2016 Cost of Insider Threats

Benchmark Study of Organizations in the United States

Sponsored by Dtex

Independently conducted by Ponemon Institute LLC

Publication Date: September 2016

2016 Cost of Insider Threats

Benchmark Study of Organizations in the United States
Ponemon Institute: September 2016

Part 1. Introduction

Ponemon Institute is pleased to present the findings of the *2016 Cost of Insider Threats* study sponsored by Dtex. The purpose of this benchmark study is to understand the direct and indirect costs that result from insider threats. 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 280 IT and IT security practitioners in 54 organizations from April to July 2016. Each organization experienced one or more material events caused by an insider. These organizations experienced a total of 874 insider incidents over the past 12 months. Our targeted organizations were business organizations with a global headcount of 1,000 or more employees located throughout the United States.

Imposter risk is the most costly

The cost ranges significantly based on the type of incident. If it involves a negligent employee or contractor, the incident can average $206,933. The average cost more than doubles if the incident involves an imposter or thief who steals credentials ($493,093). Criminal and malicious insiders cost the organizations represented in this research an average of $347,130. 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:

- Total number of benchmarked organizations = 54
- Total number of insider incidents = 874
- Total average cost = $4.3 million
- Incidents relating to negligence = 68%
- Incidents relating to criminal insider = 22%
- Incidents relating to user credential theft = 10%

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 600 (598) of the 874 incidents reported. The most expensive incidents, due to imposters stealing credentials, were the least reported and totaled 85 incidents.

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 $7.8 million to resolve the incident. To deal with the consequences of an insider incident, organizations with a headcount between 1,000 and 5,000 spent an average of $2 million. Financial services, retail, industrial and manufacturing spent an average of $5 million.

User behavior analytics combined with other tools reduce the total cost

Using incremental analysis, we recalculated the total cost of insider-related incidents under the condition that a given tool or activity is deployed across the enterprise. Companies that deploy user behavior analytics (UBA) realized an average cost reduction of $1.1 million. The use of threat intelligence systems resulted in an $0.8 million average cost reduction. Similarly, the deployment of data loss prevention (DLP) tools resulted in an average cost reduction of $0.7 million. Companies that deploy user behavior analytics in combination with threat intelligence, employee monitoring and data loss prevention have an average total cost of $2.8 million, which is $1.5 million lower than the overall average.

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 July 2016. Our final benchmark sample consisted of 54 separate organizations (or a total of 280 interviews with key personnel). 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 1,000 or more employees
- Locations throughout the United States
- 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 54 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 US-based 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 sponsor 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 include financial services, health and pharmaceutical and services. Financial service organizations include banking, insurance, investment management and brokerage. Service organizations include a wide range of companies including professional service firms.

Figure 1. Industry distribution for 54 participating organizations
n = 54 companies

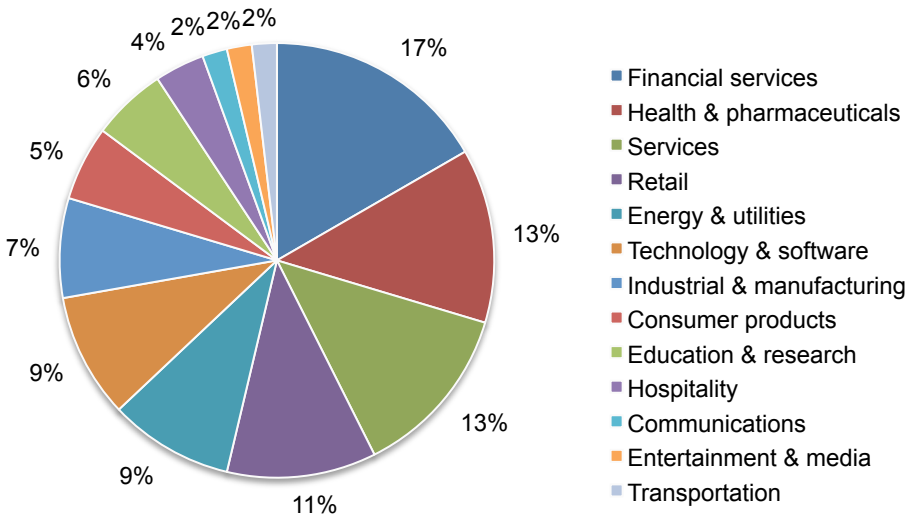
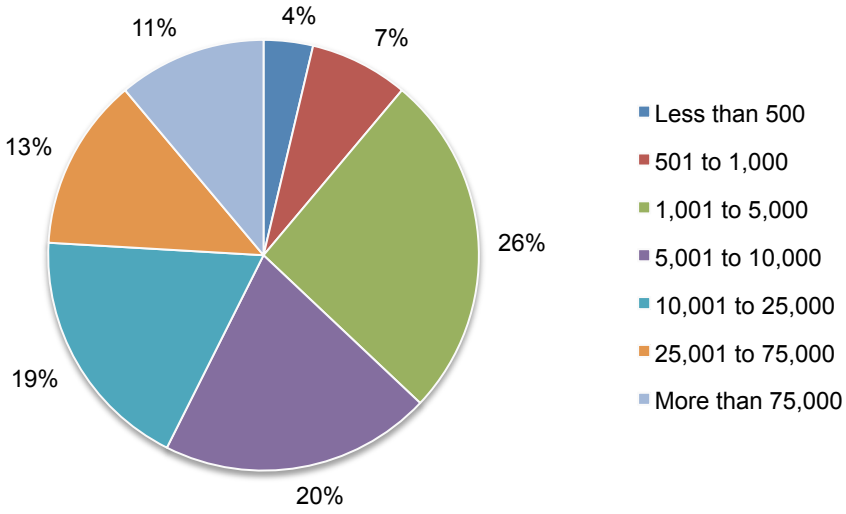


Figure 2 shows the percentage distribution of companies according to global headcount, which is a surrogate for organizational size. As can be seen, 57 percent of the sample includes larger-sized companies with more than 5,000 full-time equivalent employees.

