



2015 Cost of Cyber Crime Study: United States

Sponsored by Hewlett Packard Enterprise

Independently conducted by Ponemon Institute^{LLC}

Publication Date: October 2015

2015 Cost of Cyber Crime Study: United States

Benchmark Study of US Companies

Ponemon Institute October 2015

“A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11,” Leon E. Panetta (former US Secretary of Defense)

Part 1. Executive Summary

We are pleased to present the *2015 Cost of Cyber Crime Study: United States*, the sixth annual study of US companies. Sponsored by Hewlett Packard Enterprise, this year’s study is based on a representative sample of 58 organizations in both the public and private sectors. While our research focused on organizations located in the United States, most are multinational corporations.

This is the fourth year Ponemon Institute has conducted cyber crime cost studies for companies in the United Kingdom, Germany, Australia and Japan and the second year for the Russian Federation. This year we added Brazil.

The findings from this research are presented in separate reports.

The number of cyber attacks against US companies continues to grow in frequency and severity. Recent cyber attacks include Anthem Blue Cross and Blue Shield, United Airlines, Sabre Corp. and American Airlines.

In the public sector, the Office of Personnel Management sustained an attack that resulted in the theft of information about more than 4.2 million current and former federal employees and attacks against the Internal Revenue Service resulted in the theft of personal information about more than 100,000 taxpayers.

US Study at a Glance

58 US companies, 252 companies in 7 countries
553 interviews in the 58 US companies
638 cyber attacks used to measure total cost
\$15 million is the average annualized cost
19% net increase in cost over the past year
15% average ROI for 7 security technologies

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 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 seats¹). 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.

Cost of Cyber Crime FAQs

What is a cyber attack? A cyber attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructure, computer networks, and/or personal computer device by various means of malicious acts usually originating from an anonymous source that either steals, alters or destroys a specified target by hacking into a susceptible system.² The cost of cyber crime can vary according to the cause and the safeguards in place at the time of the attack.

How do you collect the data? Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a 10-month period. Fieldwork for the 2015 study began in January 2015 and interviews were completed in August 2015. In this year's study we interviewed 553 IT, compliance and information security practitioners who are knowledgeable about the cyber crime experienced by the organization and the costs associated with resolving the cyber attack. For privacy purposes we do not collect any organization-specific information.

How do you calculate the cost of cyber crime? To calculate the average cost of cyber crime, we analyzed 638 cyber attacks and collect both the direct and indirect expenses incurred by the organization. Direct expenses result from the direct expense outlay to accomplish a given activity. These can include engaging forensic experts and other consultants, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs result from the amount of time, effort and other organizational resources spent, but not as a direct cash outlay. Examples include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

How does benchmark research differ from survey research? The unit of analysis in the *Cost of Cyber Crime* study is the organization. In survey research, the unit of analysis is the individual. We recruited 58 large organizations with a minimum of approximately 1,000 enterprise seats to participate in this study.

Can the average cost of cyber crime be used to calculate the financial consequences of a mega cyber attack? The average cost of cyber crime in our research does not apply to catastrophic or mega security incidents because these are not typical of the cyber attack most organizations experience.

Are you tracking the same organizations each year? Each annual study involves a different sample of companies. In other words, we are not tracking the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount and geographic footprint. Since starting this research more than six years ago, we have studied the cyber crime experiences of 329 US organizations.

