Ponemon INSTITUTE



2014 Cost of Cyber Crime Study: United States

Sponsored by HP Enterprise Security

Independently conducted by Ponemon Institute LLC

Publication Date: October 2014

2014 Cost of Cyber Crime Study: United States

Benchmark Study of U.S. Companies

Ponemon Institute October 2014

Part 1. Executive Summary

We are pleased to present the *2014 Cost of Cyber Crime Study: United States*, the fifth annual study of US companies. Sponsored by HP Enterprise Security, this year's study is based on a representative sample of 59 organizations in various industry sectors. While our research focused on organizations located in the United States, most are multinational corporations.

This is the third year Ponemon Institute conducted cyber crime cost studies for companies in the United Kingdom, Germany, Australia and Japan. Last year we conducted a study of French companies for the first time and this year we added the Russian Federation. The findings from this research are presented in separate reports.

During the period we conducted interviews and analyzed the findings, mega cyber crimes took place. Most notable was the Target cyber breach, which was reported to result in the theft of 40 million payment cards.

U.S. Study at a Glance

59 US companies, 257 companies in 7 countries
544 interviews with US company personnel
138 total attacks used to measure total cost
$12.7 million is the average annualized cost
9.3 percent net increase in cost over the past year
15 percent average ROI for 7 security technologies

More recently, Chinese hackers launched a cyber attack against Canada's National Research Council as well as commercial entities in Pennsylvania, including Westinghouse Electric Company, U.S. Steel and the United Steel Workers Union. Russian hackers recently stole the largest collection of Internet credentials ever: 1.2 billion user names and passwords, plus 500 million email addresses. While the companies represented in this research did not have cyber attacks as devastating as these were, they did experience incidents that were expensive to resolve and disruptive to their operations.

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., more than 1,000 enterprise seats[1]). 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.

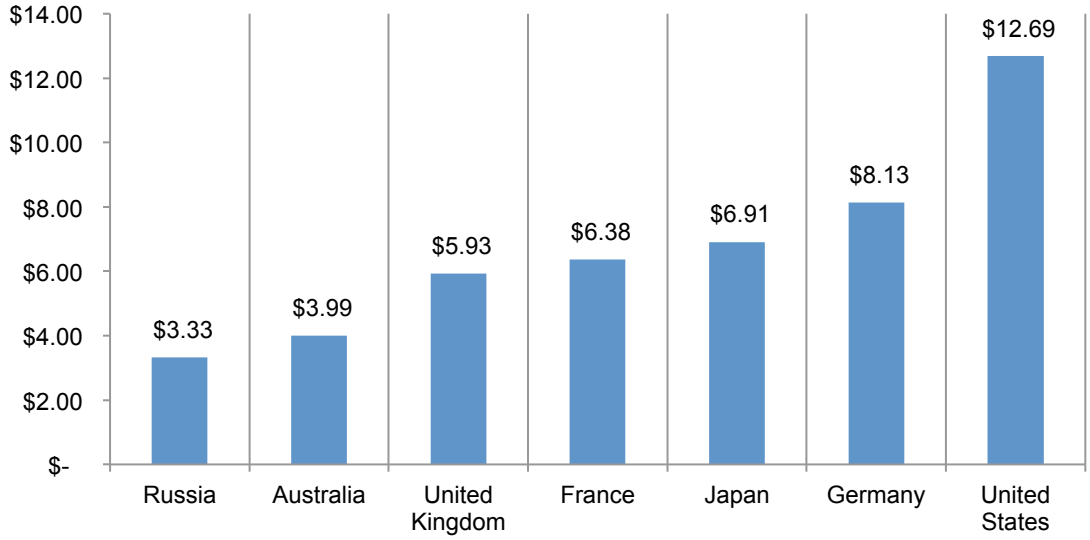
[1] Enterprise seats refer to the number of direct connections to the network and enterprise systems.

Global at a glance

This year's annual study was conducted in the United States, United Kingdom, Germany, Australia, Japan, France and for the first time, the Russian Federation, with a total benchmark sample of 257 organizations. These global results are presented in a separate manuscript entitled, *2014 Global Report on the Cost of Cyber Crime.*

Figure 1 presents the estimated average cost of cyber crime for seven country samples involving 257 separate companies. These figures are converted into U.S. dollars for comparative purposes. 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 $12.7 million and the RF sample reports the lowest total average cost at $3.3 million.

Figure 1. Total cost of cyber crime in seven countries
Cost expressed in US dollars, n = 257 separate companies



Summary of U.S. findings

Following are the most salient findings for a sample of 59 U.S.-based organizations requiring 544 separate interviews to gather cyber crime cost results. In several places in this report, we compare the present findings to the five-year average of benchmark studies.

Cyber crimes continue to be very costly for organizations. We found that the mean annualized cost for 59 benchmarked organizations is $12.7 million per year, with a range from $1.6 million to $61 million each year per company. Last year's mean cost per benchmarked organization was $11.6 million. Thus, we observe a $1.1 million (9.3 percent) increase in mean value.

Cyber crime cost varies by organizational size. Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost.[2] However, based on enterprise seats, we determined that small organizations incur a significantly higher per capita cost than larger organizations ($1,513 versus $517).

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 energy & utilities, defense and financial services experience substantially higher cyber crime costs than organizations in consumer products, healthcare and hospitality.

The most costly cyber crimes are those caused by denial of services, malicious insiders and malicious code. These account for more than 55 percent of all cyber crime costs per organization on an annual basis.[3] 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 average time to resolve a cyber attack was 45 days, with an average cost to participating organizations of $1,593,627 during this 45-day period. This represents a 33 percent increase from last year's estimated average cost of $1,035,769, which was based upon a 32-day resolution period. Results show that malicious insider attacks can take more than 65 days on average to contain.

Information theft continues to represent the highest external cost, followed by the costs associated with business disruption.[4] On an annualized basis, information theft accounts for 40 percent of total external costs (down 2 percent from the five-year average). Costs associated with disruption to business or lost productivity account for 38 percent of external costs (up 7 percent from the five-year average).

Recovery and detection are the most costly internal activities. On an annualized basis, recovery and detection combined account for 49 percent of the total internal activity cost with cash outlays and direct labor representing the majority of these costs.

---

[2]In this study, we define an enterprise seat as one end-user identity/device connected to the company's core networks or enterprise systems.
[3]This year the category malicious insider includes the cost of stolen devices.
[4]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.

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 $5.3million when compared to companies not deploying security intelligence technologies.

A strong security posture moderates the cost of cyber attacks. We utilize Ponemon Institute's proprietary metric called the Security Effectiveness Score (SES) Index to define an organization's ability to achieve reasonable security objectives.[5] The higher the SES, the more effective the organization is in achieving its security objectives. The average cost to mitigate a cyber attack for organizations with a high SES is substantially lower than organizations with a low SES score.

Companies deploying security intelligence systems experienced a substantially higher ROI at 30 percent than all other technology categories presented. Also significant are the estimated ROI results for companies that extensively deploy encryption technologies (25 percent) and advanced perimeter controls such as UTM, NGFW, IPS with reputation feeds (15 percent).

Deployment of enterprise security governance practices moderates the cost of cyber crime. Findings show companies that invest in adequate resources, appoint a high-level security leader, and employ certified or expert staff have cyber crime costs that are lower than companies that have not implemented these practices. This so-called "cost savings" for companies deploying good security governance practices is estimated at $1.7 million, on average.

[5]The Security Effectiveness Score has been developed by PGP Corporation and Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 30 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). Hence, a result greater than zero is viewed as net favorable.

Part 2. Key findings

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

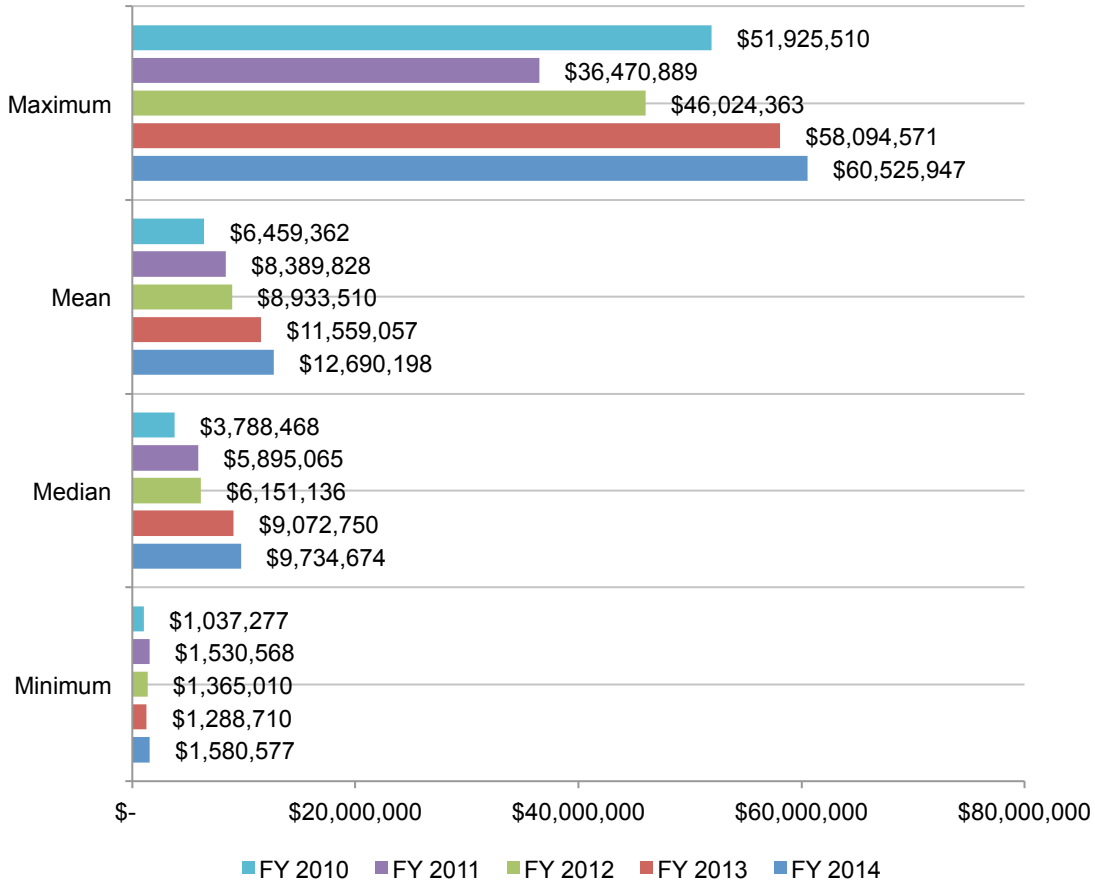
- **The average cost of cyber crime by organizational size and industry**
- **The type of attack influences the cost of cyber crime**
- **An analysis of the cost components of cyber crime**