Figure 2. Headcount of participating organizations
n = 54 companies



According to Figure 3, the three largest segments of individuals who participated in field-based interviews include security technicians, chief information security officers (CISO) and key personnel in finance and accounting.

Figure 3. Distribution of interviewees by position or function
n = 280 respondents

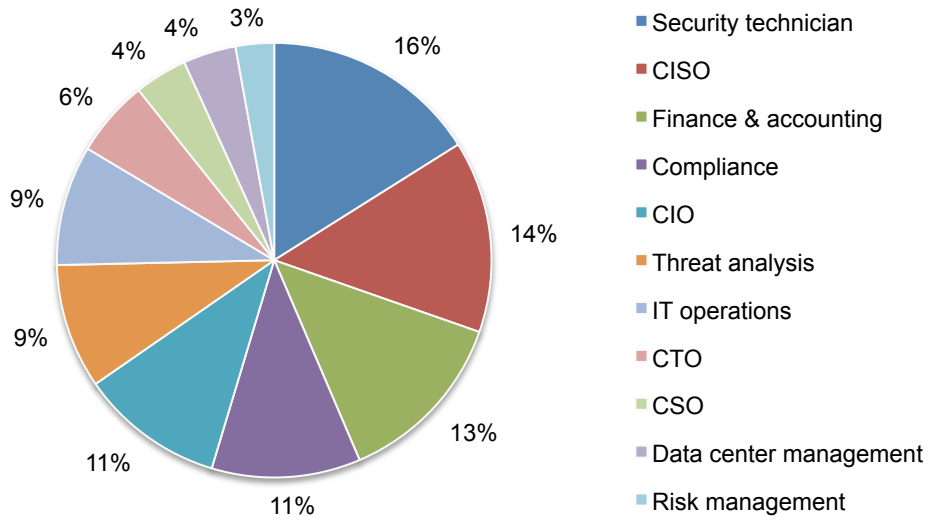
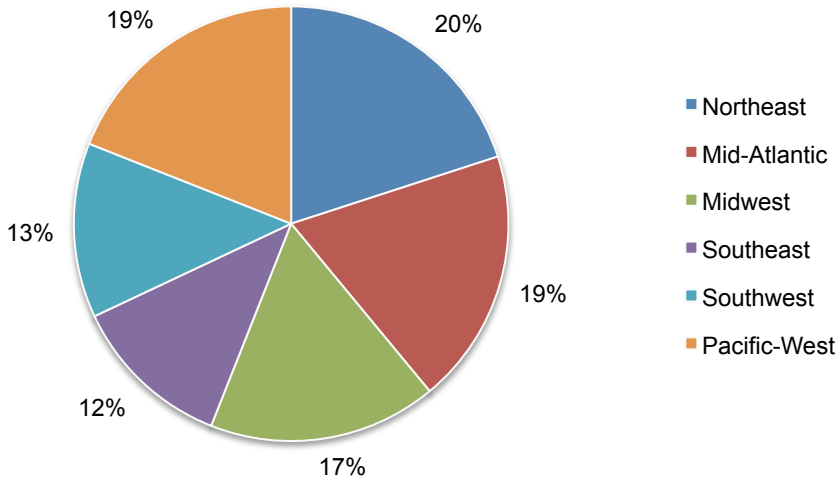


Figure 4 shows the regional location of participating companies in the United States. The largest segments include the Northeast, Mid-Atlantic and West-Pacific.

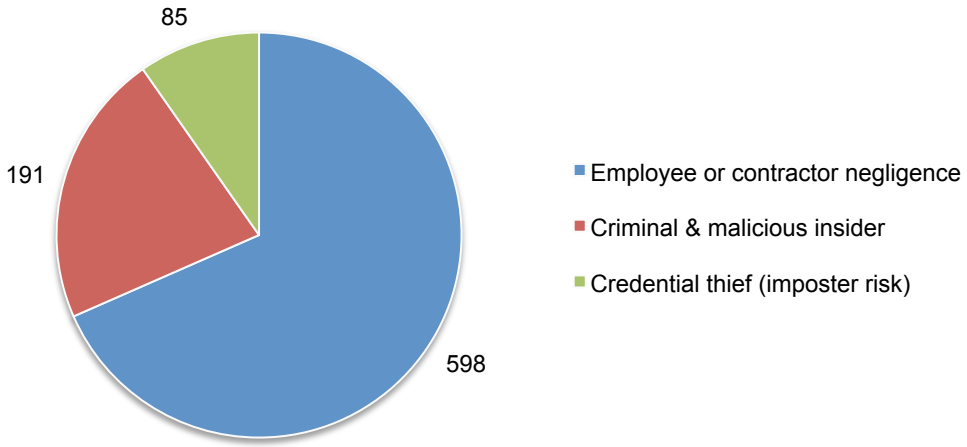
Figure 4. Regional distribution of US-based organizations
n = 54 companies



Part 3. Analysis of Insider Incidents

Figure 5 shows the distribution of 874 attacks analyzed in our sample. A total of 568 attacks (or 68 percent) pertained to employee or contractor negligence. Another 191 attacks (or 22 percent) pertained to criminal or malicious insiders. Only 85 attacks (or 10 percent) involved credential theft (a.k.a. imposter risk). The largest number of incidents for a given company is 31 and the smallest number of incidents is 1.

Figure 5. Frequency of 874 incidents for three insider profiles



Following is a graph that shows the frequency of insider incidents for our sample of 54 companies over the past 12 months. As can be seen, 15 companies experienced between 1 and 10 incidents. In contrast, only 4 companies experienced more than 25 incidents.

