



# 2015 Cost of Cyber Crime Study: Global

---

**Sponsored by Hewlett Packard Enterprise**

Independently conducted by Ponemon Institute<sup>LLC</sup>

Publication Date: October 2015

## 2015 Cost of Cyber Crime Study: Global

Benchmark Study of Global Companies

Ponemon Institute October 2015

### Part 1. Executive Summary

We are pleased to present the *2015 Cost of Cyber Crime Study: Global*, sponsored by Hewlett Packard Enterprise. This year's study is based upon a representative sample of 252 organizations in seven countries.

Ponemon Institute conducted the first *Cost of Cyber Crime* study in the United States six years ago. This is the fourth year we conducted the study in the United Kingdom, Germany, Australia and Japan and the second year the research was conducted in the Russian Federation. This year we added Brazil. The findings from seven countries are presented in separate reports.

The number of cyber attacks against global governments and commercial enterprises continues to grow in frequency and severity. To combat increasing cyber crime, the Global Cyber Alliance (GCA), an international, cross-sector effort was recently established to confront, address and prevent malicious cyber activity.

Partners who have joined the Alliance include leaders from security, defense, retail, healthcare, insurance, energy, aviation, education, law enforcement, government and finance institutions, including American Express, Barclays Bank, Citibank, US Bank and the Financial Services ISAC.<sup>1</sup>

#### Global Study at a Glance

252 companies in 7 countries

2,128 interviews with company personnel

1,928 total attacks used to measure total cost

\$7.7 million is the average annualized cost

1.9 percent net increase over the past year

15 percent average ROI for 7 security technologies

For purposes of this study, we refer to cyber attacks as criminal activity conducted via the Internet. These attacks can include stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet and disrupting a country's critical national infrastructure.

Our goal is to quantify the economic impact of cyber attacks and observe cost trends over time. We believe a better understanding of the cost of cyber crime will assist organizations in determining the appropriate amount of investment and resources needed to prevent or mitigate the consequences of an attack.

In our experience, a traditional survey approach does not capture the necessary details required to extrapolate cyber crime costs. Therefore, we conduct field-based research that involves interviewing senior-level personnel about their organizations' actual cyber crime incidents. Approximately 10 months of effort is required to recruit companies, build an activity-based cost model to analyze the data, collect source information and complete the analysis.

For consistency purposes, our benchmark sample consists of only larger-sized organizations (i.e., a minimum of approximately 1,000 enterprise seats<sup>2</sup>). The study examines the total costs organizations incur when responding to cyber crime incidents. These include the costs to detect, recover, investigate and manage the incident response. Also covered are the costs that result in after-the-fact activities and efforts to contain additional costs from business disruption and the loss of customers. These costs do not include the plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

<sup>1</sup> "Global Cyber Alliance Is Formed—Aims to Combat Increasing Cybercrime," by Ryan Daws, *TelecomsTech*, 16 September, 2015

<sup>2</sup> Enterprise seats refer to the number of direct connections to the network and enterprise systems.

## Global at a glance

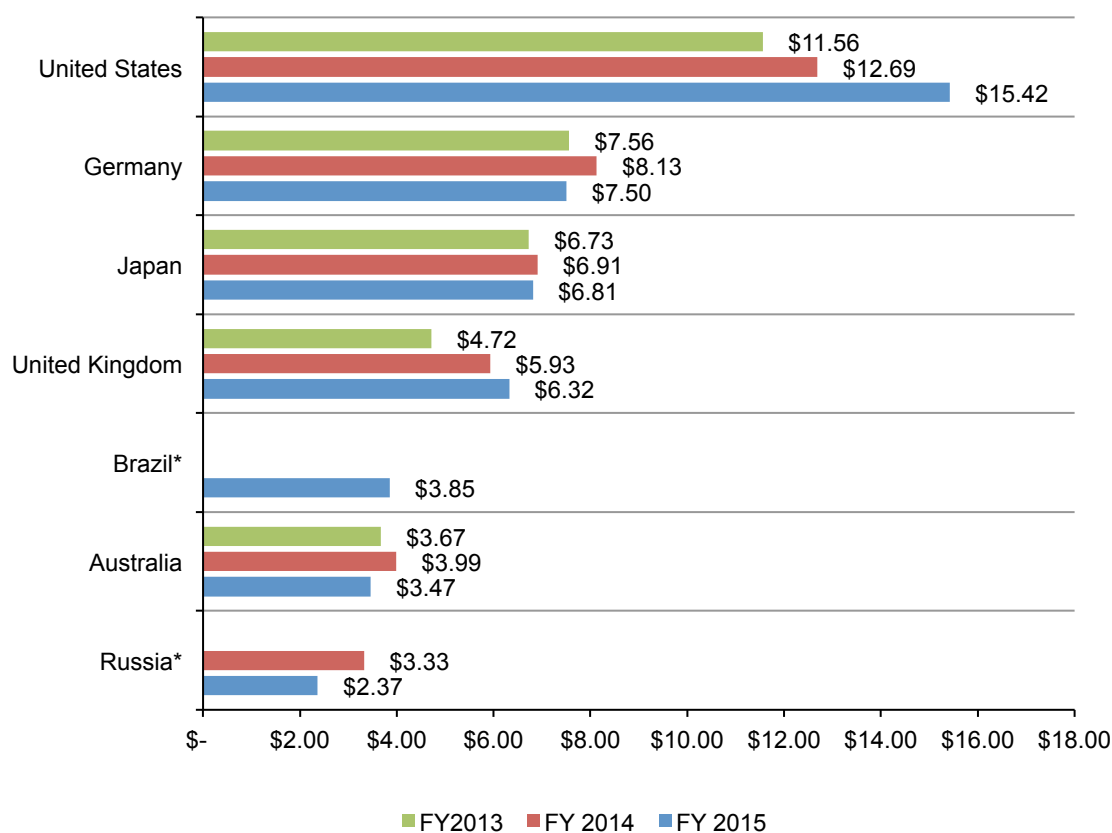
This year's annual study was conducted in the United States, United Kingdom, Germany, Australia, Japan, Russian Federation and, for the first time, Brazil with a total benchmark sample of 252 organizations. Country-specific results are presented in seven separate reports.

Figure 1 presents the estimated average cost of cyber crime for seven country samples involving 252 separate companies, with comparison to last year's country averages. Cost figures are converted into US dollars for comparative purposes.<sup>3</sup>

As shown, there is significant variation in total cyber crime costs among participating companies in the benchmark samples. The US sample reports the highest total average cost at \$15 million and the Russian sample reports the lowest total average cost at \$2.4 million. It is also interesting to note that Germany, Japan, Australia and Russia experienced a slight decrease in the cost of cyber crime cost over the past year. However, this finding is due to exchange rate differences over the past year resulting from a strong U.S. dollar relative to other local currencies. Hence, adjusting for exchange rate differences, we actually see a net increase in total cyber crime costs in all countries. The percentage net change between FY 2015 and FY 2014 in U.S. dollars (excluding Brazil) is 1.9 percent.

### Figure 1. Total cost of cyber crime in seven countries

Cost expressed in US dollars (000,000), n = 252 separate companies



\* Results were not available for all fiscal years

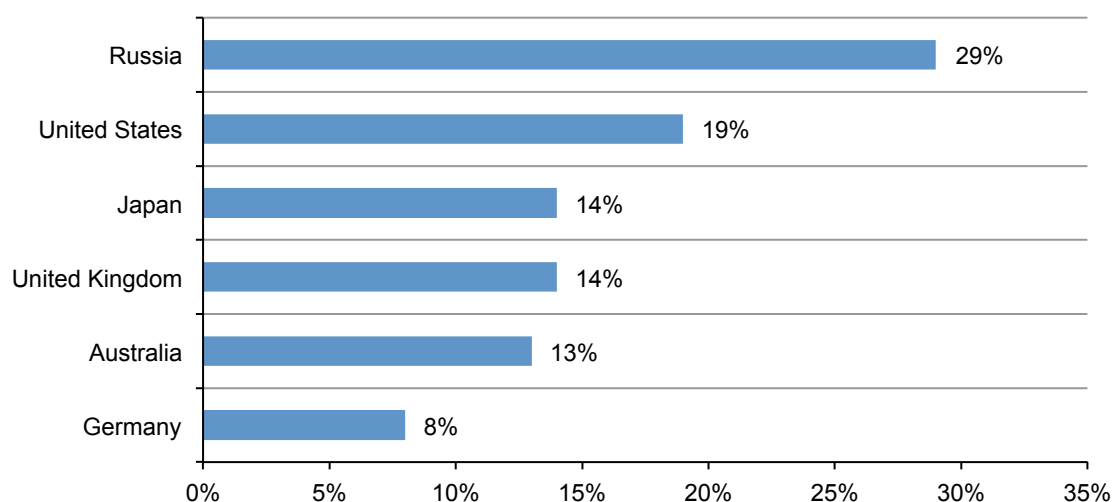
<sup>3</sup>The Wall Street Journal's September 14, 2015 currency conversion rates.

Figure 2 summarizes the net change in cyber crime costs between 2014 and 2015 as measured in local currencies. As can be seen, the most significant increase in total cyber crime cost occurs in Russia and the United States at 29 percent and 19 percent, respectively. At 8 percent, Germany has the lowest increase in the total annual cost.

**Figure 2. One-year net change in cyber crime in six countries**

Net change could not be calculated for Brazil

n = 252 separate companies



## Summary of global findings

Following are the most salient findings for a sample of 252 organizations requiring 2,128 separate interviews to gather cyber crime cost results. In several places in this report, we compare the present findings to last year's average of benchmark studies.

**Cyber crimes continue to be on the rise for organizations.** We found that the mean annualized cost for 252 benchmarked organizations is \$7.7 million per year, with a range from \$0.31 million to \$65 million. Last year's mean cost was \$7.6 million, or a 1.9 percent net change after adjustment for currency differences (excluding the Brazilian sample). As shown in Figure 2, the one-year net change as measured in local currencies is 13.9 percent.

**Cyber crime cost varies by organizational size.** Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost.<sup>4</sup> However, based on enterprise seats, we determined that small organizations incur a significantly higher per capita cost than larger organizations (\$1,388 versus \$431).