² Source: Wikipedia

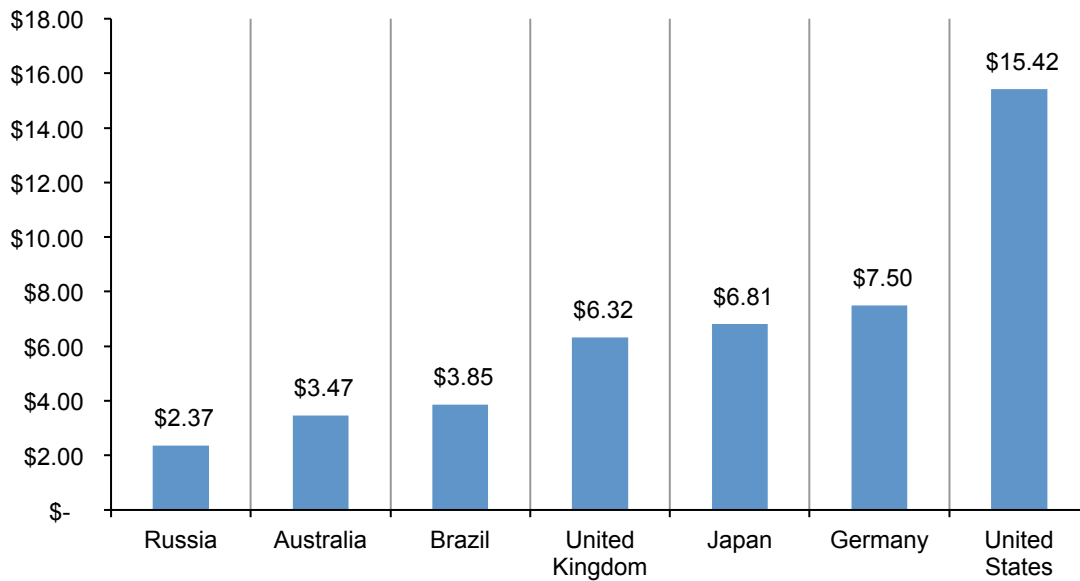
Global at a glance

This year's annual study was conducted in the United States, United Kingdom, Germany, Australia, Japan, the Russian Federation, and for the first time, Brazil, with a total benchmark sample of 252 organizations. These global results are presented in a separate reported entitled, *2015 Cost of Cyber Crime Study: Global*.

Figure 1 presents the estimated average cost of cyber crime for the seven countries represented in this research. These figures are converted into US 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 \$15 million and the RF sample reports the lowest total average cost at \$2.4 million³.

Figure 1. Global at a glance

\$1,000,000 omitted



³ For purposes of comparison, the country costs were converted from local currencies to US dollars. This conversion was influenced by exchange rate differences and a strong US dollar over the past year.

Summary of US findings

Following are the most salient findings for a sample of 58 US-based organizations requiring 553 separate interviews to gather cyber crime cost results. In several places in this report, we compare the present findings to the six-year average of benchmark studies.

Cyber crimes continue to be very costly for organizations. We found that the mean annualized cost for 58 benchmarked organizations is \$15 million per year, with a range from \$1.9 million to \$65 million each year per company. Last year's mean cost per benchmarked organization was \$12.7 million. Thus, we observe a \$2.7 million (19 percent) increase in mean value. The net increase over six years in the cost of cyber crime is 82 percent.

Cyber crime cost varies by organizational size. Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost.⁴ However, based on enterprise seats, we determined that small organizations incur a significantly higher per capita cost than larger organizations (\$1,571 versus \$667).

The cost of cyber crime increases for all industries. The average annualized cost of cyber crime appears to vary by industry segment, where organizations in financial services, energy & utilities and defense & aerospace experience a higher cost of cyber crime. Organizations in the consumer products and hospitality industries on average experience a much lower cost of cyber crime.

The most costly cyber crimes are those caused by denial of services, malicious insiders and malicious code. These account for more than 50 percent of all cyber crime costs per organization on an annual basis.⁵ 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 46 days, with an average cost to participating organizations of \$1,988,554 during this 46-day period. This represents a 22 percent increase from last year's estimated average cost of \$1,593,627, which was based upon a 45-day resolution period. Results show that malicious insider attacks can take an average of approximately 63 days to contain.

Information theft continues to represent the highest external cost, followed by the costs associated with business disruption.⁶ On an annualized basis, information theft accounts for 42 percent of total external costs. Costs associated with disruption to business or lost productivity account for 36 percent of external costs (up 4 percent from the six-year average).

Detection and recovery are the most costly internal activities. On an annualized basis, detection and recovery combined account for 55 percent of the total internal activity cost with cash outlays and direct labor representing the majority of these costs.

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

⁵This year the category malicious insider includes the cost of stolen devices.

⁶In 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. However, since 2013 this has declined from 40 percent to 36 percent in 2015. The application layer has increased in budget allocation from 15 percent in 2013 to 20 percent in 2015.

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 \$3.7 million when compared to companies not deploying security intelligence technologies.