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

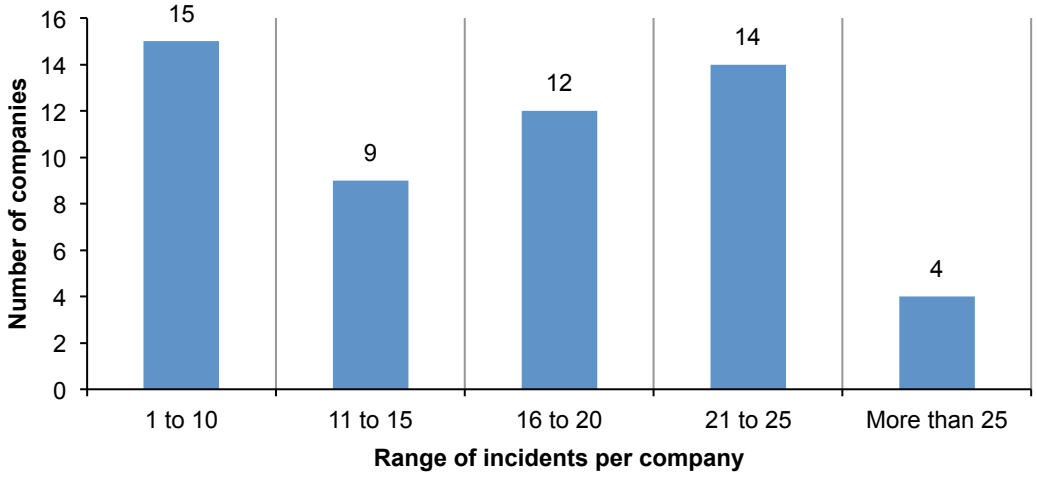
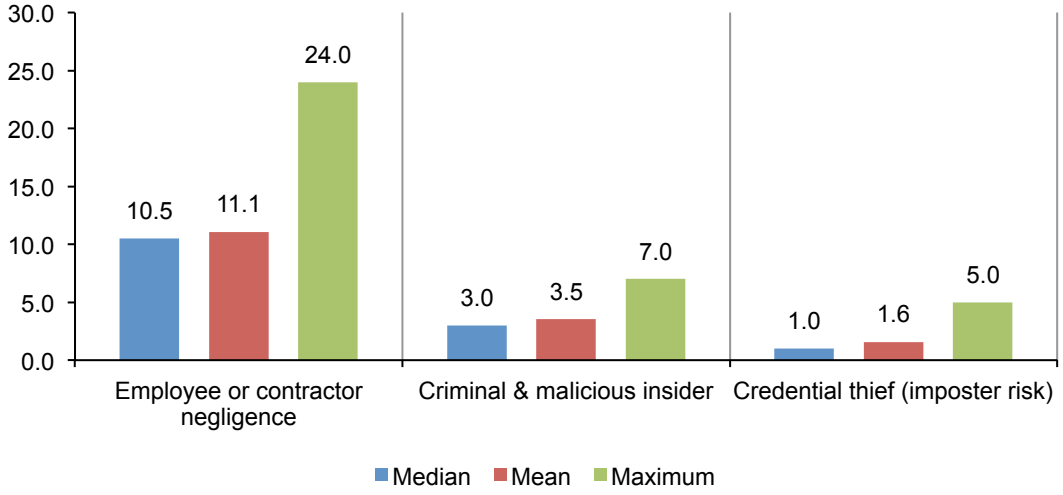


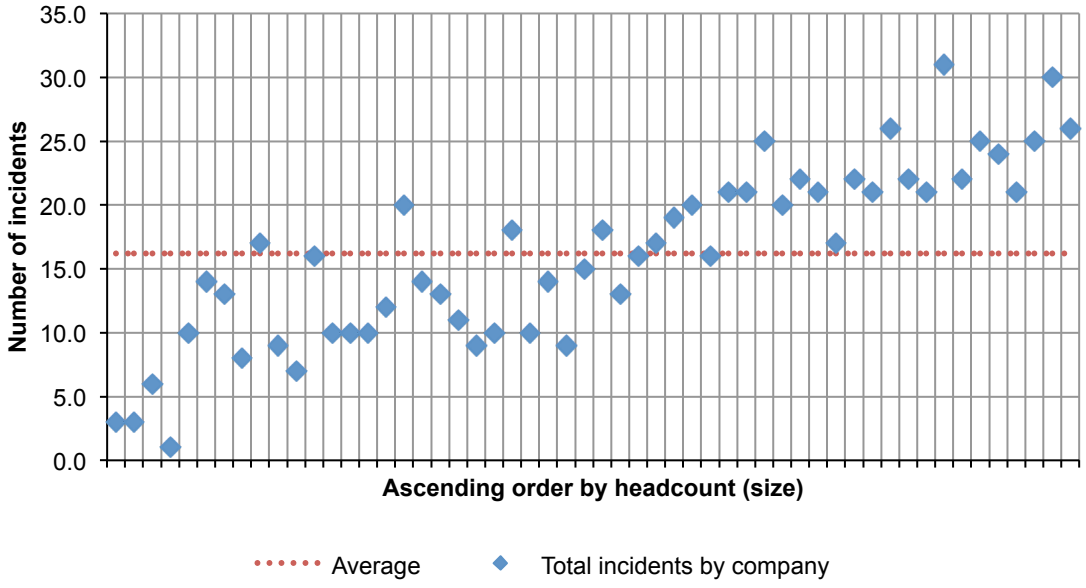
Figure 7 reports the median, mean and maximum values for incident frequency for three profiles. The mean value for employee negligence is 10.5 incidents. In contrast, the mean value for criminal and malicious insider is 3.0 incidents. The mean value for credential theft is only 1.0 incident.

Figure 7. Sample statistics on the frequency of insider-related incidents



The scattergram shown in Figure 8 shows the distribution of insider incidents in ascending order by headcount or size of the participating companies. As can be seen, the upward slope suggests that the frequency of insider incidents is highly correlated with organizational size.