**All industries fall victim to cybercrime, but to different degrees.** The average annualized cost of cyber crime appears to vary by industry segment, where organizations in financial services and utilities & energy experience substantially higher cyber crime costs than organizations in healthcare, automotive and agriculture.

**The most costly cyber crimes are those caused by malicious insiders, denial of services and web-based attacks.** Mitigation of such attacks requires enabling technologies such as SIEM, intrusion prevention systems, applications security testing solutions and enterprise GRC solutions.

**Cyber attacks can get costly if not resolved quickly.** Results show a positive relationship between the time to contain an attack and organizational cost. Please note that resolution does not necessarily mean that the attack has been completely stopped. For example, some attacks remain dormant and undetected (i.e., modern day attacks). The mean number of days to resolve cyber attacks is 46 with an average cost of \$21,155 per day – or a total cost of \$973,130 over the 46-day remediation period.

**Business disruption represents the highest external cost, followed by the costs associated with information loss.**<sup>5</sup> On an annualized basis, business disruption accounts for 39 percent of total external costs, which include costs associated with business process failures and lost employee productivity.

**Detection is the most costly internal activity followed by recovery.** On an annualized basis, detection and recovery costs combined account for 53 percent of the total internal activity cost with productivity loss and direct labor representing the majority of these costs.

**Activities relating to IT security in the network layer receive the highest budget allocation.** In contrast, the host layer receives the lowest funding level.

**Deployment of security intelligence systems makes a difference.** The cost of cyber crime is moderated by the use of security intelligence systems (including SIEM). Findings suggest companies using security intelligence technologies were more efficient in detecting and containing cyber attacks. As a result, these companies enjoyed an average cost savings of \$1.9 million when compared to companies not deploying security intelligence technologies.

---

<sup>4</sup>In this study, we define an enterprise seat as one end-user identity/device connected to the company's core networks or enterprise systems.

<sup>5</sup>In the context of this study, an external cost is one that is created by external factors such as fines, litigation, marketability of stolen intellectual properties and more.

**Companies deploying security intelligence systems experienced a substantially higher ROI (at 23 percent) than all other technology categories presented.** Also significant are the estimated ROI results for companies that extensively deploy encryption technologies (21 percent) and advanced perimeter controls such as UTM, NGFW, IPS with reputation feeds (20 percent).

**Deployment of enterprise security governance practices moderates the cost of cyber crime.** Companies that employ expert staff can reduce cyber crime costs by an average of \$1.5 million and those that appoint a high-level security leader reduce costs by an average of \$1.3 million. Please note that these extrapolated cost savings are independent of each other and cannot be added together.



## Part 2. Key findings

In this section, we provide an analysis of the key findings organized according to the following topics:

- The average cost of cyber crime by organizational size and industry
- The type of attack influences the cost of cyber crime
- An analysis of the cost components of cyber crime

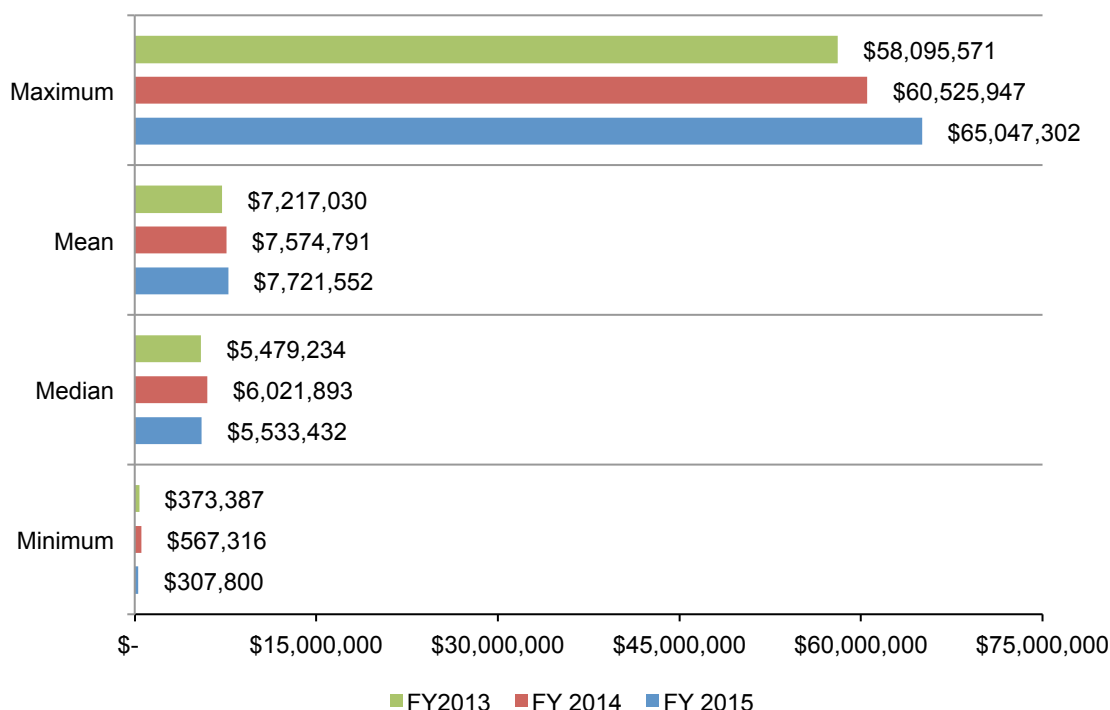
### The average cost of cyber crime by organizational size and industry

To determine the average cost of cyber crime, the 252 organizations in the study were asked to report what they spent to deal with cyber crimes experienced over four consecutive weeks. Once costs over the four-week period were compiled and validated, these figures were then grossed-up to determine the annualized cost.<sup>6</sup>

As shown in Figure 3, the total annualized cost of cyber crime in 2015 ranges from a low of \$.31 million to a high of \$65 million. The median annualized cost of cyber crime in the benchmark sample is \$5.5 million – a slight decrease from \$6 million in 2014. The mean value is \$7.7 million. A slight increase from last year's mean of \$7.6 million. The percentage net change from last year's mean for seven countries is 1.9 percent.

### Figure 3. The cost of cyber crime

Consolidated view, n = 252 separate companies  
Cost expressed in US dollars

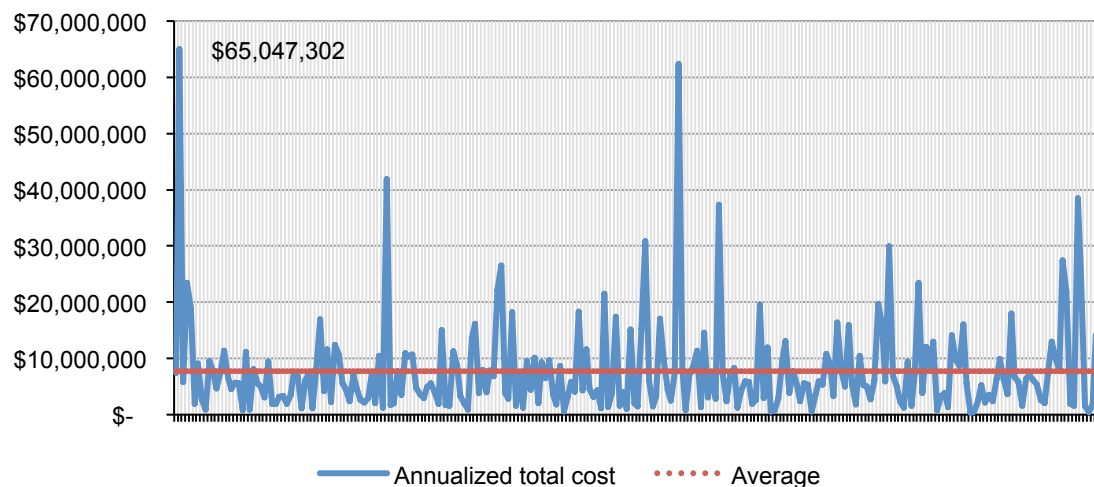


<sup>6</sup>Following is the gross-up statistic: Annualized revenue = [cost estimate]/[4/52 weeks].

Figure 4 reports the distribution of annualized total cost for 252 companies. As can be seen, 90 companies in our sample incurred total costs above the mean value of \$7.7 million, thus indicating a skewed distribution. The highest cost estimate of \$65 million was determined not to be an outlier based on additional analysis. A total of 162 organizations experienced an annualized total cost of cyber crime below the mean value.

**Figure 4. Annualized total cost of cyber crime for 252 participating companies**

Cost expressed in US dollars

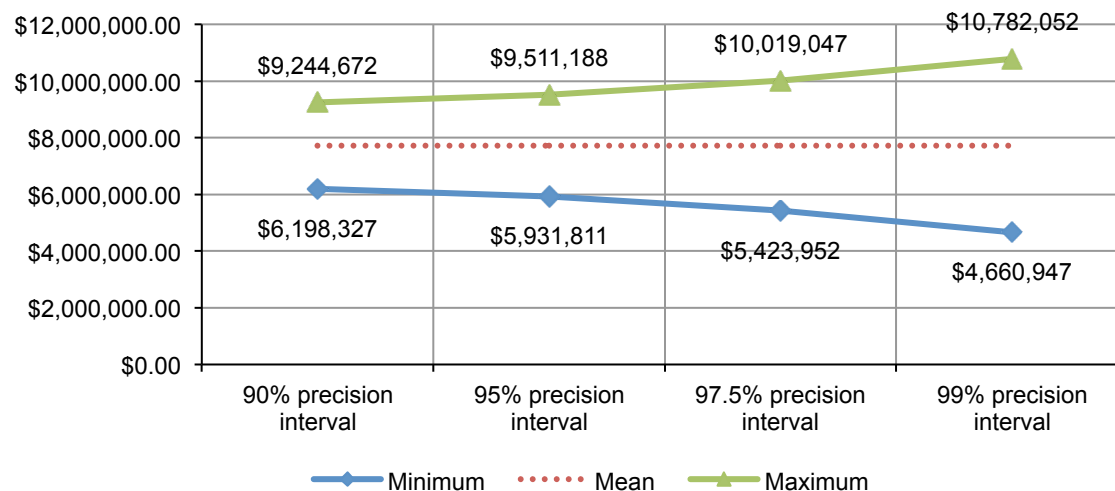


As part of our analysis we calculated a precision interval for the average cost of \$7.7 million. The purpose of this interval is to demonstrate that our cost estimates should be thought of as a range of possible outcomes rather than a single point or number.