The average cost of cyber crime by organizational size and industry

To determine the average cost of cyber crime, the 59 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.[6]

As shown in Figure 2, the total annualized cost of cyber crime in 2014 ranges from a low of $1.6 million to a high of $60.5 million. The median annualized cost of cyber crime in the benchmark sample is $9.7 million – an increase from last year's median value of $9.1. The mean value is $12.7 million. This is an increase of $1.1 million or a 9.3 percent from last year's mean of $11.6 million.

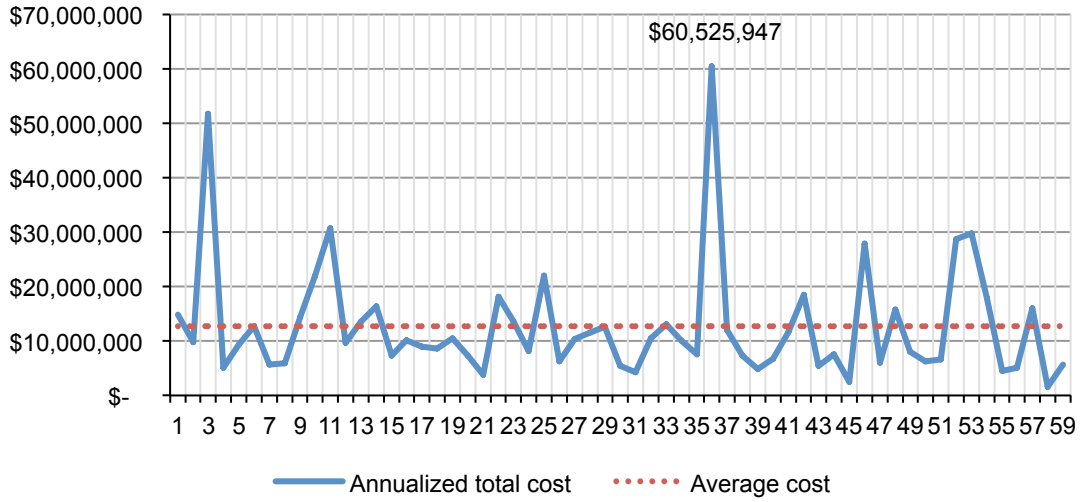
Figure 2. The cost of cyber crime



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

Figure 3 reports the distribution of annualized total cost for 59 companies. As can be seen, 40 companies in our sample incurred total costs below the mean value of $12.7 million, thus indicating a skewed distribution. The highest cost estimate of $61 million was determined not to be an outlier based on additional analysis. Nineteen other organizations experienced an annualized total cost of cyber crime above the mean value.

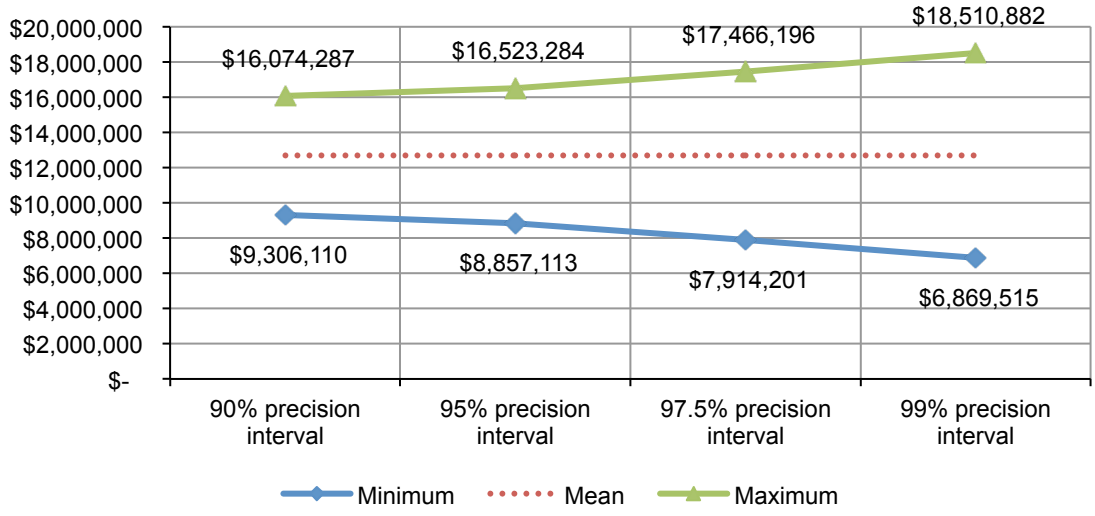
Figure 3. Annualized total cost of cyber crime for 59 participating companies



As part of our analysis we calculated a precision interval for the average cost of $12.7 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.

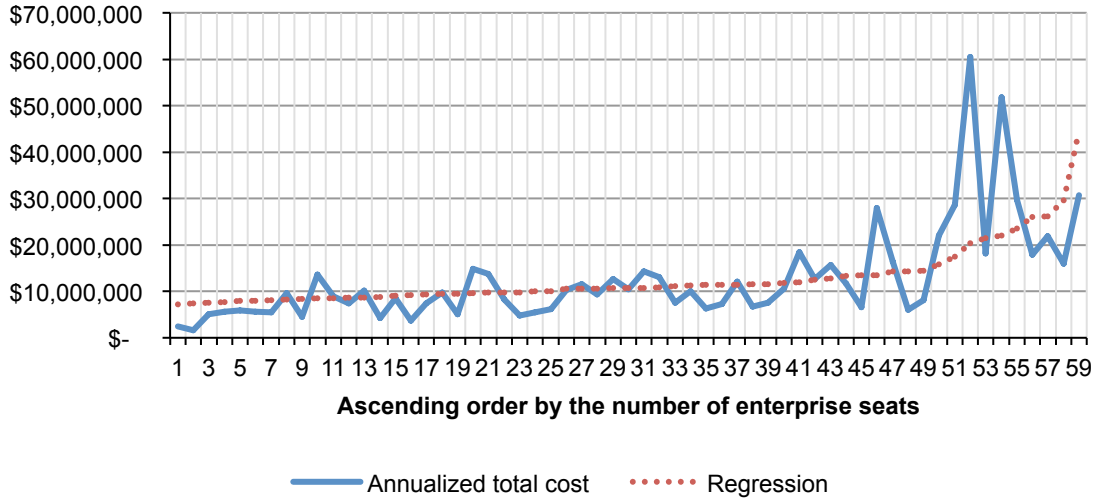
The range of possible cost estimates widens at increasingly higher levels of confidence, as shown in Figure 4. Specifically, at a 90 percent level of confidence we expect the range of cost to be between $9.3 million to $16 million.

Figure 4. Precision interval for the mean value of annualized total cost



The cost of cyber crime varies by organizational size. As shown in Figure 5, 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.

Figure 5. Annualized cost in ascending order by the number of enterprise seats



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 five years. Approximately 14 companies are in each quartile.

Table 1. Quartile analysis for annualized total cost in ascending order

Study	Quartile 1	Quartile 2	Quartile 3	Quartile 4
FY 2010	1,650,976	3,180,182	4,611,172	15,567,136
FY 2011	2,872,913	5,167,657	7,576,693	17,455,124
FY 2012	2,832,962	5,440,553	8,664,578	18,795,950
FY 2013	4,120,930	7,224,624	11,129,065	23,761,610
FY 2014	4,789,743	7,951,486	12,109,437	26,854,409

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 2014 average per capita cost for organizations with the fewest seats is three times higher than the average per capita cost for organizations with the most seats.