Companies deploying security intelligence systems experienced a substantially higher ROI at 32 percent than all other technology categories presented. Also significant are the estimated ROI results for companies that extensively deploy encryption technologies (27 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, employ certified or expert staff and appoint a high-level security leader have cyber crime costs that are lower than companies that have not implemented these practices. Specifically, a sufficient budget can save an average of \$2.8 million, employment of certified/expert security personnel can save \$2.1 million and the appointment of a high-level security leader can reduce costs by \$2 million.

Part 2. Key findings

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

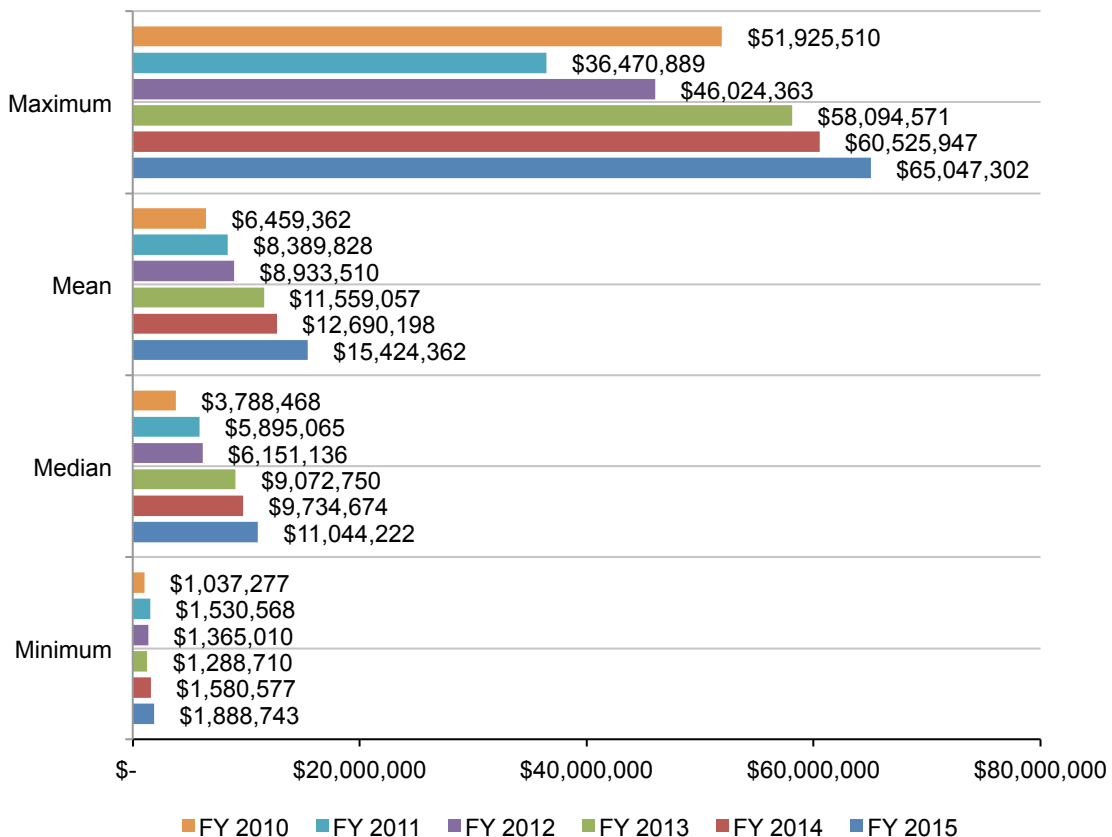
- **The average cost of cyber crime by organizational size and industry**
- **The type of attack influences the cost of cyber crime**
- **An analysis of the cost components of cyber crime**

The average cost of cyber crime by organizational size and industry

To determine the average cost of cyber crime, the 58 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.⁷

As shown in Figure 2, the total annualized cost of cyber crime in 2015 ranges from a low of \$1.89 million to a high of \$65 million. The median annualized cost of cyber crime in the benchmark sample is \$11 million – an increase from last year’s median value of \$9.7. The mean value is \$15.4 million. This is an increase of \$2.7 million or 19 percent from last year’s mean of \$12.7 million. The net increase over six years in the cost of cyber crime is 82 percent.