The range of possible cost estimates widens at increasingly higher levels of confidence, as shown in Figure 5. Specifically, at a 90 percent level of confidence we expect the range of cost to be between \$6.2 million to \$9.2 million.

**Figure 5. Precision interval for the mean value of annualized total cost**

Cost expressed in US dollars

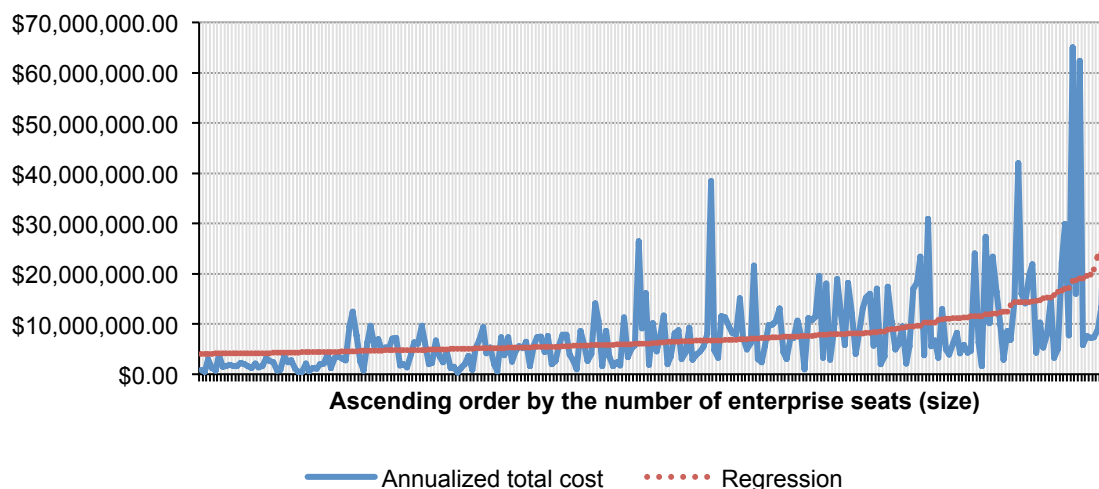




**The cost of cyber crime varies by organizational size.** As shown in Figure 6, organizational size, as measured by the number of enterprise seats or nodes, is positively correlated to annualized cyber crime cost. This positive correlation is indicated by the upward slopping regression line. The number of seats ranges from a low of 673 to a high of 79,367.

**Figure 6. Annualized cost in ascending order by the number of enterprise seats**

Cost expressed in US dollars



Organizations are placed into one of four quartiles based on their total number of enterprise seats (which we use as a size surrogate). We do this to create a more precise understanding of the relationship between organizational size and the cost of cyber crime. Table 1 shows the quartile average cost of cyber crime for three years. Approximately 63 companies are in each quartile.

Table 1. Quartile analysis Cost expressed in US dollars	FY 2015 (n=252)	FY 2014 (n=257)	FY 2013 (n=234)
Quartile 1 (smallest)	\$3,279,376	\$2,967,723	\$2,965,464
Quartile 2	\$5,246,519	\$5,107,532	\$4,453,688
Quartile 3	\$8,987,450	\$8,321,024	\$6,659,478
Quartile 4 (largest)	\$13,372,861	\$13,805,529	\$14,707,980

Table 2 reports the average cost per enterprise seat (a.k.a. per capita cost) compiled for four quartiles ranging from the smallest (Quartile 1) to the largest (Quartile 4). Consistent with prior years, the 2015 average per capita cost for organizations with the fewest seats is approximately four times higher than the average per capita cost for organizations with the most seats (\$1,555 vs. \$368).

Table 2. Quartile analysis Cost expressed in US dollars	2015 cost per seat	2014 cost per seat	2013 cost per seat
Quartile 1 (smallest)	\$1,555	\$1,601	\$1,388
Quartile 2	\$878	\$962	\$710
Quartile 3	\$709	\$726	\$532
Quartile 4 (largest)	\$368	\$437	\$431

**Certain attacks are more costly based on organizational size.** The study focuses on nine different attack vectors as the source of the cyber crime. In Figure 7, we compare smaller and larger-sized organizations based on the sample median of 8,703 seats. Smaller organizations (below the median) experience a higher proportion of cyber crime costs relating to web-based attacks; phishing & social engineering; malware; viruses, worms, trojans; and botnets.

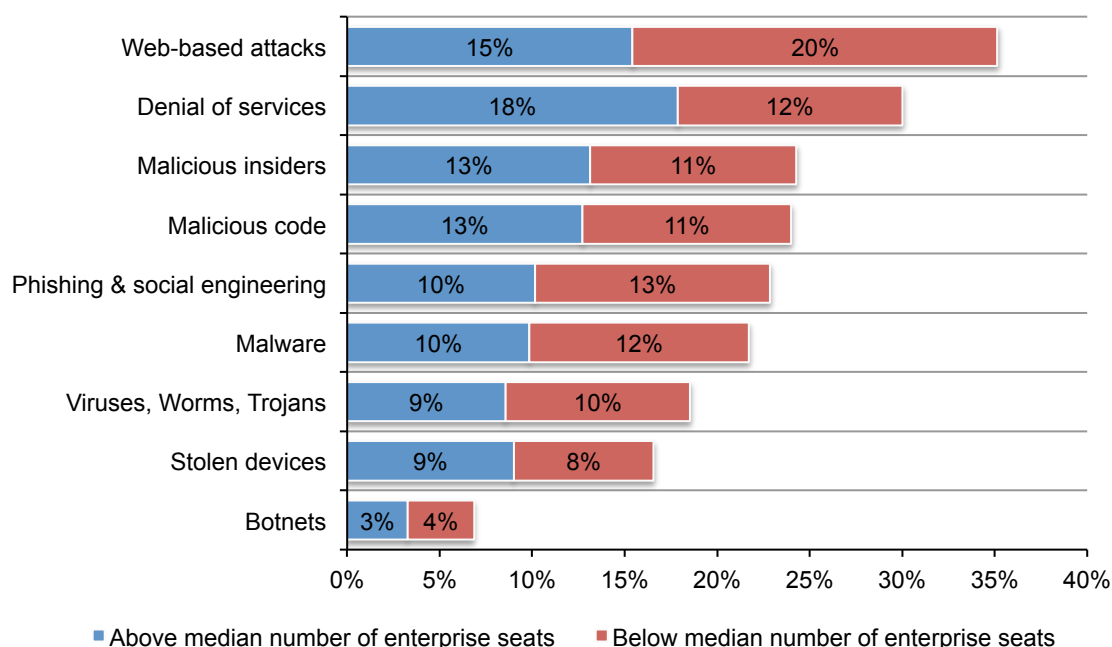
In contrast, larger organizations (above the median) experience a higher proportion of costs relating to denial of services, malicious insiders, malicious code and stolen devices. In the context of this research, malicious insiders include employees, temporary employees, contractors and, possibly other business partners.

We also distinguish viruses from malware. Viruses reside on the endpoint and as yet have not infiltrated the network but malware has infiltrated the network. Malicious code attacks the application layer and includes SQL attack.

**Figure 7. Organizational size affects the cost of dealing with nine attack types**

Size measured according to the number of enterprise seats within the participating organizations

Consolidated view, n = 252 separate companies

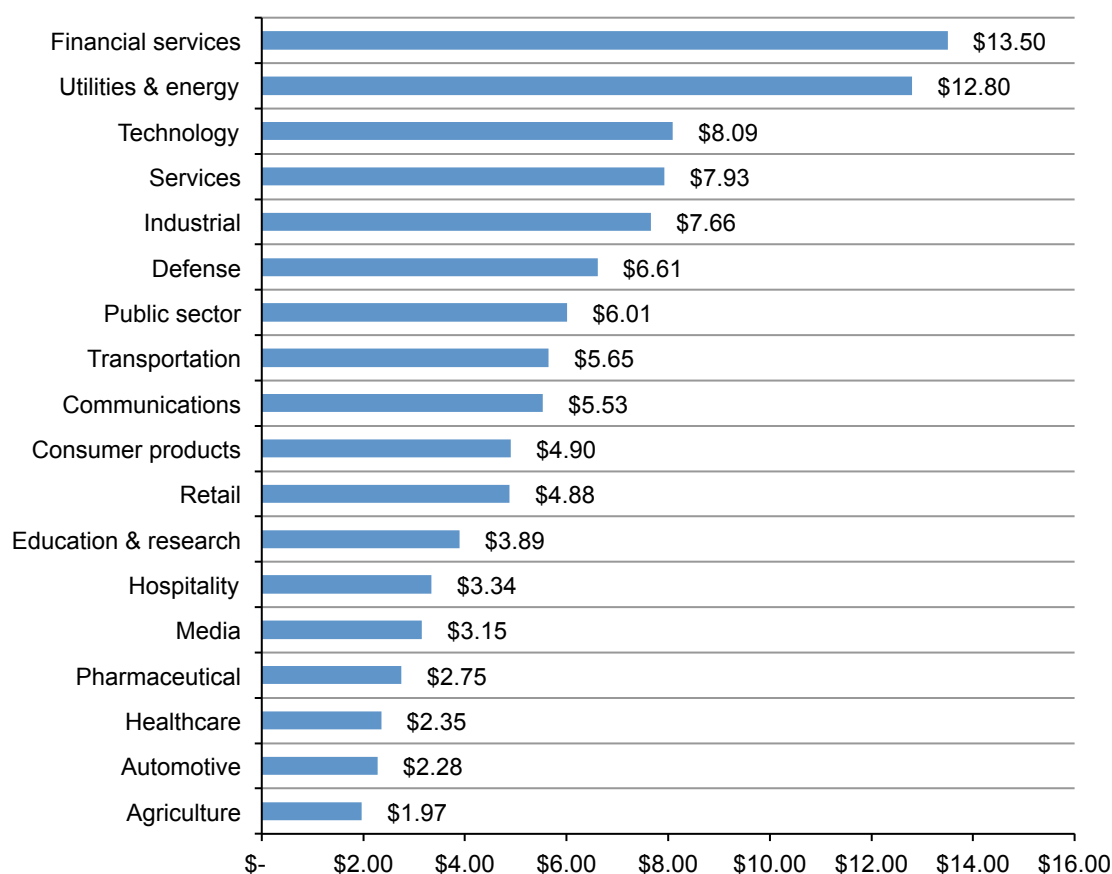


**The cost of cyber crime impacts all industries.** The average annualized cost of cyber crime appears to vary by industry segment. In this year's study we compare cost averages for 18 different industry sectors. As shown in Figure 8, the cost of cyber crime for companies in financial services and utilities & energy experienced the highest annualized cost. In contrast, companies in healthcare, automotive and agriculture incurred a much lower cost on average.<sup>7</sup>

**Figure 8. Average annualized cost by industry sector**

Cost expressed in US dollars, \$1,000,000 omitted

Consolidated view, n = 252 separate companies



<sup>7</sup>This analysis is for illustration purposes only. The sample sizes in several sectors are too small to make definitive conclusions about industry differences.