Table 2. Quartile analysis for annualized cost per seat in ascending order

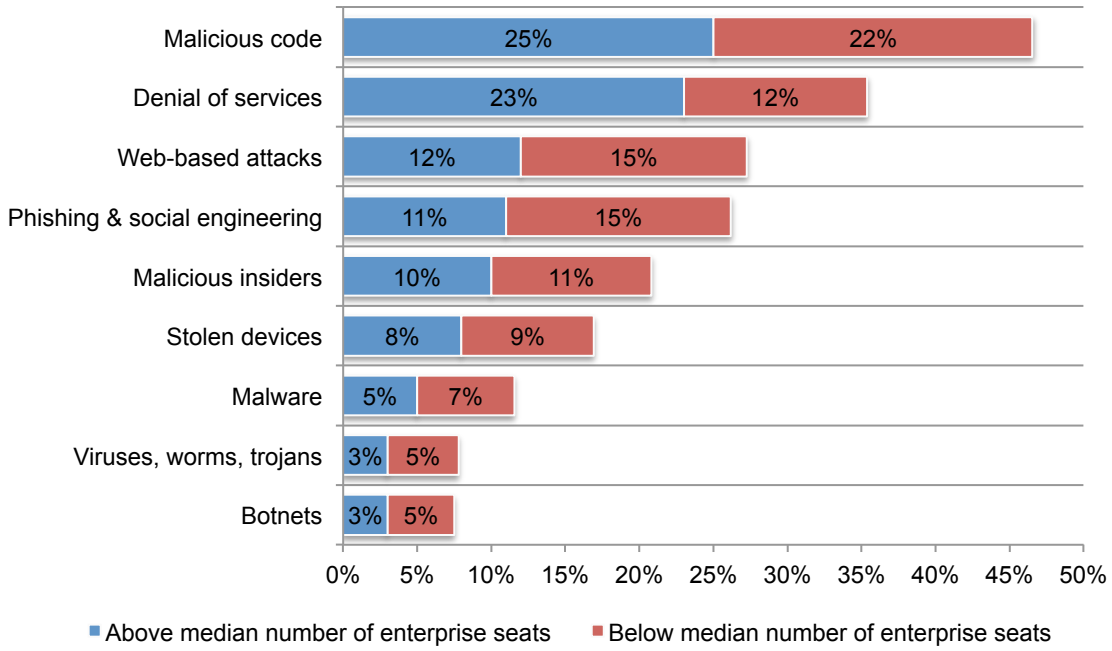
Study	Quartile 1	Quartile 2	Quartile 3	Quartile 4
FY 2010	$1,291	$688	$517	$307
FY 2011	$1,088	$710	$783	$284
FY 2012	$1,324	$621	$490	$305
FY 2013	$1,564	$900	$798	$371
FY 2014	$1,513	$860	$652	$517

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 6, we compare smaller and larger-sized organizations based on the sample median of 12,799 seats. Smaller organizations (below the median) experience a higher proportion of cyber crime costs relating to web-based attacks and phishing and social engineering (both 15 percent of total costs).

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

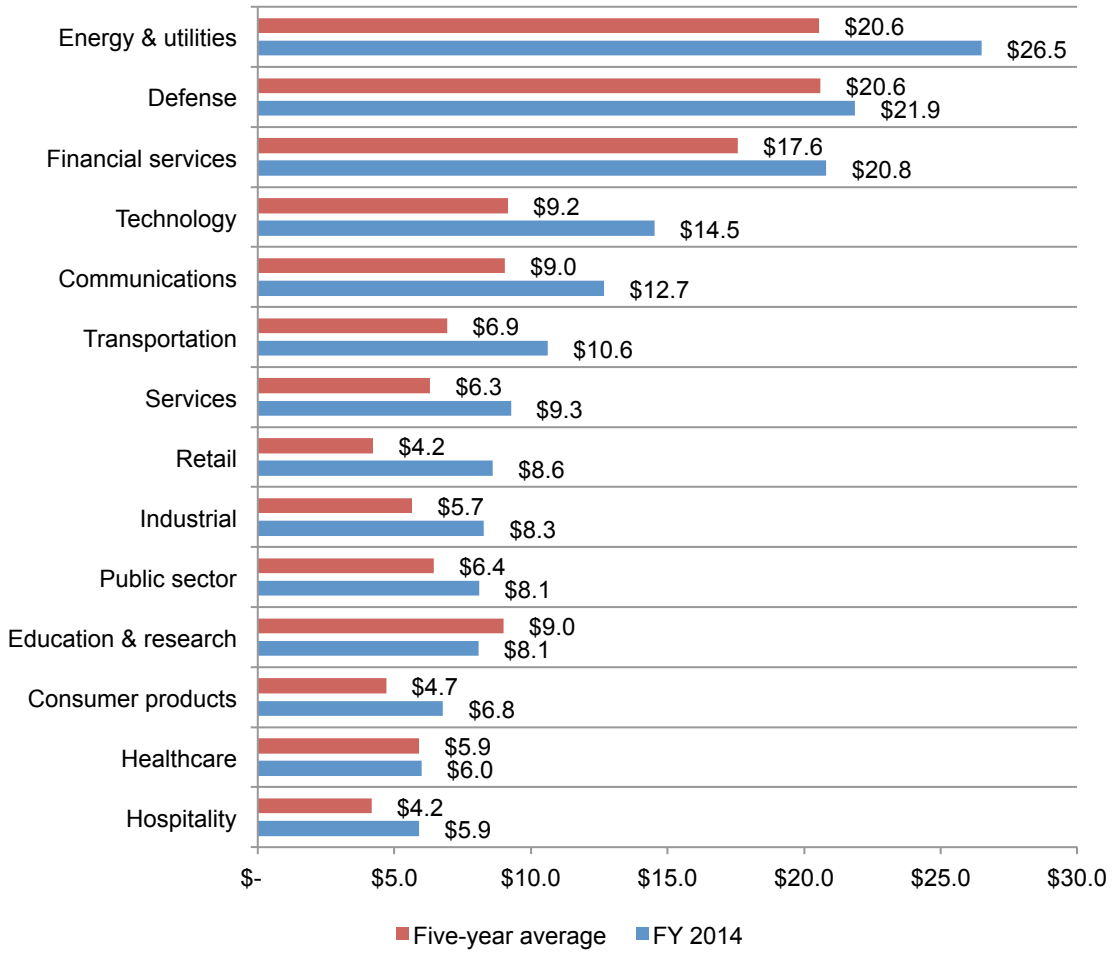
We also distinguish viruses from malware. Viruses reside on the endpoint and as yet have not infiltrated the network but malware has infiltrated the network. Malicious code attacks the application layer and includes SQL attack.

Figure 6. Organizational size affects the cost of dealing with nine attack types
Size measured according to the number of enterprise seats within the participating organizations



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 the 2014 results to the past five years the study was conducted. As seen in Figure 7, the cost of cyber crime in the energy and utilities, technology and retail industries rose significantly. Organizations in consumer products, healthcare and hospitality appear to have a lower overall cyber crime cost over five years.[7]

Figure 7. Average annualized cost by industry sector
$1,000,000 omitted



[7]This analysis is for illustration purposes only. The sample sizes in all five years makes its difficult to draw definitive conclusions about industry segment differences.

The type of cyber attack influences the cost of cyber crime

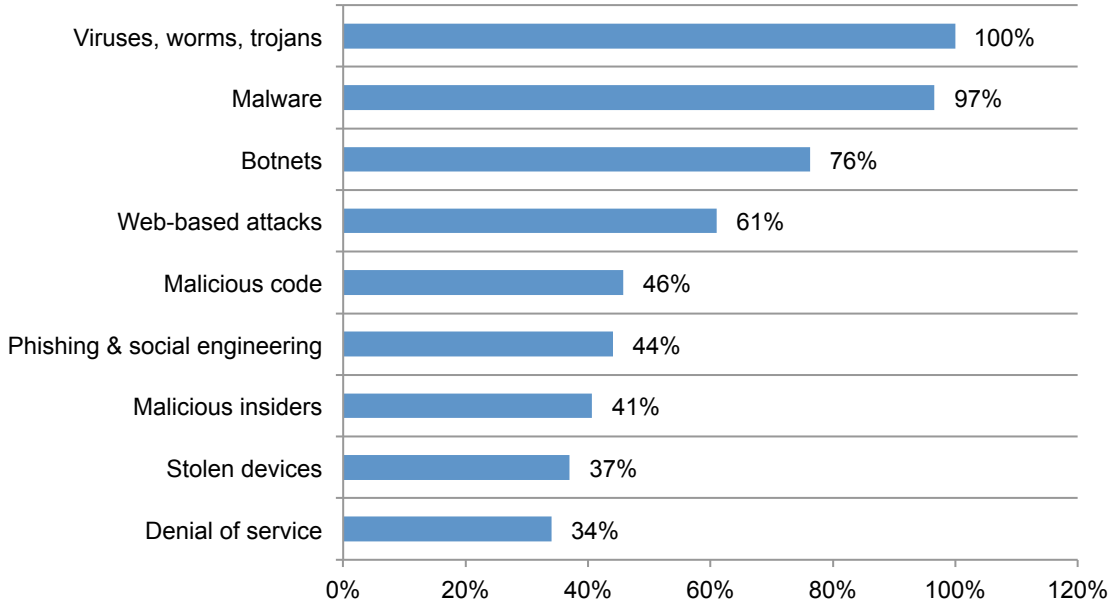
In our studies we look at nine different attack vectors as the source of the cyber crime. This year, the benchmark sample of 59 organizations experienced 138 discernible cyber attacks per week, which translates to 2.34 successful attacks per benchmarked organization each week. The list below shows the number of successful attacks for the four previous years of this research. It is clear how the number of attacks per week have steadily increased.

- FY 2013, 122 attacks in 60 organizations
- FY 2012, 102 attacks in 56 organizations
- FY 2011, 72 attacks in 50 organizations
- FY 2010, 50 attacks in 46 organizations

Figure 8 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.