Figure 8. Scattergram of insider incidents in ascending order by headcount



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, incident response and containment represents the most expensive activity centers.

Table 1. Cost activity centers	Employee or contractor negligence	Criminal & malicious insider	Credential thief (imposter risk)	Average cost
Monitoring & surveillance	$8,827	$10,119	$9,883	$9,610
Investigation	$21,883	$45,711	$56,790	$41,461
Escalation	$4,170	$11,590	$10,997	$8,919
Incident response	$47,345	$63,898	$87,868	$66,370
Containment	$44,007	$107,881	$216,500	$122,796
Ex-post analysis	$7,983	$8,131	$9,381	$8,498
Remediation	$72,718	$99,800	$101,674	$91,397
Total	$206,933	$347,130	$493,093	$349,052

As shown in the accompanying bar chart, the most costly insider incidents involve credential theft – which is more than twice as expensive for incidents involving employee or contractor negligence.

Figure 9. Average cost per incident for three profiles

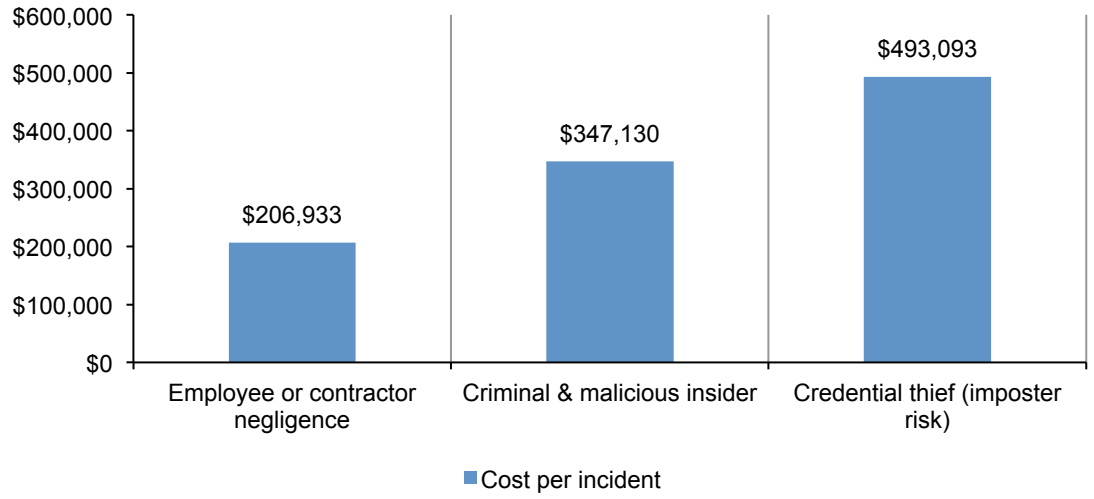


Figure 10 reports the extrapolated annualized insider-related costs for three profiles. In terms of total annual costs, it is clear that employee or contractor negligence represents the most expensive insider profile. While credential theft is the most expensive on a unit cost basis, it represents the least expensive profile on an annualized basis.

Figure 10. Average annualized cost for three profiles

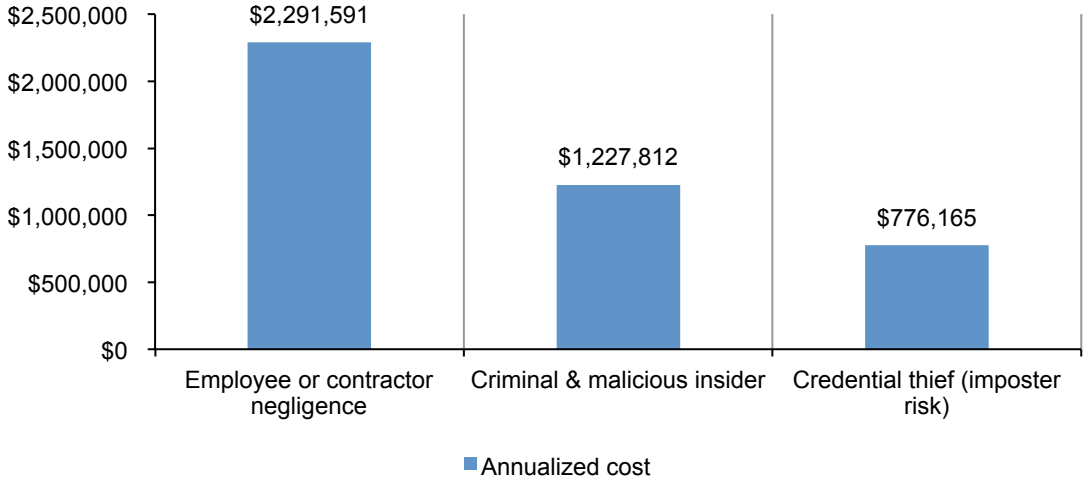


Figure 11 reports the median, mean, minimum and maximum values for insider cost (combining three profiles) over the past 12 months. The mean and median are $4.3 million and $4.6 million, respectively. The minimum cost value is $.35 million and the maximum cost value is $17.2 million.