## The type of cyber attack influences the cost of cyber crime

In our studies we look at 9 different attack vectors as the source of the cyber crime. This year, the benchmark sample of 252 organizations experienced a total of 477 discernible cyber attacks. The list below shows the number of successful attacks for the past four years, which has steadily increased.

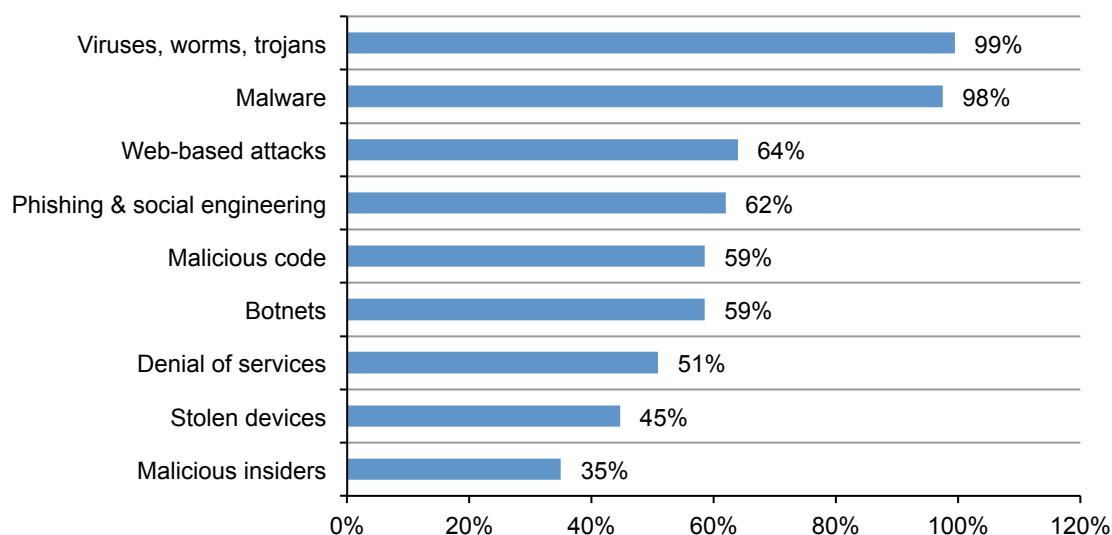
- FY 2015, 477 attacks in 252 organizations or 1.9 successful attacks per company each week
- FY 2014, 429 attacks in 257 organizations or 1.7 successful attacks per company each week
- FY 2013, 343 attacks in 234 organizations or 1.4 successful attacks per company each week
- FY 2012, 262 attacks in 199 organizations or 1.3 successful attacks per company each week

Figure 9 summarizes in percentages the types of attack methods experienced by participating companies. Virtually all organizations had attacks relating to viruses, worms and/or trojans and malware over the four-week benchmark period. Malware attacks and malicious code attacks are inextricably linked. We classified malware attacks that successfully infiltrated the organizations' networks or enterprise systems as a malicious code attack.

Sixty-four percent experienced web-based attacks and 62 percent experienced phishing & social engineering attacks. Most companies also experienced malicious code and botnets (both 59 percent) and denial of service attacks (51 percent). Only 35 percent of companies say a malicious insider was the source of the cyber crime.

**Figure 9. Types of cyber attacks experienced by 252 benchmarked companies**

Consolidated view, n = 252 separate companies



**Costs vary considerably by the type of cyber attack.** Figure 10 compares benchmark results for seven countries, showing the proportion of annualized cost of cyber crime allocated to nine attack types compiled from all benchmarked organizations.

Malicious code is the most costly problem for US companies. Countries with the highest costs related to denial of services attacks are the UK and Australia. Malware is most costly in the Russian Federation. In most countries, botnets are the least costly type of attack.

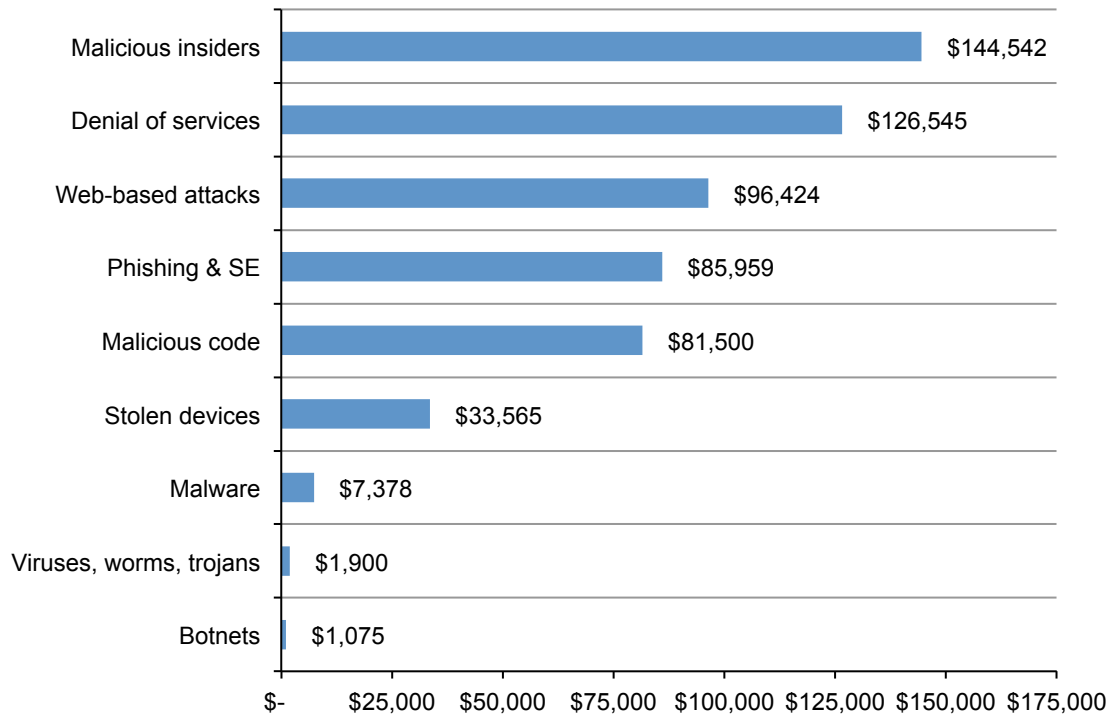
**Figure 10. Percentage annualized cyber crime cost by attack type**

Consolidated view, n = 252 separate companies



**The cost of cyber crime is also influenced by the frequency of attacks.** Figure 11 reveals the most to least expensive cyber attacks when analyzed by the frequency of incidents. The most expensive attacks are malicious insiders, denial of service and web-based attacks.

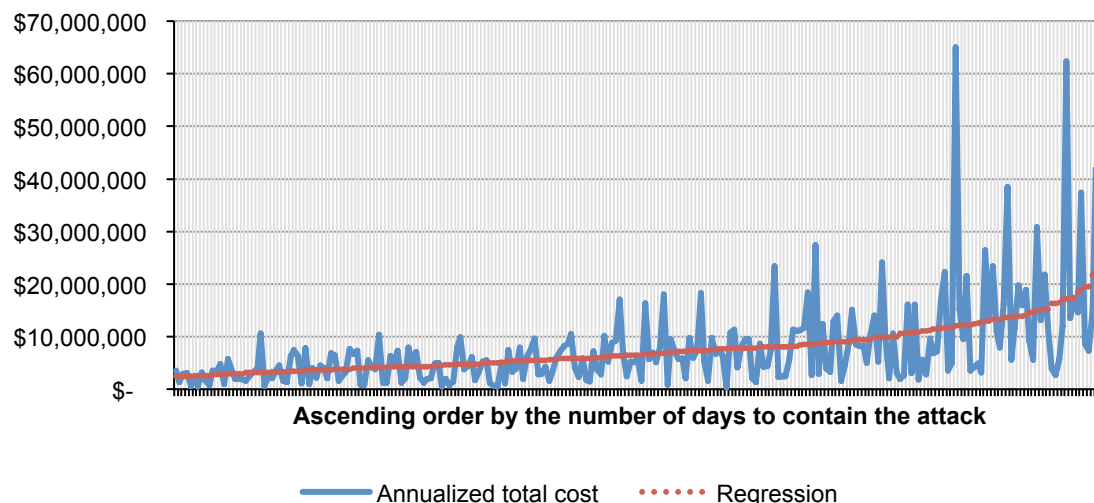
**Figure 11. Average annualized cyber crime cost weighted by attack frequency**  
Consolidated view, n = 252 separate companies



**Time to resolve or contain cyber crimes increases the cost.** The mean number of days to resolve cyber attacks is 46 with an average cost of \$21,155 per day – or a total cost of \$973,130 over the 46-day remediation period. Please note that resolution does not necessarily mean that the attack has been completely stopped. For example, some attacks remain dormant and undetected (i.e., modern day attacks).