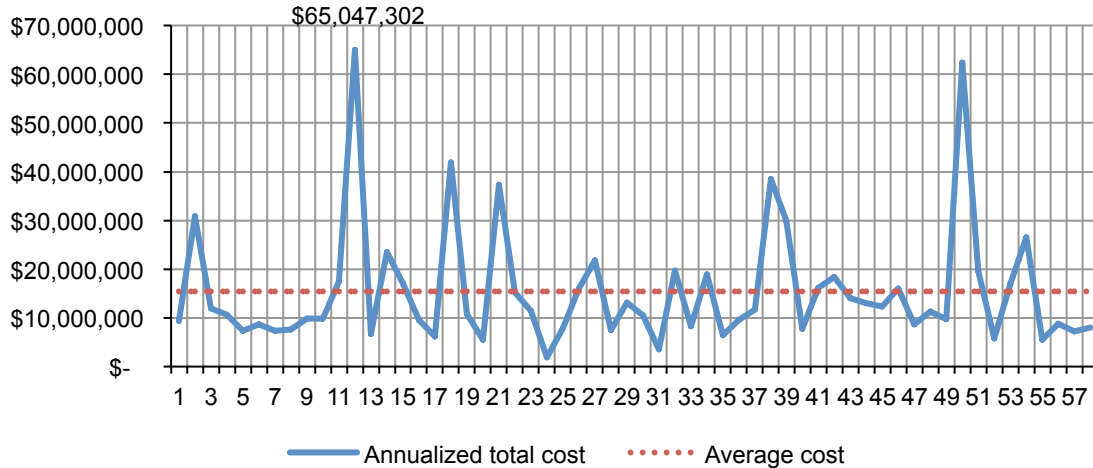
Figure 2. The cost of cyber crime



⁷Following is the gross-up statistic: Annualized revenue = [cost estimate]/[4/52 weeks].

Figure 3 reports the distribution of annualized total cost for 58 companies. As can be seen, 38 companies in our sample incurred total costs below the mean value of \$15 million, thus indicating a skewed distribution. The highest cost estimate of \$65 million was determined not to be an outlier based on additional analysis. Twenty other organizations experienced an annualized total cost of cyber crime above the mean value.

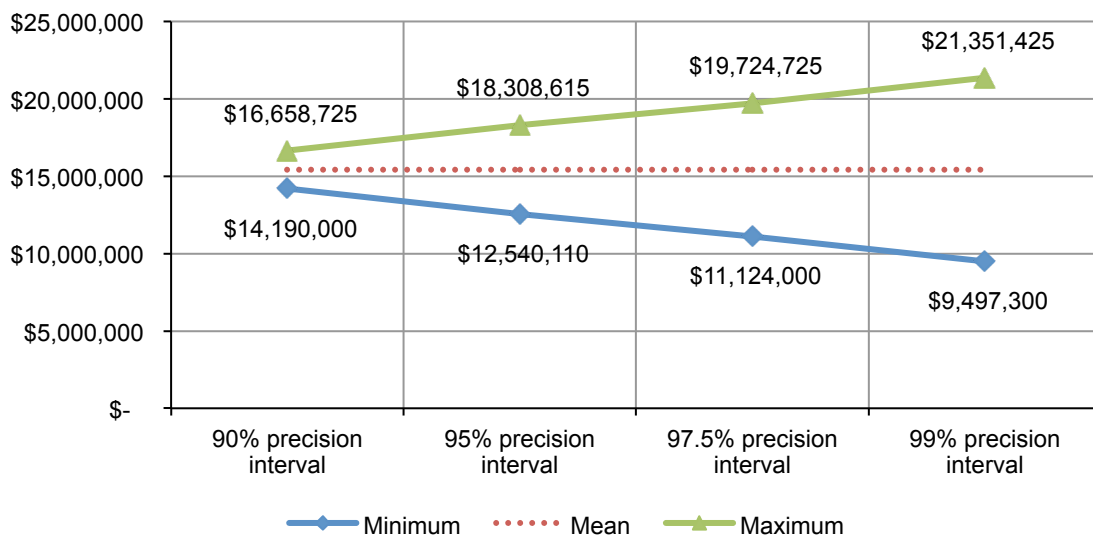
Figure 3. Annualized total cost of cyber crime for 58 participating companies



As part of our analysis we calculated a precision interval for the average cost of \$15 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.