Figure 11. Sample statistics on the cost of insider incidents over the past 12 months
Consolidated for three profiles

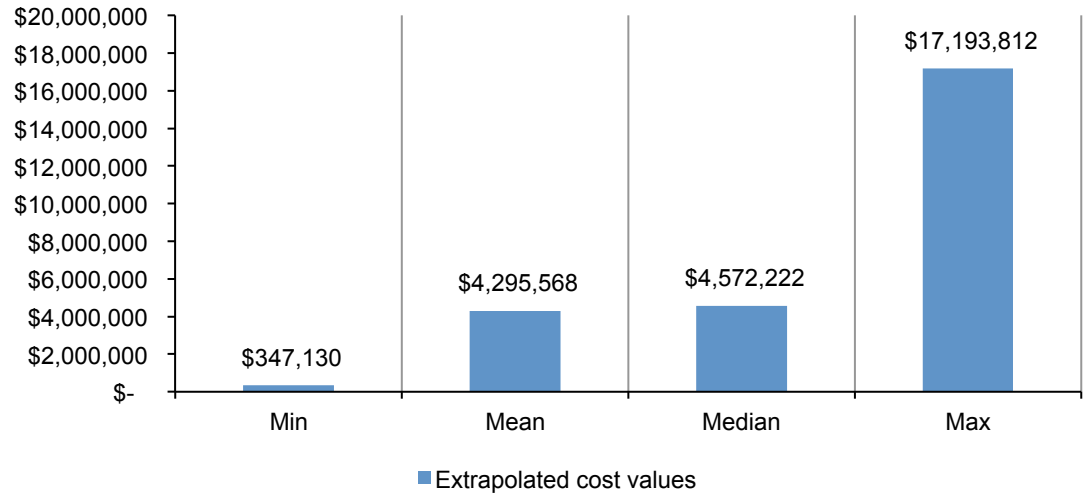
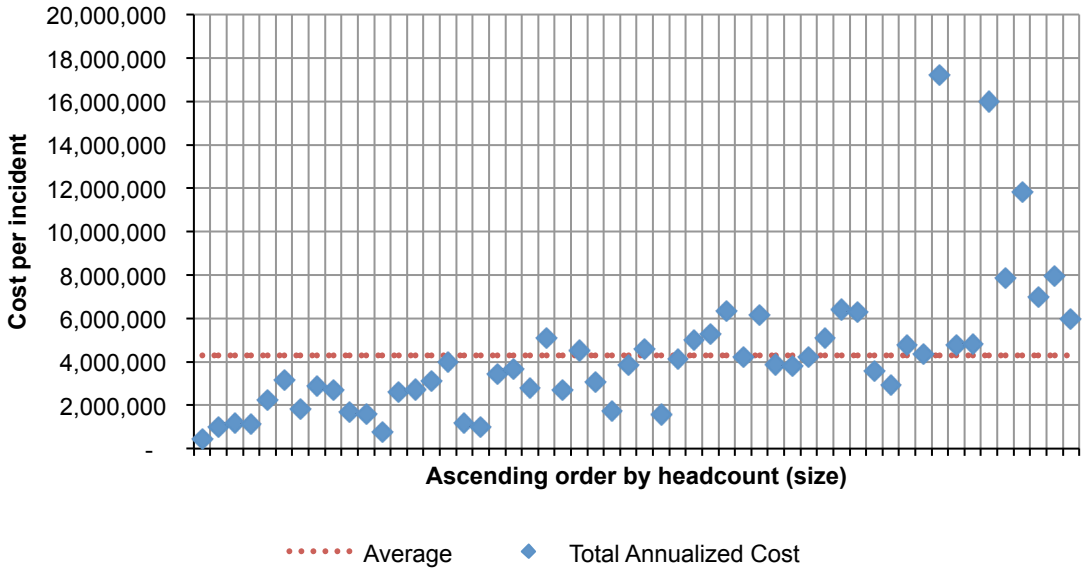


Figure 12 shows a scattergram on the total annualized cost of insider incidents per company in ascending order by headcount or size. The upward slope of the graph suggests that the cost of insider incidents is highly correlated with size.

Figure 12. Scattergram on the total cost of insider incidents in ascending order by headcount



The following pie chart shows the percentage cost for seven activity centers. As can be seen, remediation represents 31 percent of total annualized insider-related costs. Activities relating to containment and incident response represent 28 percent and 21 percent of total annualized cost, respectively.

Figure 13. Percentage cost of insider incidents by activity center

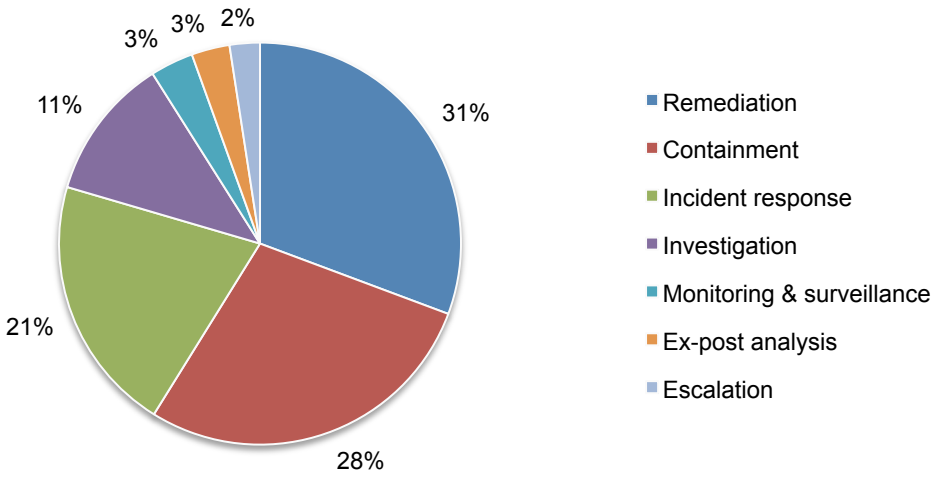
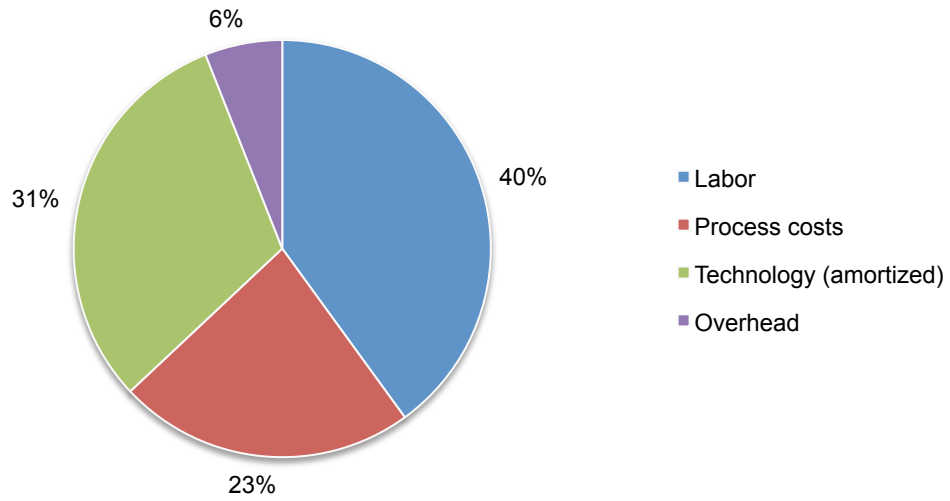