Figure 12 shows the annualized cost of cyber crime in ascending order by the average number of days to resolve attacks. The regression line shows an upward slope, which suggests cost and time variables are positively related.

**Figure 12. Total annualized cost by the number of days to contain the attack**



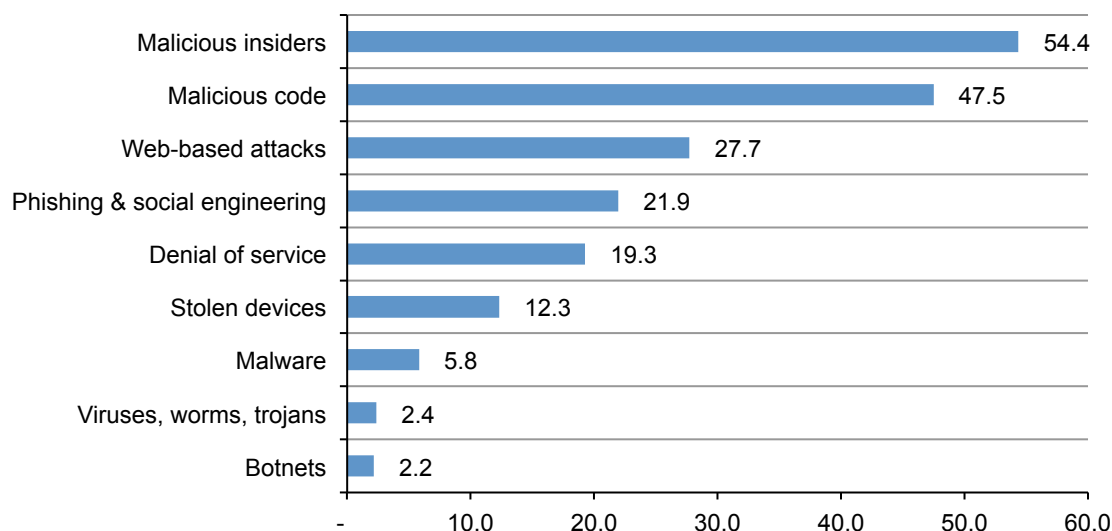


**Some attacks take longer to resolve and as a result are more costly.** As shown, the time it takes to resolve the consequences of the attack increases the cost of a cyber crime.

Figure 13 reports the average days to resolve cyber attacks for attack types studied in this report. It is clear from this chart that it takes the most amount of time, on average, to resolve attacks from malicious insiders, malicious code and web-based attackers (hackers). Malware, viruses and botnets on average are resolved relatively quickly (i.e., in a few days).

**Figure 13. Some attacks take longer to resolve**

Estimated average time is measured for each attack type in days  
Consolidated view, n = 252 separate companies



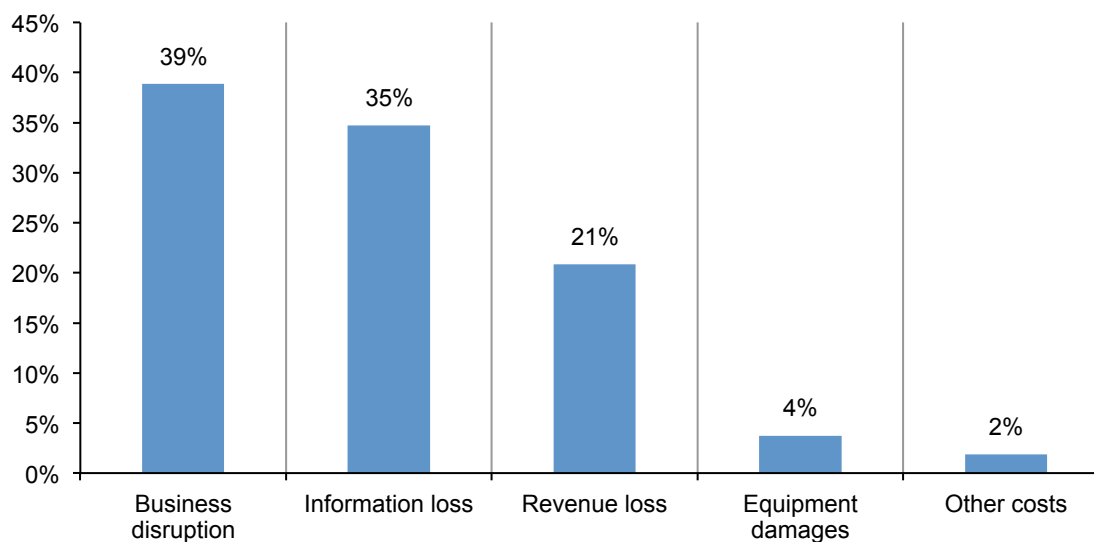
## An analysis of the cost components of cyber crime

**Information theft remains the most expensive consequence of a cyber crime.** In this research we look at four primary consequences of a cyber attack: business disruptions, the loss of information, loss of revenue and damage to equipment.

As shown in Figure 14, among the organizations represented in this study, business disruption represents the largest cost component (39 percent). The cost of business disruption includes diminished employee productivity and business process failures that happen after a cyber attack. Information and revenue loss follow at 35 percent and 21 percent, respectively.

**Figure 14. Percentage cost for external consequences**

Consolidated view, n = 252 separate companies

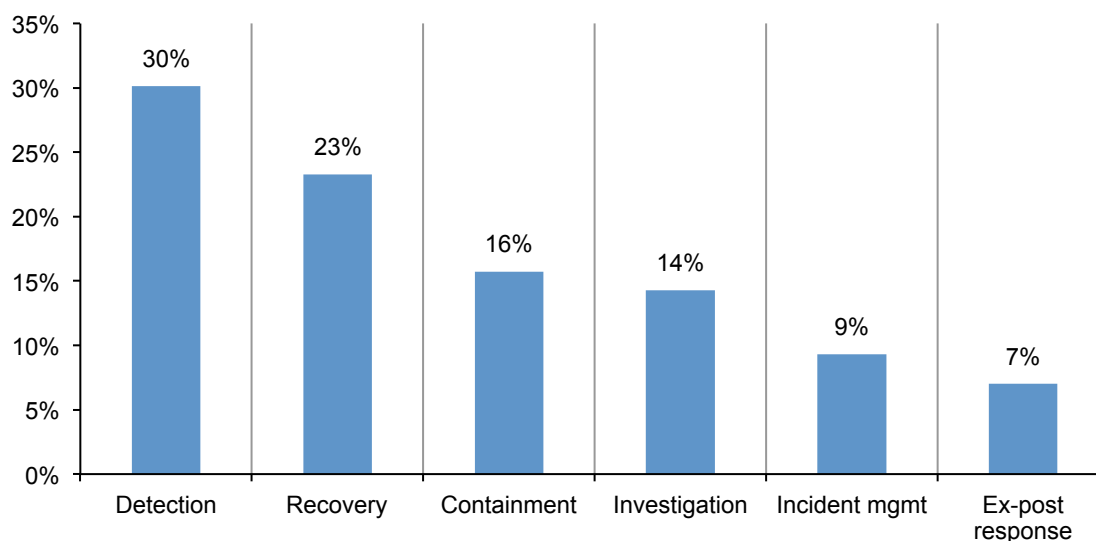


**Companies spend the most on detection and recovery.** Cyber crime detection and recovery activities account for 53 percent of total internal activity cost, as shown in Figure 15. This is followed by containment and investigation cost (at 16 percent and 14 percent, respectively).

Detection and recovery cost elements highlight a significant cost-reduction opportunity for organizations that are able to systematically manage recovery and deploy enabling security technologies to help facilitate the detection process.

**Figure 15. Percentage cost by activities conducted to resolve a cyber attack**

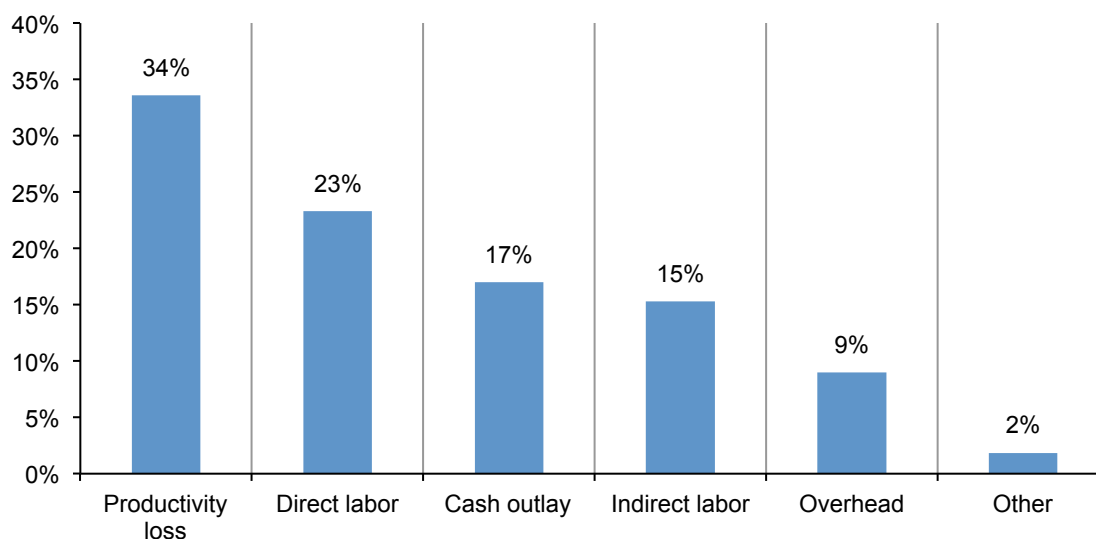
Consolidated view, n = 252 separate companies



The percentage of annualized costs can be further broken down into five specific expenditure components, which include: productivity loss (34 percent) direct labor (23 percent), cash outlays (17 percent), indirect labor (15 percent) and overhead (9 percent). Costs not included in these components are represented in the “other” category.

