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).

Part 7. Limitations

Our study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations with this benchmark research that need to be carefully considered before drawing conclusions from findings.

- **Non-statistical results**: Our study draws upon a representative, non-statistical sample of organizations experiencing one or more insider-related incidents during the past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.

- **Non-response**: The current findings are based on a small representative sample of benchmarks. In this study, 159 companies completed the benchmark process. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of underlying data breach cost.

- **Sampling-frame bias**: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.

- **Company-specific information**: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category.

- **Unmeasured factors**: To keep the interview script concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined.

- **Extrapolated cost results**: The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

Ponemon Institute

Advancing Responsible Information Management

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

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