Figure 14 reports the percentage of insider cost by standard accounting categories. Labor includes both direct and indirect costs associated with in-house personnel plus temporary and contract workers. Process costs include governance and control system activities in response threats and attacks. This category also includes the cost of disruption and diminished employee/user productivity as a result of insider incidents.

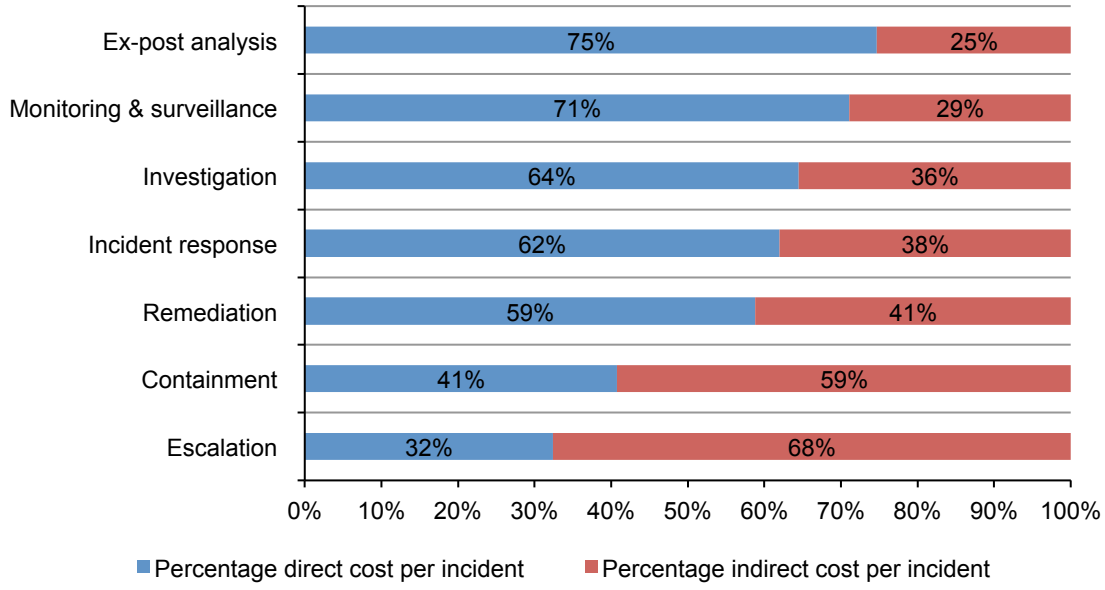
Technology costs include the amortized value plus licensing fees for software and hardware that are deployed in response to insider-related incidents. Overhead includes a wide array of miscellaneous costs incurred to support personnel as well as the IT security infrastructure.

Figure 14. Percentage of insider cost by standard category



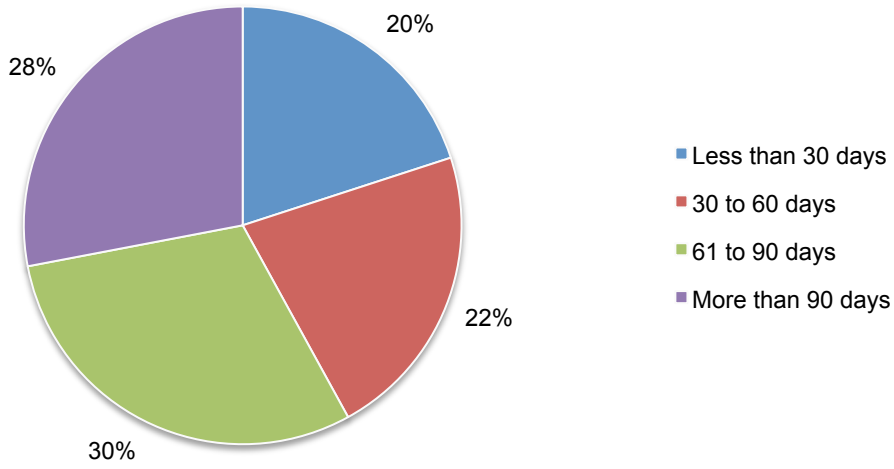
The next bar chart shows the proportion of direct and indirect costs for seven internal activity centers. As can be seen, ex-post response has the highest direct cost percentage. In contrast, escalation has the highest percentage of indirect cost.