Seventy-six percent experienced botnets and web-based attacks affected 61 percent of companies. Denial of service attacks declined significantly from 50 percent to 34 percent. Forty-six percent experienced malicious code and 44 percent experienced a phishing & social engineering scheme. Only 37 percent of companies say a stolen device was the source of the cyber crime.

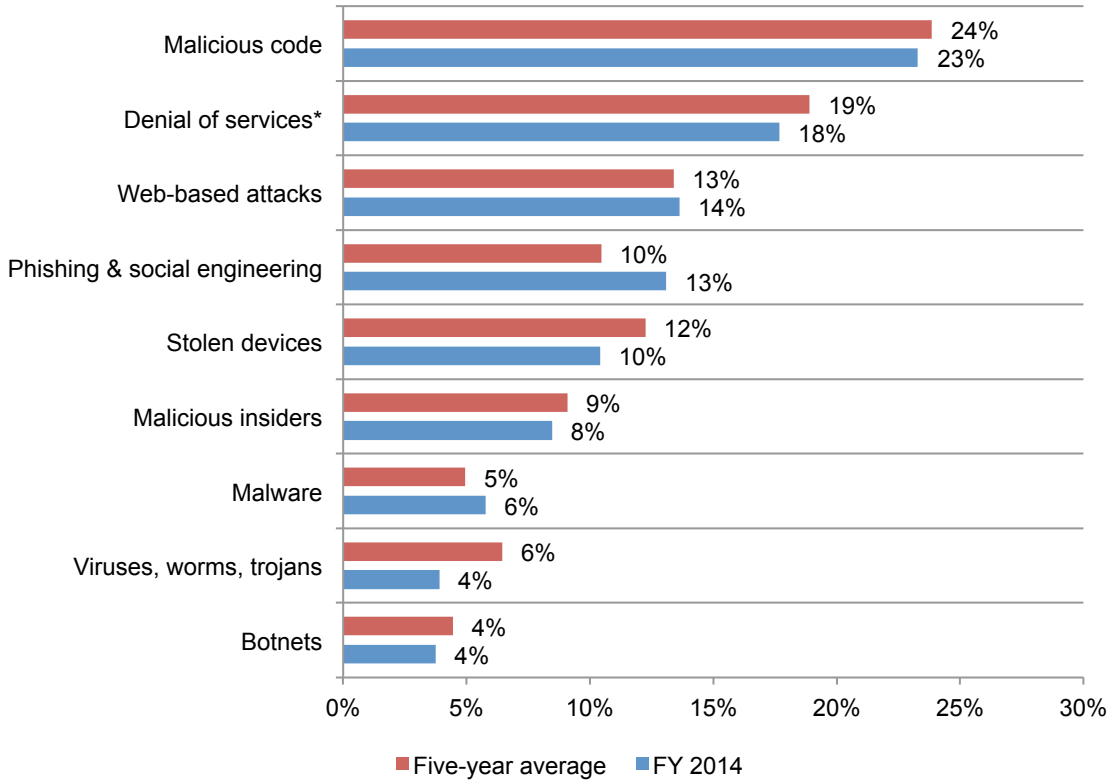
Figure 8. Types of cyber attacks experienced by 59 benchmarked companies



Costs vary considerably by the type of cyber attack. Figure 9 compares benchmark results over five years, showing the percentage of annualized cost of cyber crime allocated to nine attack types compiled from all benchmarked organizations.

In total, the top three attacks account for more than 55 percent of the total annualized cost cyber crime experienced by 59 companies. While they do not occur as frequently as viruses and malware, malicious code and denial of service (DoS) attacks are the most costly as a percentage of the average cost of cyber crime. The least costly are botnets, viruses, worms and trojans and malware.

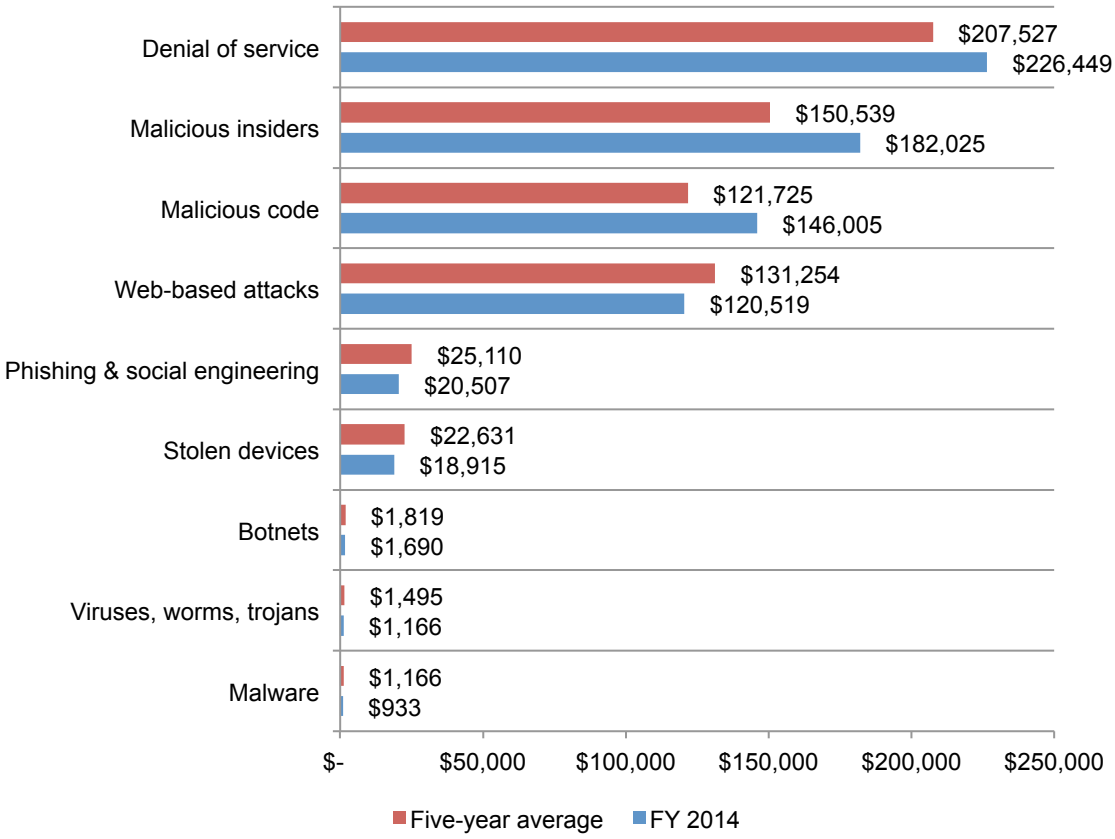
Figure 9. Percentage annualized cyber crime cost by attack type



The cost of cyber crime is also influenced by the frequency of the different attack types. Figure 10 reveals the most to least expensive cyber attacks when analyzed on the frequency of incidents. The most expensive attacks are denial of services, malicious insiders and malicious code.

Another interesting finding is the significant cost increase for the attack category termed malicious insiders, which rose by more than $31,000 over the five-year average. In the context of our study, malicious insiders include employees, temporary employees, contractors and, possibly, business partners. Denial of service and malicious code also increased. However, web-based attacks, phishing & social engineering and stolen devices decreased over the five-year average.

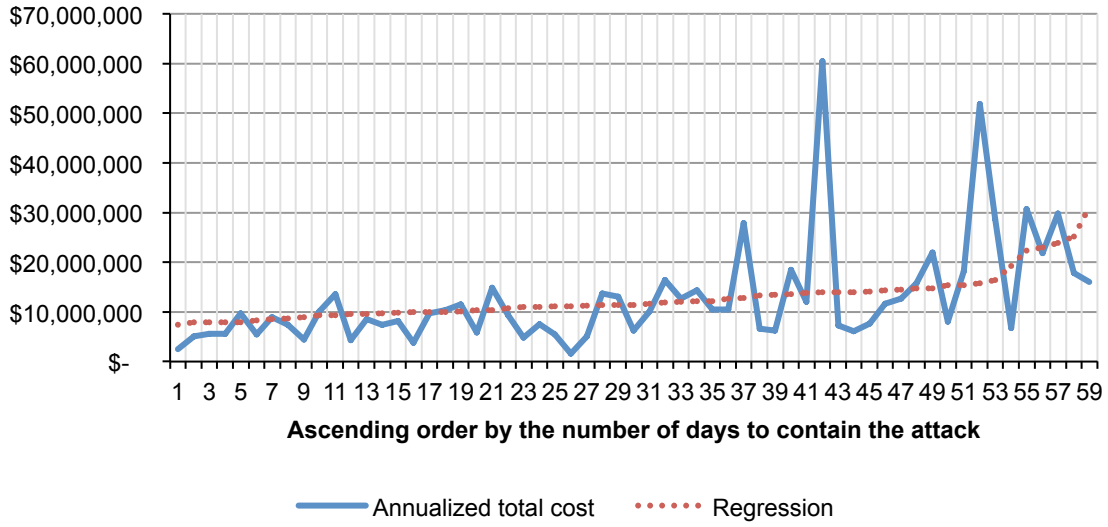
Figure 10. Average annualized cyber crime cost weighted by attack frequency



Time to resolve or contain cyber crimes increases the cost. The mean number of days to resolve cyber attacks is 45 with an average cost of $35,647 per day – or a total cost of $1,593,627 over the 45-day remediation period. This represents a 33 percent increase from last year's cost estimate of $1,035,769. 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 11 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.