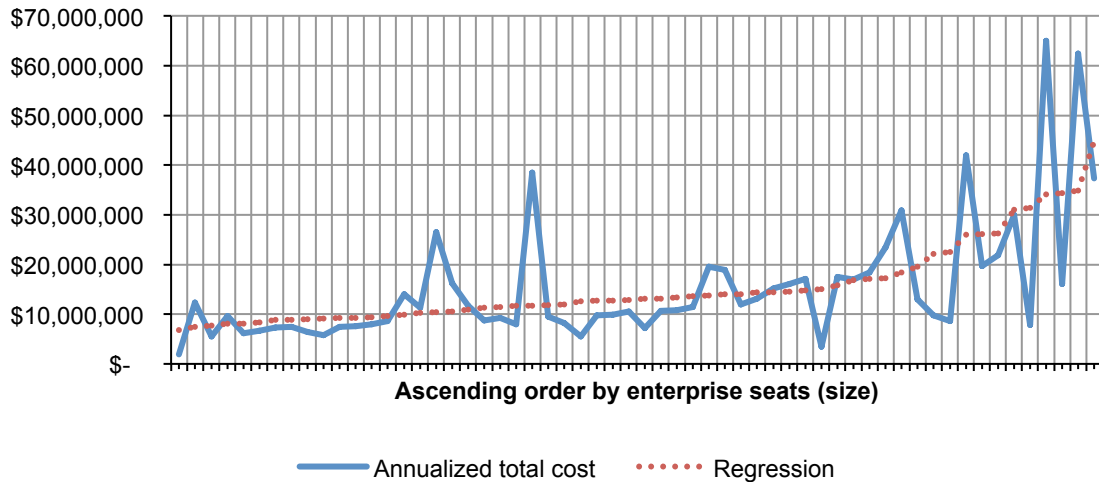
The range of possible cost estimates widens at increasingly higher levels of confidence, as shown in Figure 4. Specifically, at a 90 percent level of confidence we expect the range of cost to be between \$14.2 million to \$16.7 million.

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. The number of enterprise seats ranges from 1,063 to 75,199. This positive correlation is indicated by the upward sloping 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 six years. Approximately 14 companies are in each quartile.

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
FY 2015	\$6,170,526	\$9,334,141	\$14,030,298	\$31,452,625

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

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
FY 2015	\$1,571	\$1,276	\$854	\$667

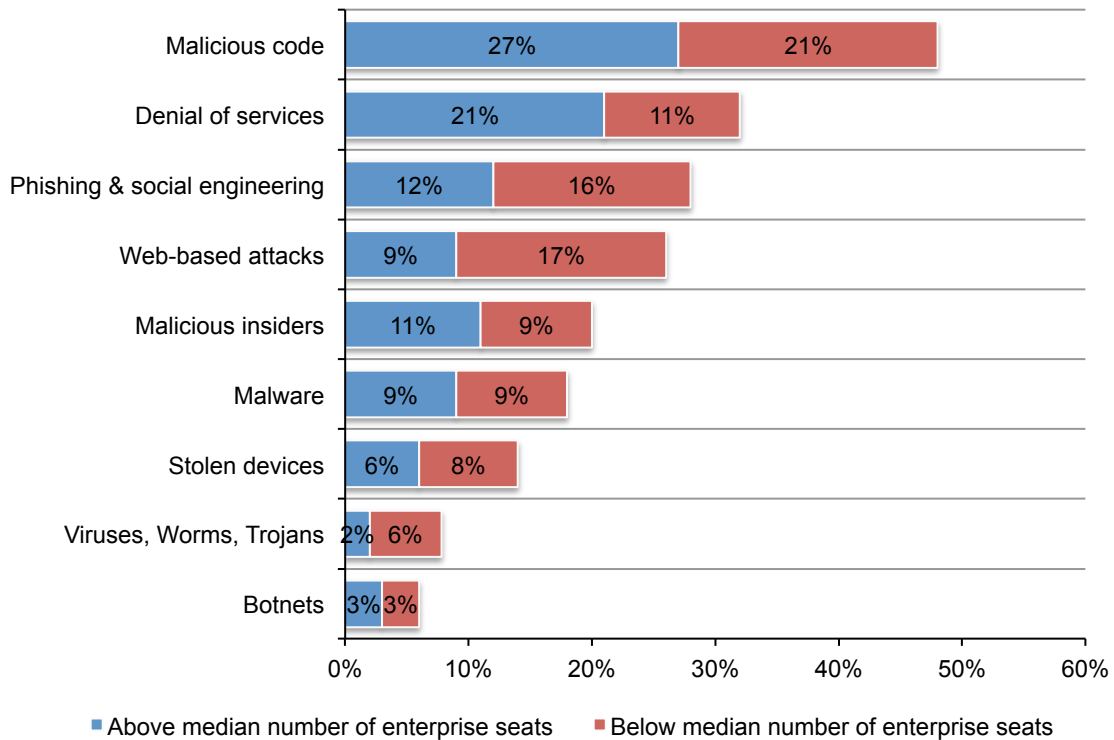
Certain attacks are more costly based on organizational size. The study focuses on nine different attack vectors as the source of the cyber crime. In the context of this research, malicious insiders include employees, temporary employees, contractors and, possibly other business partners. We also distinguish 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 attacks.