**Figure 16. Percentage activity cost by five specific cost components**

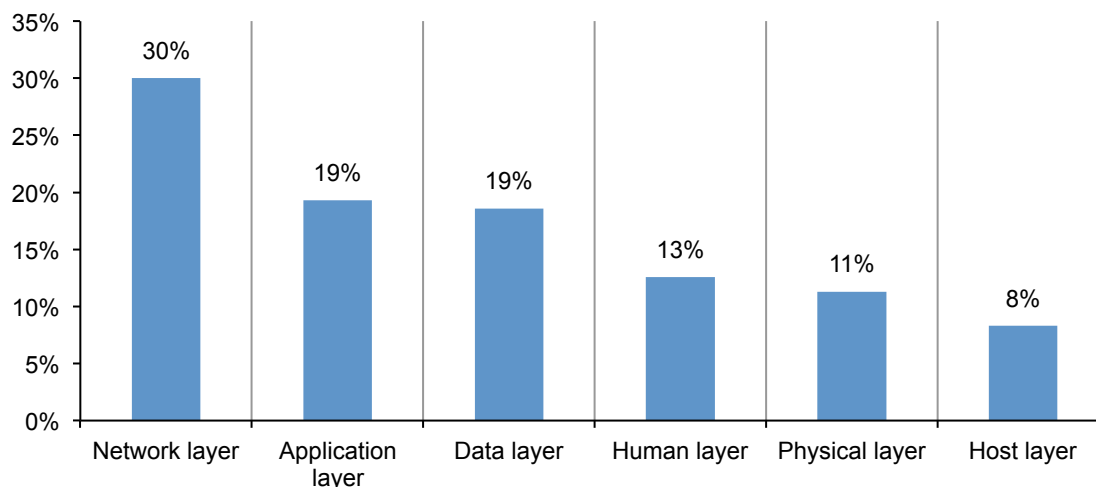
Consolidated view, n = 252 separate companies



**The largest portion of the security budget is allocated to the network layer.** Figure 17 summarizes six layers in a typical multi-layered IT security infrastructure for all benchmarked companies. Each bar reflects the percentage dedicated spending according to the presented layer. The network layer receives the highest allocation at 30 percent of total dedicated IT security funding. At only eight percent, the host layer receives the lowest funding level.

**Figure 17. Budgeted or earmarked spending according to six IT security layers**

Consolidated view, n = 252 separate companies



**Organizations deploying security intelligence technologies realize a lower annualized cost of cyber crime.** Figure 18 reveals the average amount of money companies can save with SEIM in the six activities conducted to resolve the cyber attack. The figure compares companies deploying and not deploying security intelligence systems. In total, 110 companies (44 percent) deploy security intelligence tools such as SIEM, IPS with reputation feeds, network intelligence systems, big data analytics and others.

With one exception (investigative costs), companies using security intelligence systems experience lower activity costs than companies that do not use these technologies. The largest cost differences in millions pertain to detection (\$3.42 vs. \$2.50) and containment (\$1.01 vs. \$1.28) activities.

**Figure 18. Activity cost comparison and the use of security intelligence technologies**

Cost expressed in US dollars (000,000), n = 252 separate companies

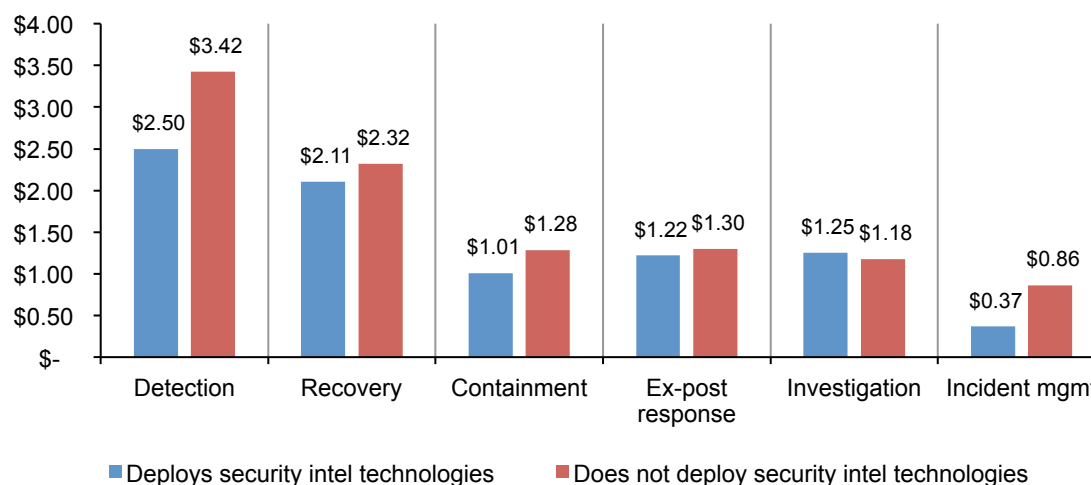


Figure 19 shows seven enabling security technology categories by a subset of benchmarked companies. Each bar represents the percentage of companies fully deploying each given security technology. The top three technology categories include: access governance tools (50 percent), security intelligence systems (44 percent) and encryption technologies (43 percent).

**Figure 19. Seven enabling security technologies deployed**

Consolidated view, n = 252 separate companies

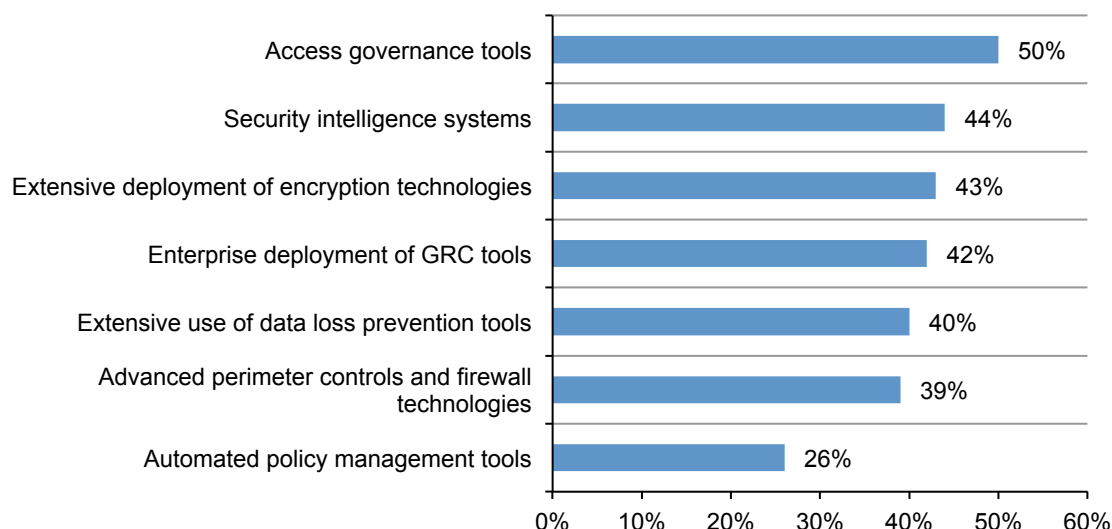
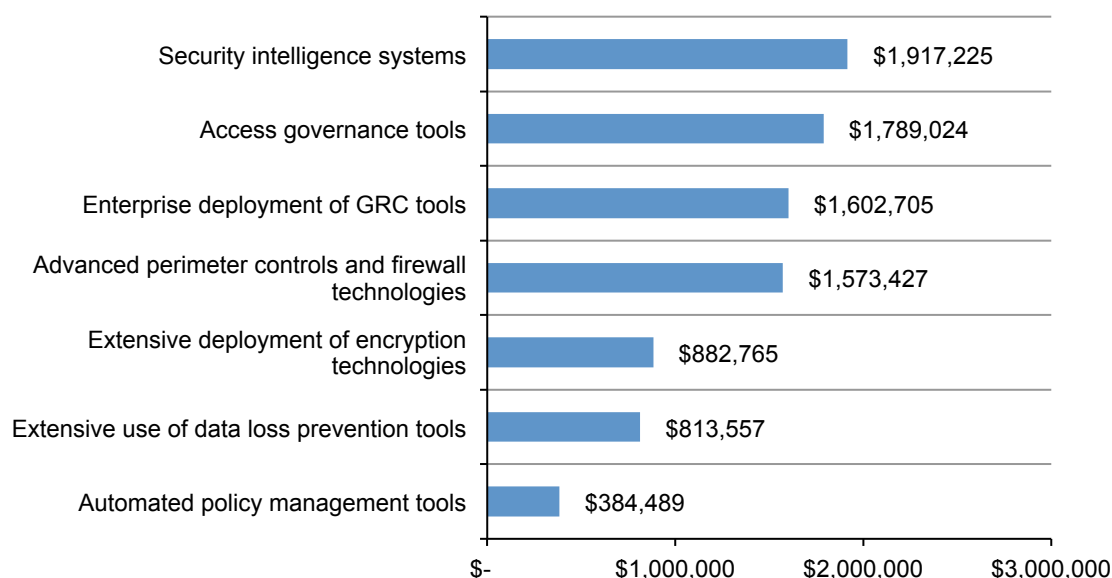


Figure 20 shows the money companies can save by deploying each one of seven enabling security technologies. For example, companies deploying security intelligence systems, on average, experience a substantial cost savings of \$1.9 million. Similarly, companies deploying access governance tools experience cost savings of \$1.8 million on average. Please note that these extrapolated cost savings are independent of each other and cannot be added together.