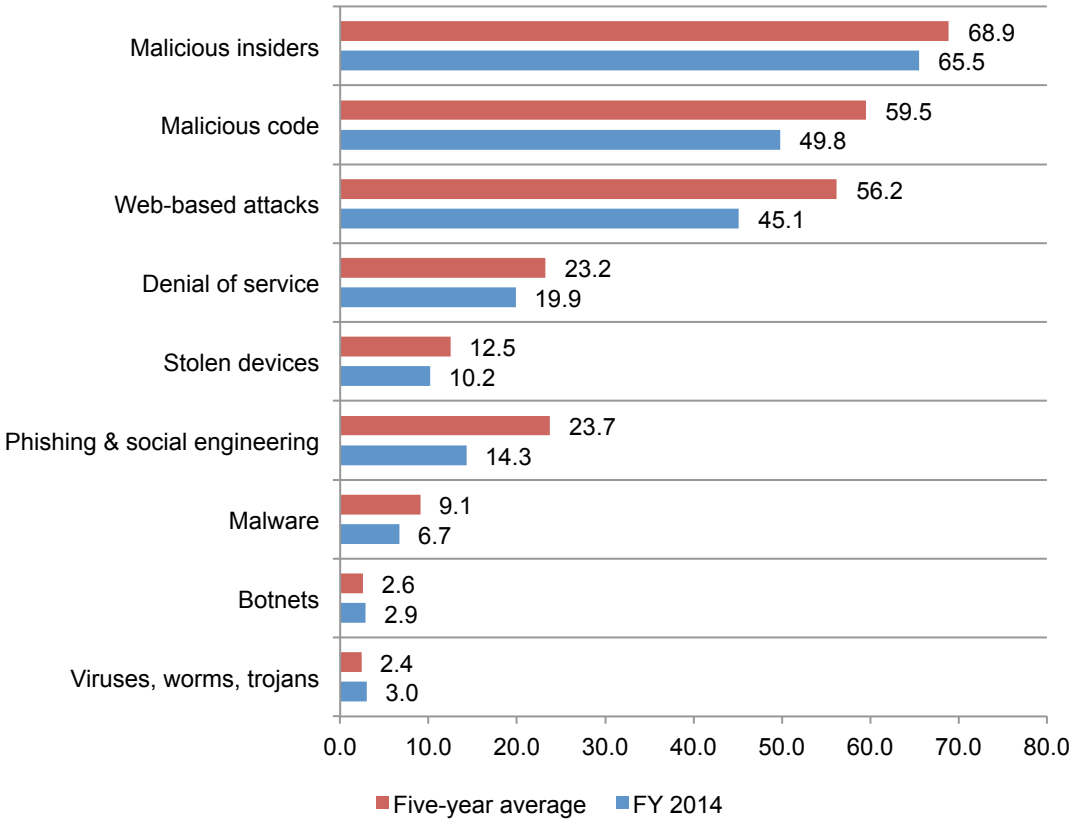
Figure 11. Total annualized cost by the number of days to contain the attack



Some attacks take longer to resolve and as a result are more costly. As show in Figure 11, the time it takes to resolve the consequences of the attack increases the cost of a cyber crime.

Figure 12 reports the average days to resolve cyber attacks for nine different 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, botnets and viruses on average are resolved in just more than a week or fewer days.

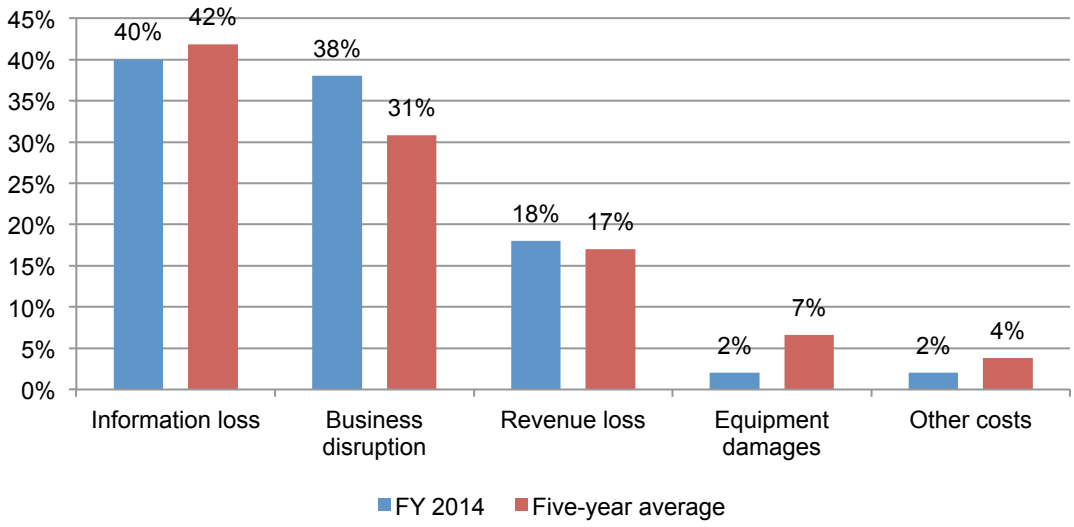
Figure 12. Some attacks take longer to resolve
Estimated average time is measured for each attack type in days



Information theft remains the most expensive consequence of a cyber crime. In this research we look at four primary consequences of a cyber attack: the loss of information, disruption of business, loss of revenue and damage to equipment. As shown in Figure 13, among the organizations represented in this study information loss represents the highest component (40 percent) of the total cost to an organization that has a cyber attack. This is a slight decrease from the five-year average of 42 percent.

Business disruption or loss of productivity has increased to 38 percent from the five-year average of 31 percent percent of total costs. Revenue losses (18 percent) and equipment damages (2 percent) yield a much lower cost impact.

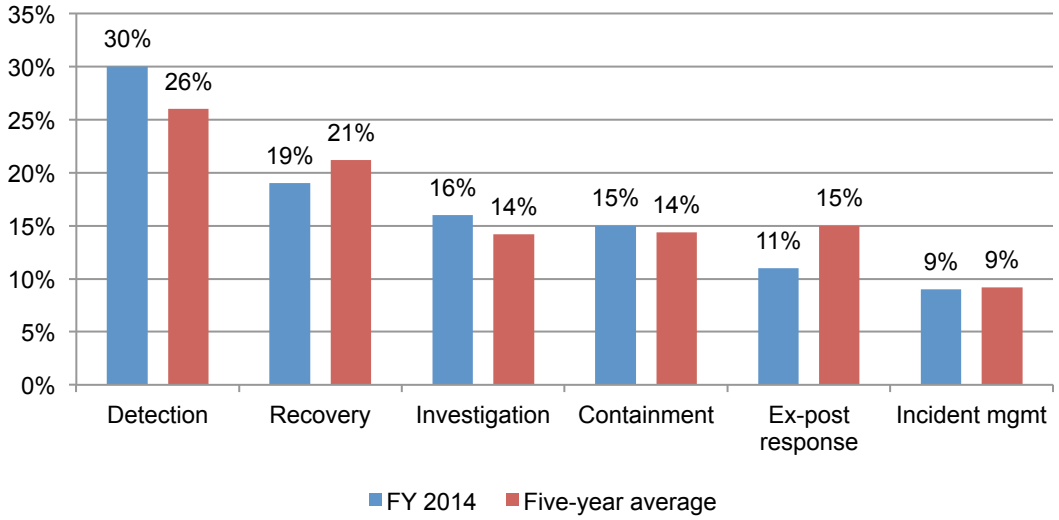
Figure 13. Percentage cost for external consequences



Companies spend the most on recovery and detection. Cyber crime detection and recovery activities account for 49 percent of total internal activity cost (47 percent is the five-year average), as shown in Figure 14. This is followed by investigation and containment (16 percent and 15 percent, respectively).

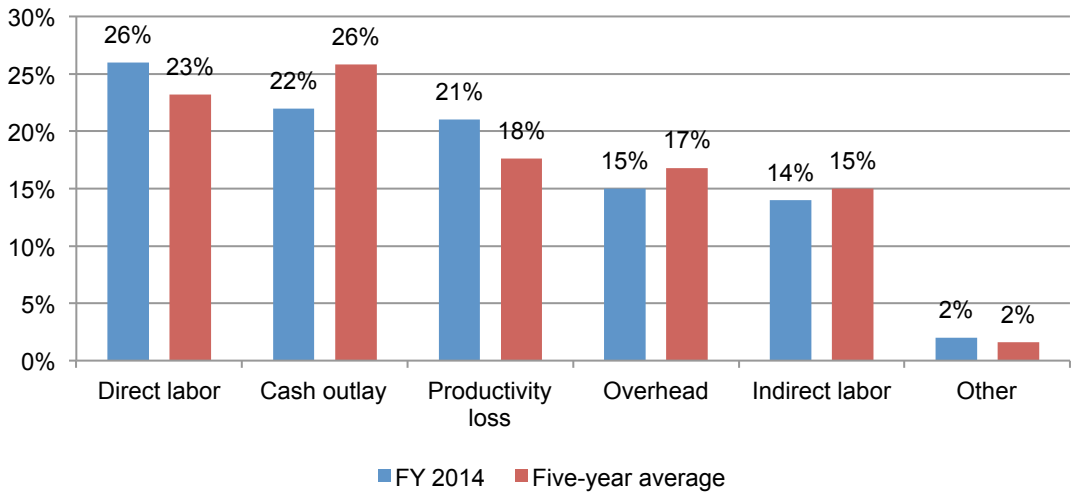
Detection and recovery cost elements highlight a significant cost-reduction opportunity for organizations that are able to systematically manage recovery and to deploy enabling security technologies to help facilitate the detection process.