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



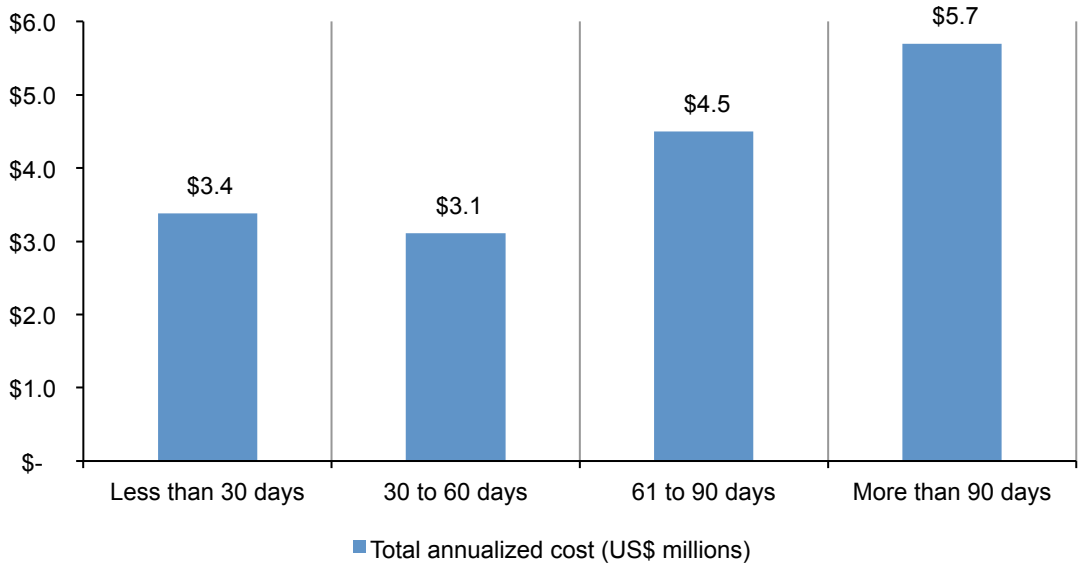
The following pie chart shows the time to contain 874 insider-related incidents in our benchmark sample. As can be seen, it took more than 60 days to contain the incident or attack for 58 percent of our sample. Another 20 percent experienced containment within 30 days.

Figure 16. Percentage distribution of insider-related incidents based on the time to contain
Average = 65.4 days



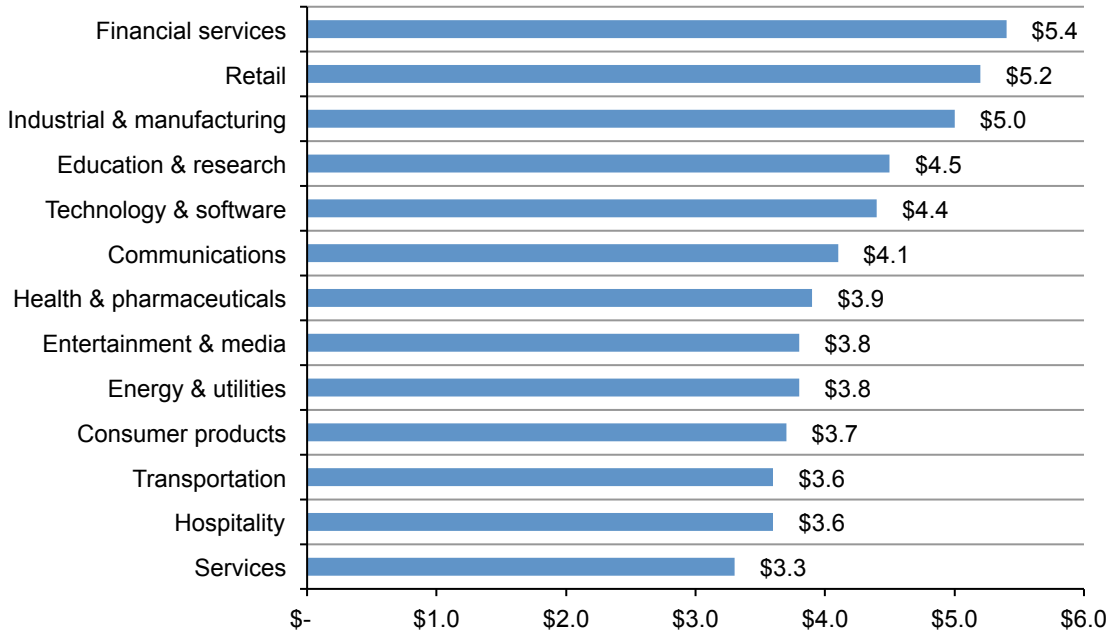
Total annualized cost appears to be positively correlated with the time to contain insider-related incidents. As shown in Figure 17, incidents that took more than 90 days to contain experienced the highest total cost. In contrast, incidents that took between 30 to 60 days to contain had the lowest total cost.

Figure 17. Total annualized cost by time (days) to contain the incident



Total annualized cost for 13 industry sectors is reported in Figure 18. At $5.3 million, companies in financial services experienced the highest total cost. Retail organizations experienced the second highest cost at $5.2 million. At $3.3 million and $3.6 million, companies in services and hospitality have the lowest total cost.

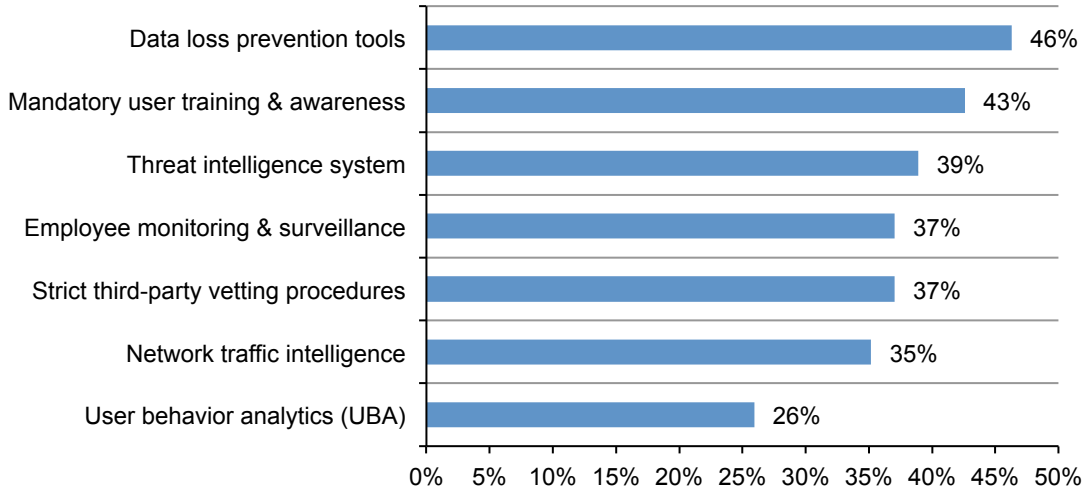
Figure 18. Total annualized cost by industrial sector[1]
US$ millions