In Figure 6, we compare smaller and larger-sized organizations based on the sample median of 13,251 seats. Smaller organizations (below the median) experience a higher proportion of cyber crime costs relating to phishing & social engineering, web-based attacks and stolen devices (16 percent, 17 percent and 8 percent of total costs, respectively).

Similarly, larger organizations (above the median) experience a higher proportion of costs relating to malicious code (27 percent of total costs). They also have a higher incidence of denial of services (21 percent of total costs) and malicious insiders (11 percent).

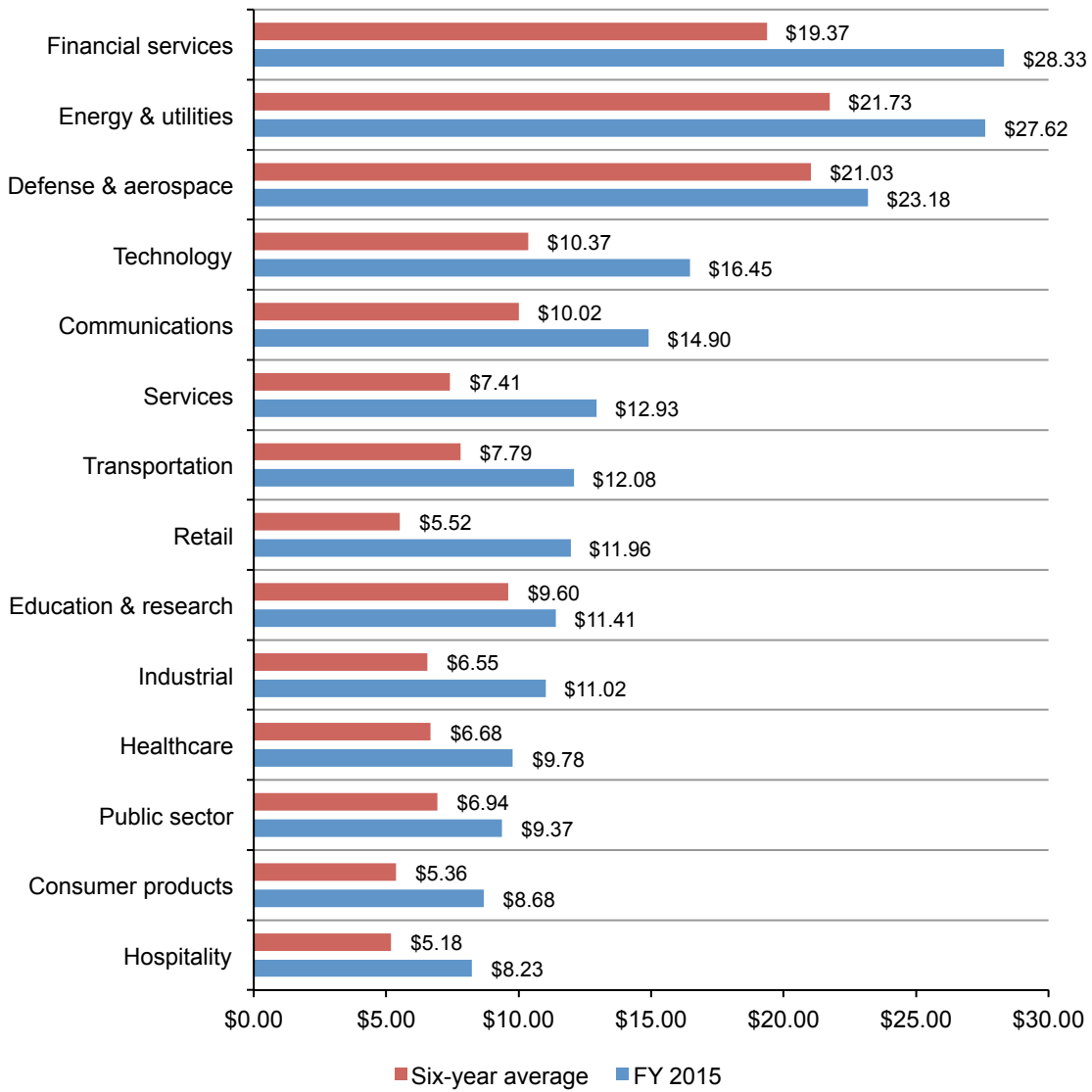
Figure 6. Percentage of total cost for nine attack types by organizational size