Figure 14. Percentage cost by activities conducted to resolve a cyber attack



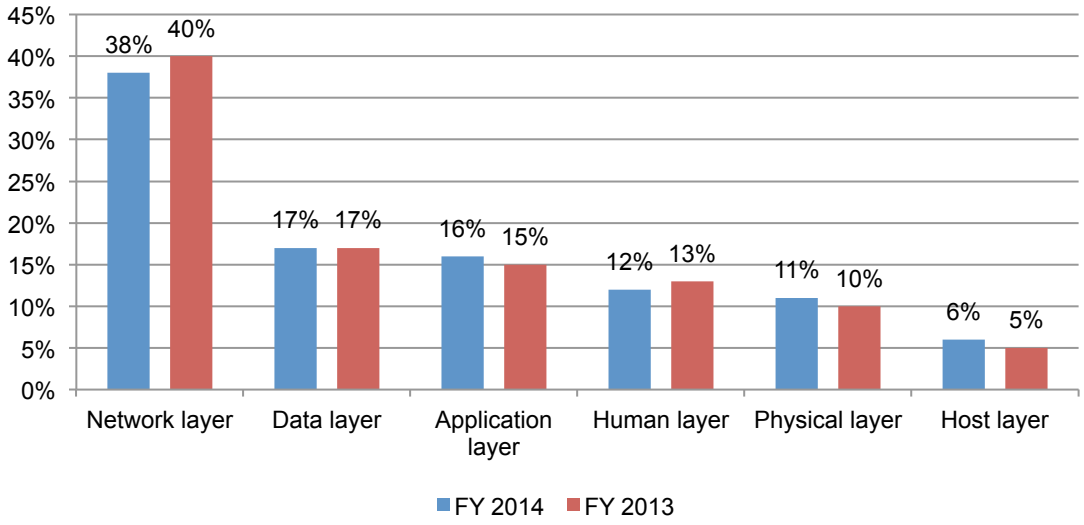
The percentage of annualized costs can be further broken down into **6** specific expenditure components, which include: direct labor (26 percent), cash outlays (22 percent), productivity losses (21 percent), overhead (15 percent), indirect labor (14 percent) and other. As shown in Figure 15, the distribution of cash outlays, overhead and, to a small extent, indirect labor has decreased over five years. In contrast, direct labor and productivity losses have increased over five years.

Figure 15. Percentage activity cost by 6 specific cost components



The largest portion of the security budget is allocated to the network layer. Figure 16 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 38 percent of total dedicated IT security funding. At only six percent, the host layer receives the lowest funding level.

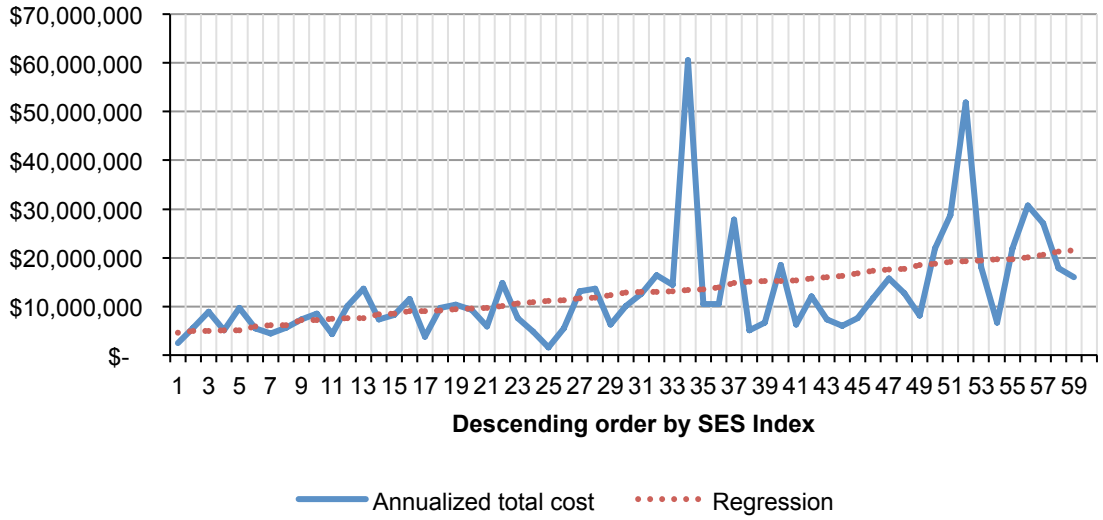
Figure 16. Budgeted or earmarked spending according to six IT security layers



The organization's security posture influences the cost of cyber crime. We measure the security posture of participating organizations as part of the benchmarking process. Figure 17 reports the annualized cost and regression of companies in descending order of their security effectiveness as measured by the SES (see footnote 6).

The figure shows an upward sloping regression, suggesting that companies with a stronger security posture experience a lower overall cost. The SES range of possible scores is +2 (most favorable) to -2 (least favorable). Compiled results for the present benchmark sample vary from a high of +1.90 to a low of -1.57 with an SES mean value at .25.

Figure 17. Annualized cost in descending order by SES



A comparison of organizations grouped into four quartiles based on SES reveals cost differences. According to Table 3 the average cost for companies in SES quartile 1 is $7.12 million, while the average cost for SES quartile 4 is substantially higher at $20.64 million. This analysis supports the above regression equation, which shows a company's security posture has a net favorable affect on cyber crime costs.

Table 3. Quartile analysis for annualized cost by SES index ($000,000 omitted)

Study	Quartile 1 (highest SES)	Quartile 2	Quartile 3	Quartile 4 (lowest SES)
FY 2010	5.00	7.23	8.98	15.77
FY 2011	6.80	7.10	7.29	12.16
FY 2012	4.34	6.00	8.45	16.94
FY 2013	5.47	10.00	12.90	17.86
FY 2014	7.12	8.53	14.81	20.64

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, 29 companies (49 percent) deploy security intelligence tools such as SIEM, IPS with reputation feeds, network intelligence systems, big data analytics and others.

With two exceptions (investigative and incident management 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 ($4.74 vs. $2.73), recovery ($2.96 vs. $1.89) and containment ($2.67 vs. $1.57) activities, respectively.

Figure 18. Activity cost comparison and the use of security intelligence technologies
$1,000,000 omitted

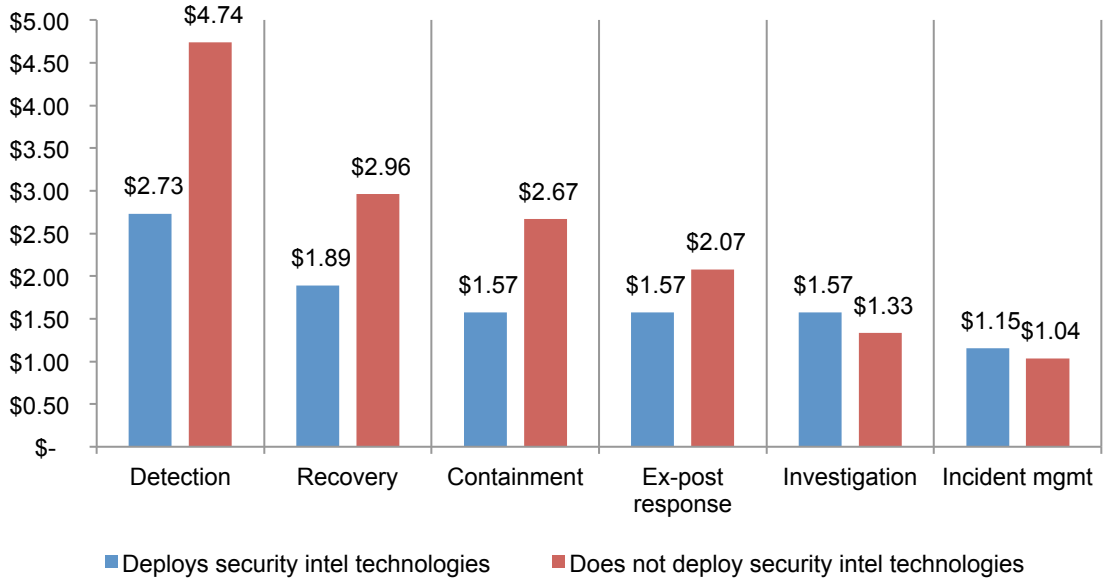


Figure 19 shows seven enabling security technology categories experienced by a subset of benchmarked companies. Each bar represents the percentage of companies fully deploying each given security technology. The top three technology categories include: advanced perimeter control and firewall technologies (61 percent), enterprise encryption technologies (53 percent), and security intelligence systems (49 percent).