**Figure 20. Cost savings when deploying seven enabling technologies**

Cost expressed in US dollars. Consolidated view, n = 252 separate companies

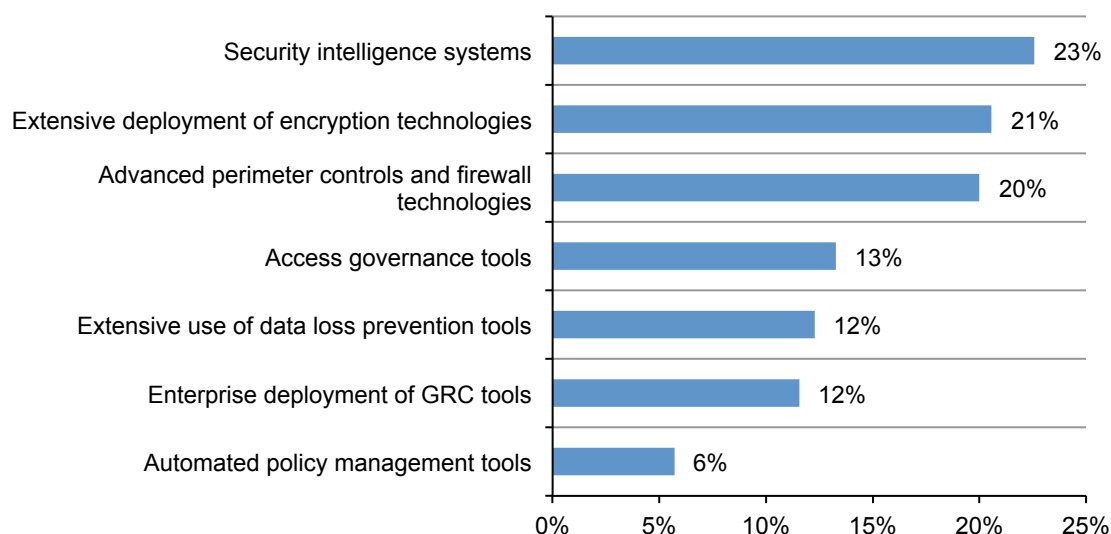


**Security intelligence systems have the biggest return on investment.** Figure 21 summarizes the estimated return on investment (ROI) realized by companies for each one of the seven categories of enabling security technologies indicated above.<sup>8</sup> At 23 percent, companies deploying security intelligence systems, on average, experience a substantially higher ROI than all other technology categories in this study.

Also significant are the estimated ROI results for companies that extensively deploy encryption technologies (21 percent) and advanced perimeter controls such as UTM, NGFW, IPS with reputation feeds and more (20 percent). The estimated average ROI for all seven categories of enabling security technologies is 15 percent.

**Figure 21. Estimated ROI for seven categories of enabling security technologies**

Consolidated view, n = 252 separate companies



<sup>8</sup>The return on investment calculated for each security technology category is defined as: (1) gains from the investment divided by (2) cost of investment (minus any residual value). We estimate a three-year life for all technology categories presented. Hence, investments are simply amortized over three years. The gains are the net present value of cost savings expected over the investment life. From this amount, we subtract conservative estimates for operations and maintenance cost each year. The net present value used the prime plus 2 percent discount rate per year. We also assume no (zero) residual value.

**Certain governance activities can reduce the cost of cyber crime.** Figure 22 shows seven enterprise governance activities experienced by a subset of benchmarked companies. Each bar represents the percentage of companies fully executing each stated governance activity. The top three governance activities are: employment of expert security personnel and appointment of a high-level security leader (both 57 percent). Most companies are also certifying against industry-leading standards (52 percent) and obtaining sufficient budgeted resources (51 percent).

**Figure 22. Seven enterprise security governance activities deployed**

Consolidated view, n = 252 separate companies

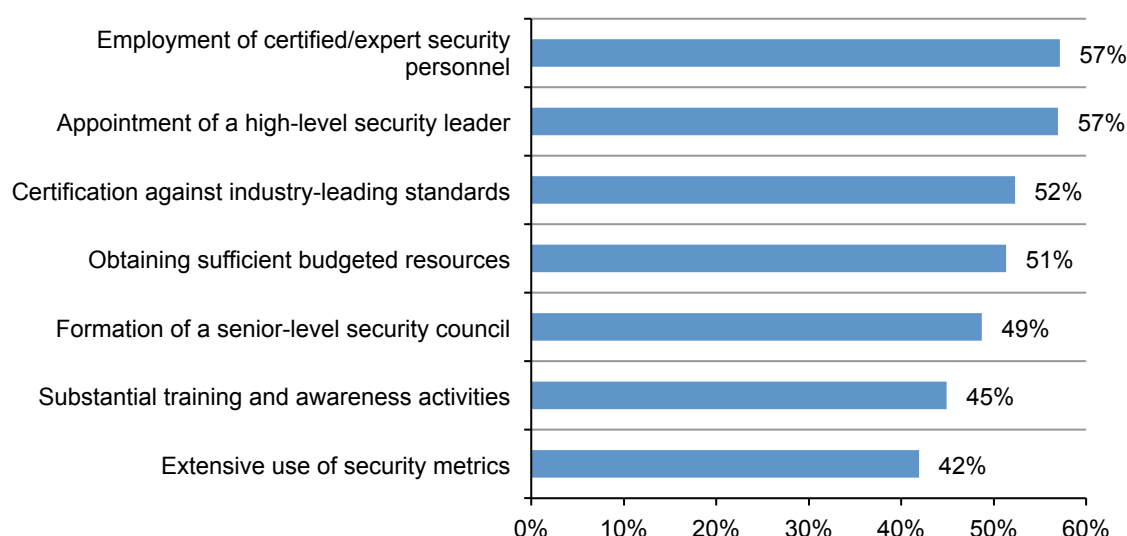
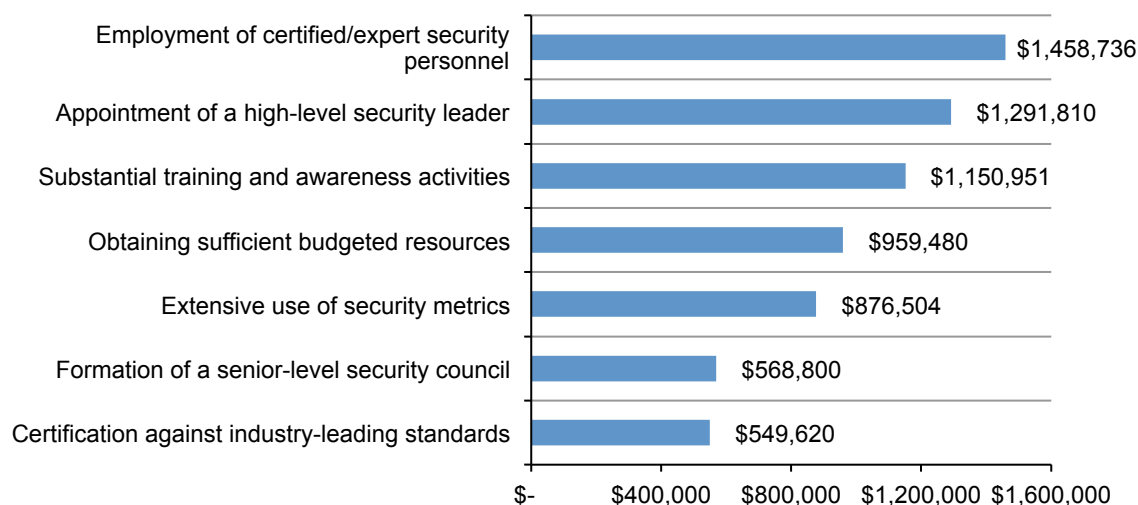


Figure 23 shows the incremental cost savings for each one of seven enterprise governance activities. As shown, companies that employ expert staff can reduce cyber crime costs by an average of \$1.5 million and those that appoint a high-level security leader reduce costs by an average of \$1.3 million. Please note that these extrapolated cost savings are independent of each other and cannot be added together.

**Figure 23. Cost savings when executing seven enterprise security governance activities**

Cost expressed in US dollars. Consolidated view, n = 252 separate companies





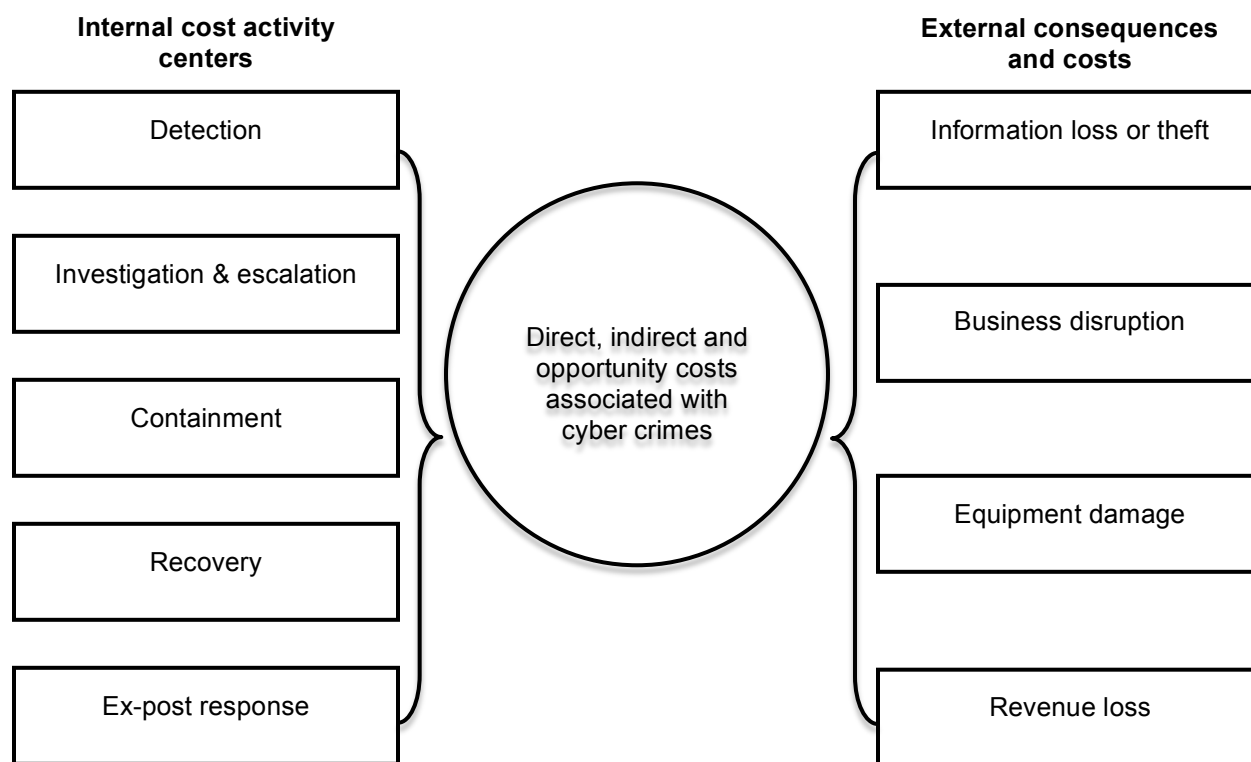
### Part 3. Framework

The purpose of this research is to provide guidance on what a successful cyber attack can cost an organization. Our cost of cyber crime 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 cyber crime. In this study, we define a successful attack as one that results in the infiltration of a company's core networks or enterprise systems. It does not include the plethora of attacks stopped by a company's firewall defenses.