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

Figure 19 lists seven tools and activities that attempt to reduce insider risk. The percentage indicates the proportion of the sample that uses each tool or activity. As can be seen, the use of data loss prevention tools and mandatory user training are most frequently deployed. In contrast, user behavior analytics has the lowest deployment rate.

Figure 19. Tools and activities that reduce insider risk



The adjusted total cost of insider-related incidents for each tool or activity is listed in Figure 20. Using incremental analysis, we recalculate the total cost under the condition that each tool or activity is deployed across the enterprise. For example, companies that have mandatory user training realize an average total cost at $4.0 million, which is $300,000 lower than the overall average at $4.3 million. Similarly, companies that deploy user behavior analytics have an average total cost of $3.2 million, which is $1.1 million lower than the overall average.

Figure 20. Adjusted total cost resulting from the use of risk reducing tools and activities
US$ millions

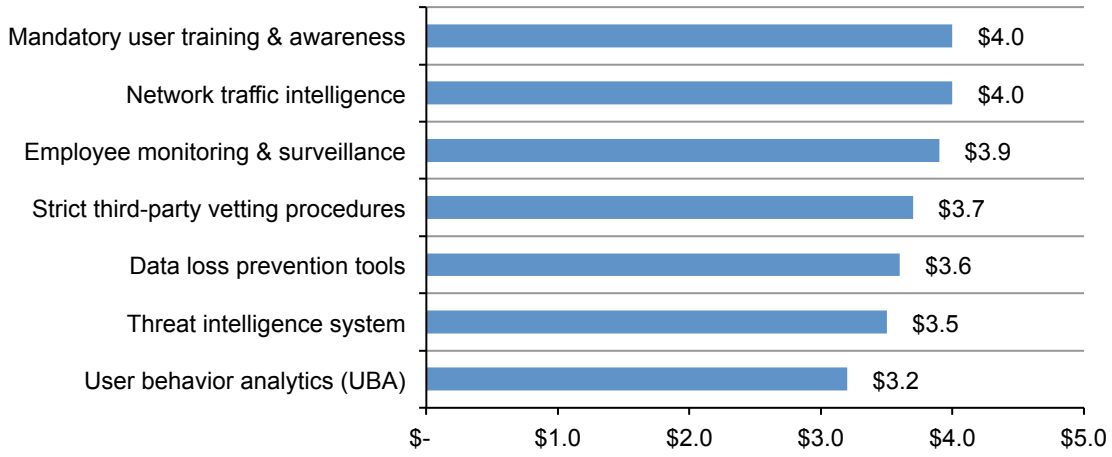
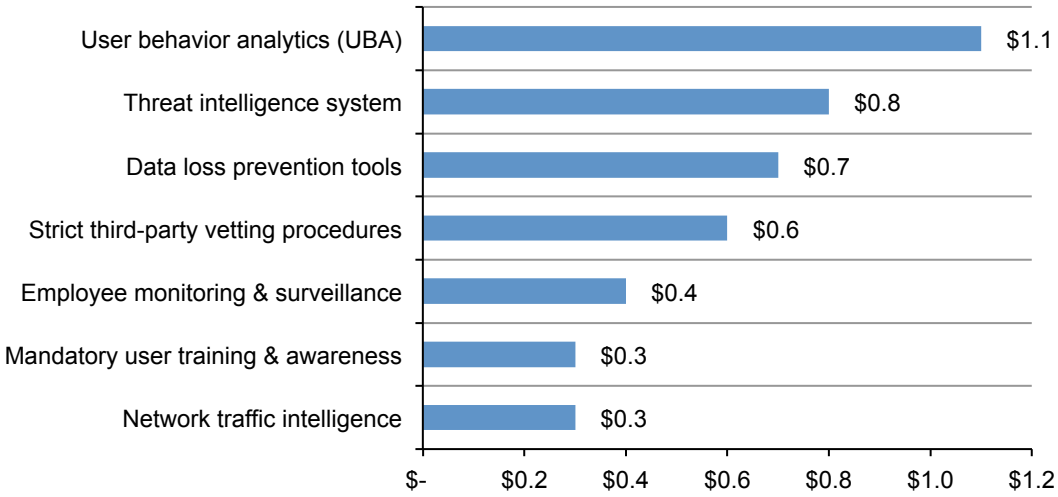


Figure 21 shows the incremental cost savings that result from the deployment of each one of seven risk-reducing tools and activities. Cost savings are defined as the mean value ($4.3 million) minus adjusted cost (reported in Figure 20). As can be seen, UBA provides the largest cost savings at $1.1 million, which is followed by threat intelligence at $0.8 million and data loss prevention at $0.7 million in cost savings.

Figure 21. Incremental cost savings from the use of risk-reducing tools and activities
Mean value minus adjusted cost
US$ millions



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 consequences 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, which involves dealing with 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, including 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.[2]

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:[3]

- 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.

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

[3] 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.

- 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 we 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 conducted over several months concluding in July 2016. 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, indirect and opportunity costs of cost 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, 54 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.

As a member of the **Council of American Survey Research Organizations (CASRO)**, 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.