Figure 19. Seven enabling security technologies deployed

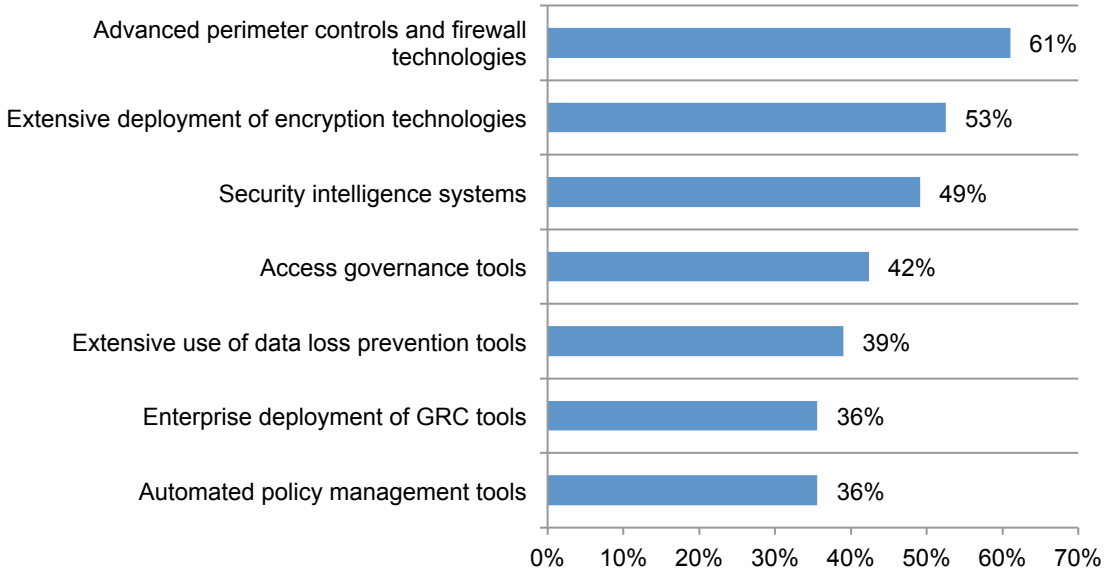
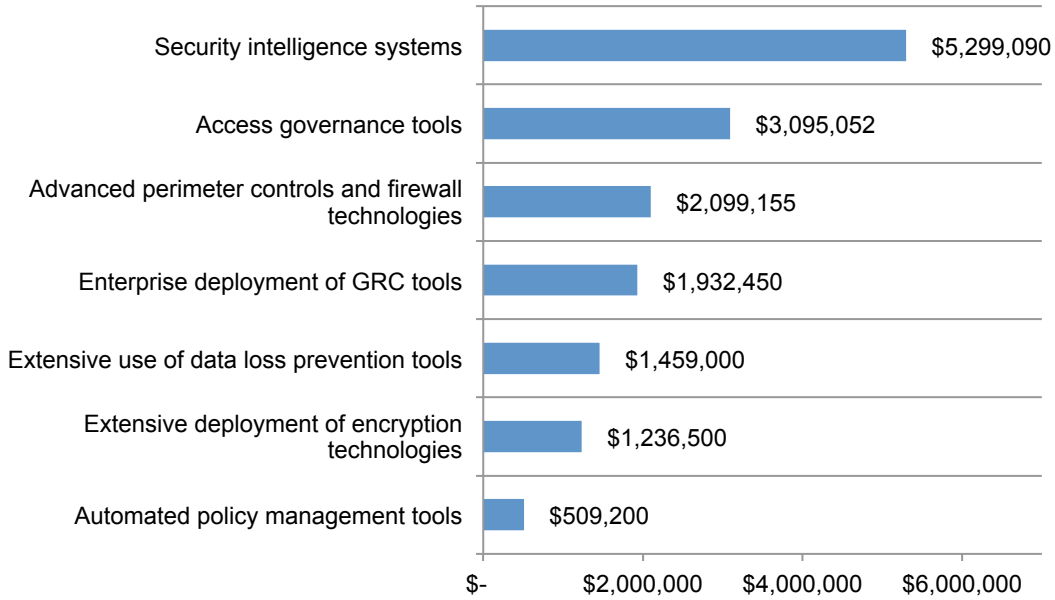


Figure 20 shows the money companies can save by deploying each one of seven enabling security technologies. For example, companies deploying security intelligence systems, on average, experience a substantial cost savings of $5.3 million. Similarly, companies deploying access governance tools experience cost savings of $3.1 million on average. Please note that these extrapolated cost savings are independent of each other and cannot be added together.

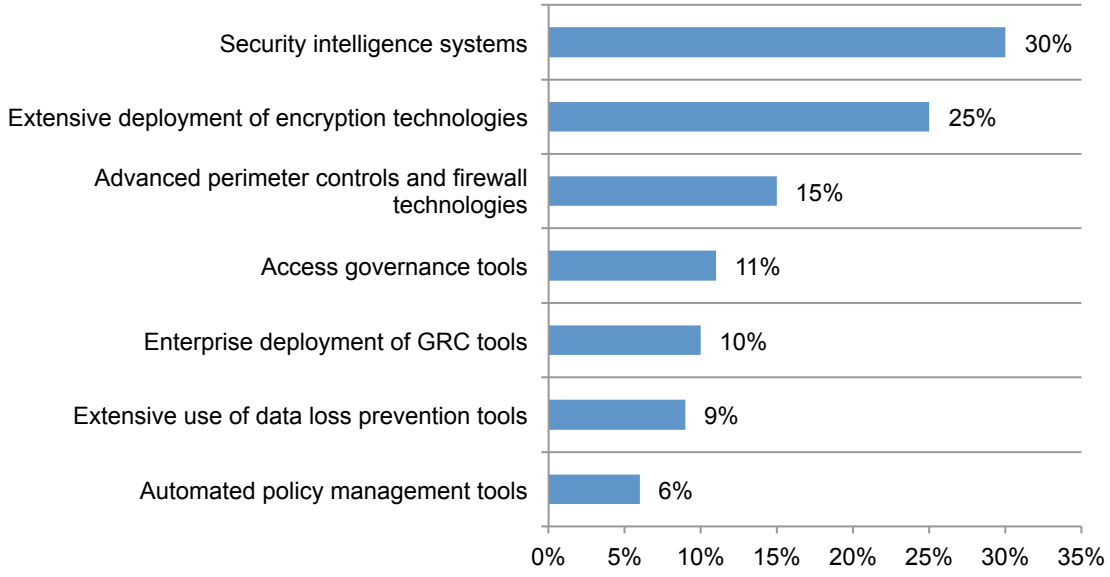
Figure 20. Cost savings when deploying seven enabling technologies



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.[8] At 30 percent, companies deploying security intelligence systems, on average, experienced a substantially higher ROI than all other technology categories presented.

Also significant are the estimated ROI results for companies that extensively deploy encryption technologies (25 percent) and advanced perimeter controls such as UTM, NGFW, IPS with reputation feeds and more (15 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



[8]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: formation of a senior-level security council (53 percent), appointment of a high-level security leader (53 percent) and certification against industry-leading standards (49 percent).

Figure 22. Seven enterprise security governance activities deployed

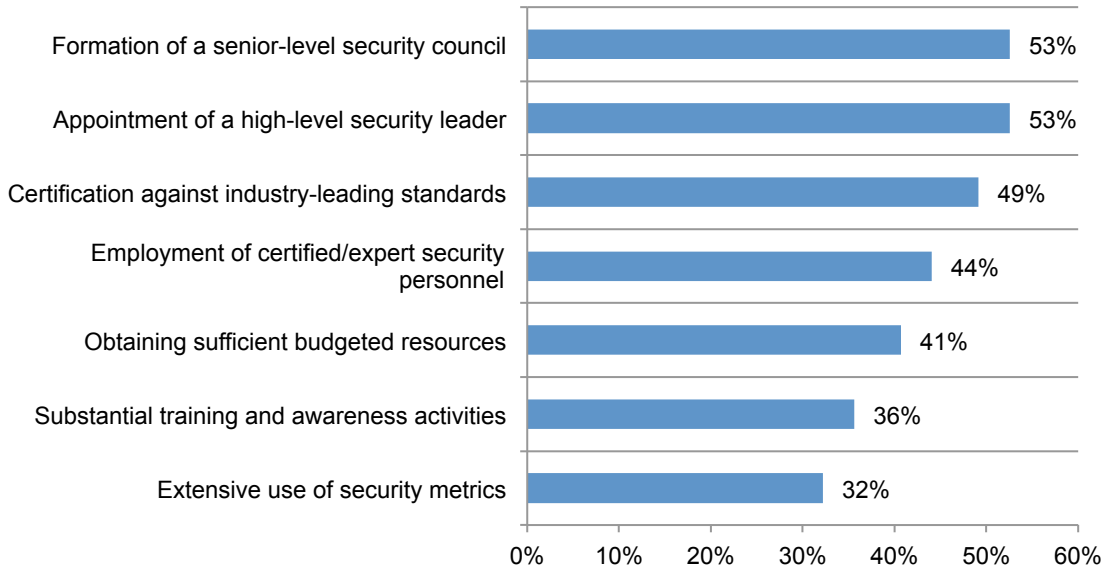
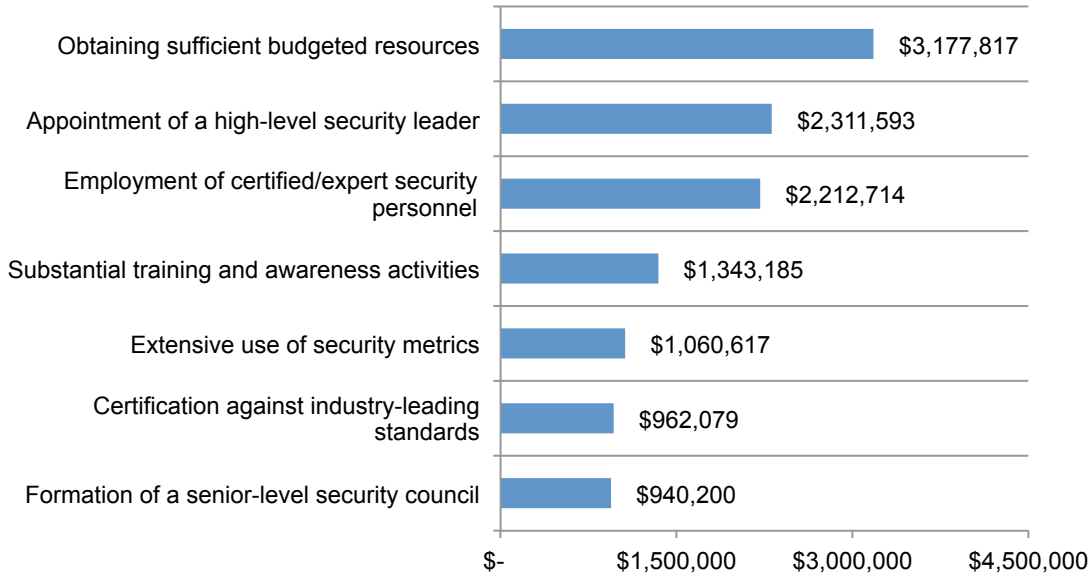