Figure 24 presents the activity-based costing framework used to calculate the average cost of cyber crime. Our benchmark methods attempt to elicit the actual experiences and consequences of cyber attacks. 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 dealing with the cyber crime or what we refer to as the internal cost activity centers.
- The costs related to the consequences of the cyber attack or what we refer to as the external consequences of the cyber attack.

**Figure 24. Cost Framework for Cyber Crime**



As shown above, we analyze the internal cost centers sequentially—starting with the detection of the incident and ending with the ex-post or final response to the incident, 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 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 nine discernible attack vectors: viruses, worms, trojans; malware; botnets; web-based attacks; phishing and social engineering; malicious insiders; stolen or damaged devices; malicious code (including SQL injection); and denial of services.<sup>9</sup>

This study addresses the core process-related activities that drive a range of expenditures associated with a company's cyber attack. The five internal cost activity centers in our framework include:<sup>10</sup>

- Detection: Activities that enable an organization to reasonably detect and possibly deter cyber attacks or advanced threats. This includes allocated (overhead) costs of certain enabling technologies that enhance mitigation or early detection.
- Investigation and escalation: Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents. The escalation activity also includes the steps taken to organize an initial management response.
- Containment: Activities that focus on stopping or lessening the severity of cyber attacks or advanced threats. These include shutting down high-risk attack vectors such as insecure applications or endpoints.
- Recovery: Activities associated with repairing and remediating the organization's systems and core business processes. These include the restoration of damaged information assets and other IT (data center) assets.
- Ex-post response: Activities to help the organization minimize potential future attacks. These include containing costs from business disruption and information loss as well as adding new enabling technologies and control systems.

In addition to the above process-related activities, organizations often experience external consequences or costs associated with the aftermath of successful attacks – which are defined as attacks that infiltrate the organization's network or enterprise systems. Accordingly, 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 a cyber 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.

---

<sup>9</sup> We acknowledge that these nine attack categories are not mutually independent and they do not represent an exhaustive list. Classification of a given attack was made by the researcher and derived from the facts collected during the benchmarking process.

<sup>10</sup> 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.

- 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 cyber 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 a cyber 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 4. Benchmarking

The cost of cyber crime 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 cyber 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. Table 3 reports the frequency of individuals by their approximate functional discipline that participated in this year’s global study. As can be seen, this year’s study in seven countries involved 2,128 interviews for 252 benchmarked companies.<sup>11</sup>

	<b>Freq.</b>	<b>Pct%</b>
IT security	377	18%
IT operations	366	17%
Compliance	211	10%
Data center management	187	9%
Accounting & finance	124	6%
Network operations	121	6%
Legal	113	5%
IT risk management	93	4%
Physical security/facilities mgmt	90	4%
Human resources	86	4%
Internal or IT audit	80	4%
Application development	64	3%
Enterprise risk management	62	3%
Procurement/vendor mgmt	61	3%
Industrial control systems	51	2%
Quality assurance	42	2%
Total	2,128	
Interviews per company on average	8.44	

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.

<sup>11</sup>Last year’s study involved 2,081 individuals or an average of 8.1 interviews for each benchmarked company.

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	<div style="border-bottom: 1px solid black; height: 20px; position: relative;"> <div style="position: absolute; left: 50%; transform: translateX(-50%); border-left: 1px solid black; border-right: 1px solid black; height: 10px;"></div> </div>	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 cyber crime.

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 cyber crime 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 August 2015. To maintain consistency for all benchmark companies, information was collected about the organizations' cyber crime 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 cyber crime were annualized by dividing the total cost collected over four weeks (ratio = 4/52 weeks).

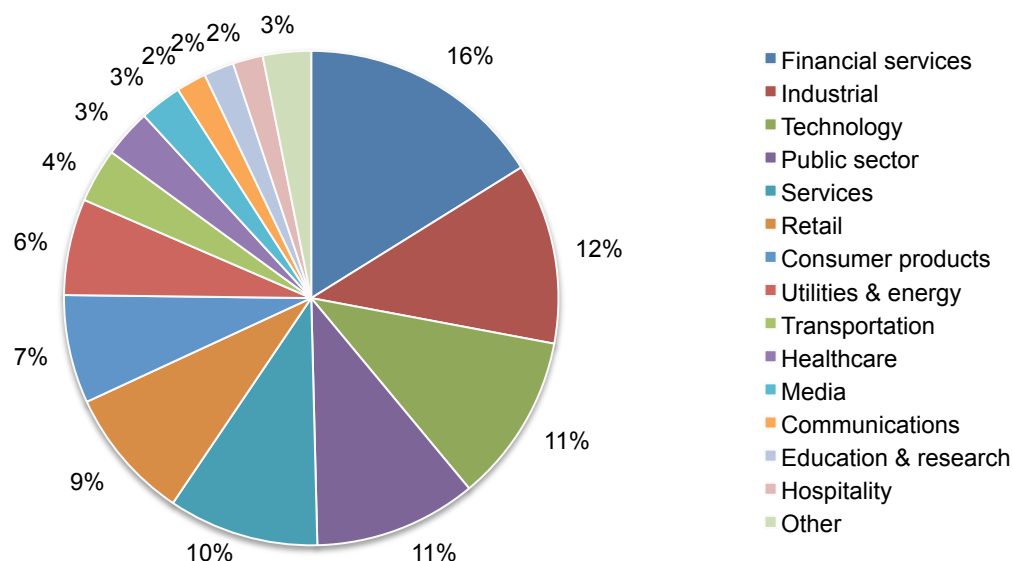
## Part 5. Benchmark Sample

The recruitment of the annual study started with a personalized letter and a follow-up phone call to 1,502 contacts for possible participation and 252 organizations permitted Ponemon Institute to perform the benchmark analysis.

Pie Chart 1 summarizes the current (FY 2015) sample of participating companies based on 18 primary industry classifications<sup>12</sup>. As can be seen, financial services (16 percent) represent the largest segment. This includes retail banking, insurance, brokerage and credit card companies. The second and third largest segments include industrial (12 percent) and technology (11 percent). The technology segment includes companies in software and IT management.

### Pie Chart 1. Industry sectors of participating organizations

Consolidated view, n = 252 separate companies

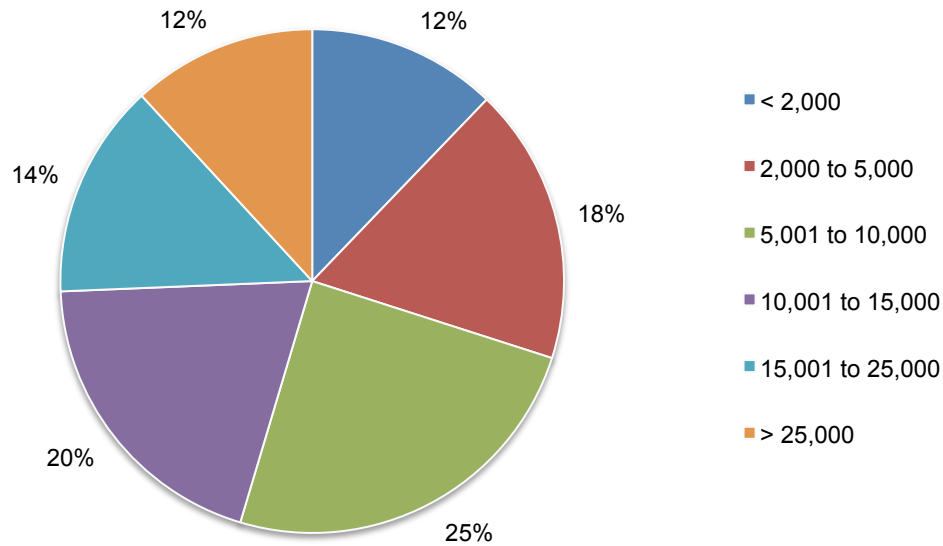


<sup>12</sup> The "other" category includes: automotive, pharma, agriculture and defense

Pie Chart 2 reports the percentage frequency of companies based on the number of enterprise seats connected to networks or systems. Our analysis of cyber crime cost only pertains to organizations with a minimum of approximately 600 seats. The largest number enterprise seats in the 2015 global study exceeds 79,000.

**Pie Chart 2. Distribution of participating organizations by enterprise seats (size)**

Consolidated view, n = 252 separate companies



## Part 6. Limitations & Conclusions

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

- **Non-statistical results:** The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of organizations of mostly larger-sized entities experiencing one or more cyber attacks during a four-week fielding period. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the nature of our sampling plan.
- **Non-response:** The current findings are based on a small representative sample of completed case studies. An initial mailing of benchmark surveys was sent to a targeted group of organizations, all believed to have experienced one or more cyber attacks. A total of 252 companies provided usable benchmark surveys. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the methods used to manage the cyber crime containment and recovery process, as well as the underlying costs involved.
- **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 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. Industry classification relies on self-reported results.
- **Unmeasured factors:** To keep the survey 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 estimated at this time.
- **Estimated cost results.** The quality of survey research is based on the integrity of confidential responses received from companies. While certain checks and balances can be incorporated into the survey process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique (termed shadow costing methods) rather than actual cost data could create significant bias in presented results.



---

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 49629 USA  
1.800.887.3118  
[research@ponemon.org](mailto:research@ponemon.org)

## **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.