Figure 23 shows the incremental cost savings for each one of seven enterprise governance activities. As shown, companies obtaining sufficient resources save an average of $3.2 million. On average, companies appointing a high-level security leader (CISO) save $2.3 million. Similar to security technology categories, cost savings resulting from improved governance activities are independent of each other and cannot be added together.

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



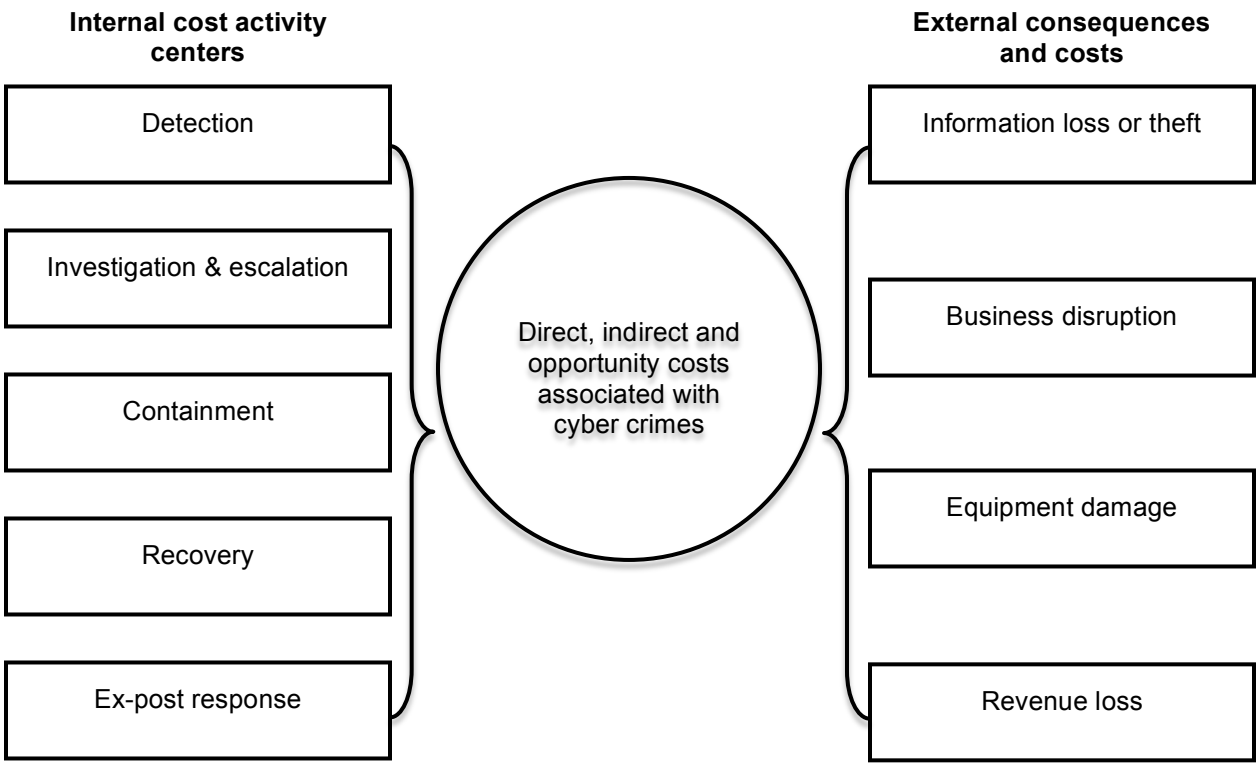
Part 3. Framework

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 (including stolen devices); malicious code (including SQL injection); and denial of services.[9]

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:[10]

- 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.

[9] We acknowledge that these seven 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.

[10] 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 5 reports the frequency of individuals by their approximate functional discipline that participated in this year's U.S. study. As can be seen, this year's study involved 544 interviews for each benchmarked company.[11]

Table 4: Functional areas of interview participants	**Frequency**	**Pct%**
IT security	99	18%
IT operations	94	17%
Compliance	63	12%
Legal	49	9%
Data center management	49	9%
Network operations	30	6%
IT risk management	26	5%
Accounting & finance	22	4%
Physical security/facilities mgmt	19	3%
Enterprise risk management	16	3%
Internal or IT audit	16	3%
Quality assurance	14	3%
Human resources	14	3%
Procurement/vendor mgmt	12	2%
Industrial control systems	11	2%
Application development	10	2%
Total	544	100%
Interviews per company	9.22	

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

[11]Last year's study involved 418 individuals or an average of 7.46 interviews for each benchmarked company.

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 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.

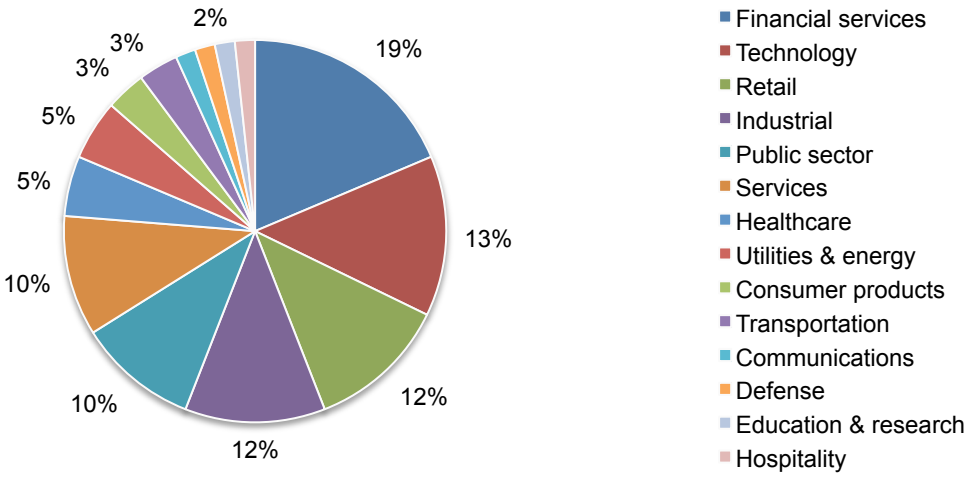
Field research was conducted over several months concluding in June 2014. To maintain consistency for all benchmark companies, information was collected about the organizations' cyber crime experience was limited to four consecutive weeks. This time frame was not necessarily the same time period as other 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 410 U.S.-based organizations for possible participation and[12]59 organizations permitted Ponemon Institute to perform the benchmark analysis.

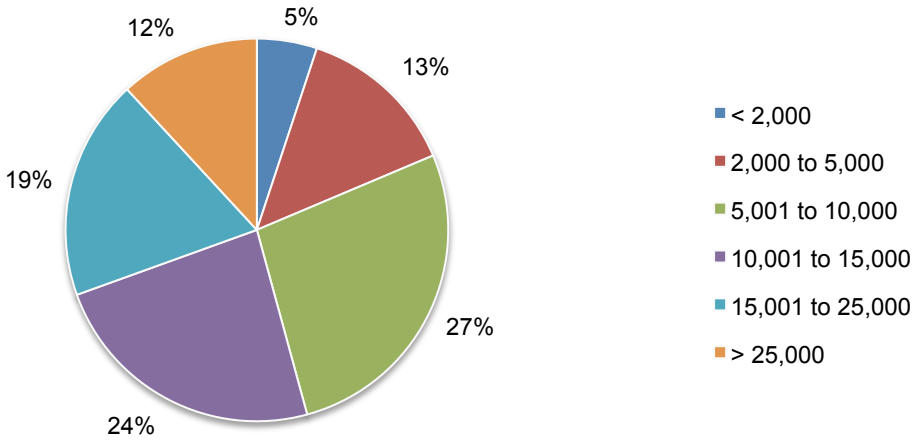
Pie Chart 1 summarizes the current (FY 2014) sample of participating companies based on 14 primary industry classifications. As can be seen, financial services (19 percent) represent the largest segment. This includes retail banking, insurance, brokerage and credit card companies. The second largest segments are technology and retail (both at 13 and 12 percent, respectively). The technology segment includes organizations in software and IT management.

Pie Chart 1. Industry sectors of participating organizations



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 over 1,000 seats. The largest enterprise has 125,000 seats.

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



[12]Approximately, half of the organizations contacted for possible participation in this year's study are members of Ponemon Institute's benchmarking community.

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, all US-based 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. Fifty-nine 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

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.