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



The cost of cyber crime increases for all industries. The average annualized cost of cyber crime appears to vary by industry segment. In this year's study we compare the 2015 results to the six-year average. As shown in Figure 7, the cost of cyber crime for most industries has increased significantly since the study was conducted six years ago. This is especially the case for financial services (an increase of \$8.96 million), energy & utilities (an increase of \$5.89 million), technology (an increase of \$6.08 million) and retail (an increase of \$6.44).⁸

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



⁸This analysis is for illustration purposes only. The sample size in all six years makes its difficult to draw definitive conclusions about industry segment differences.

The type of cyber attack influences the cost of cyber crime

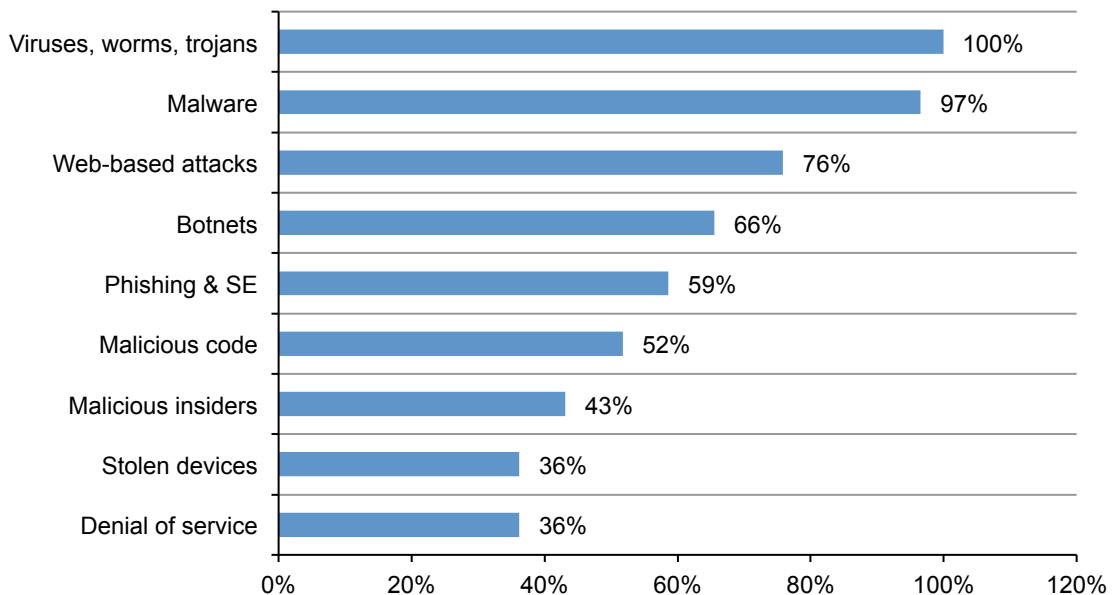
In our studies we look at nine different attack vectors as the source of the cyber crime. This year, the benchmark sample of 58 organizations experienced 160 discernible cyber attacks per week, which translates to 2.8 successful attacks per benchmarked organization each week. The list below shows the number of successful attacks for the five previous years of this research. It is clear how the number of attacks per week have steadily increased.

- FY 2014 138 attacks in 59 organizations
- 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 web-based attacks and botnets affected 66 percent of companies. The majority of companies experienced phishing and social engineering attacks (59 percent) and malicious code (52 percent). Only 36 percent of companies say a stolen device or denial of service was the source of the cyber crime.

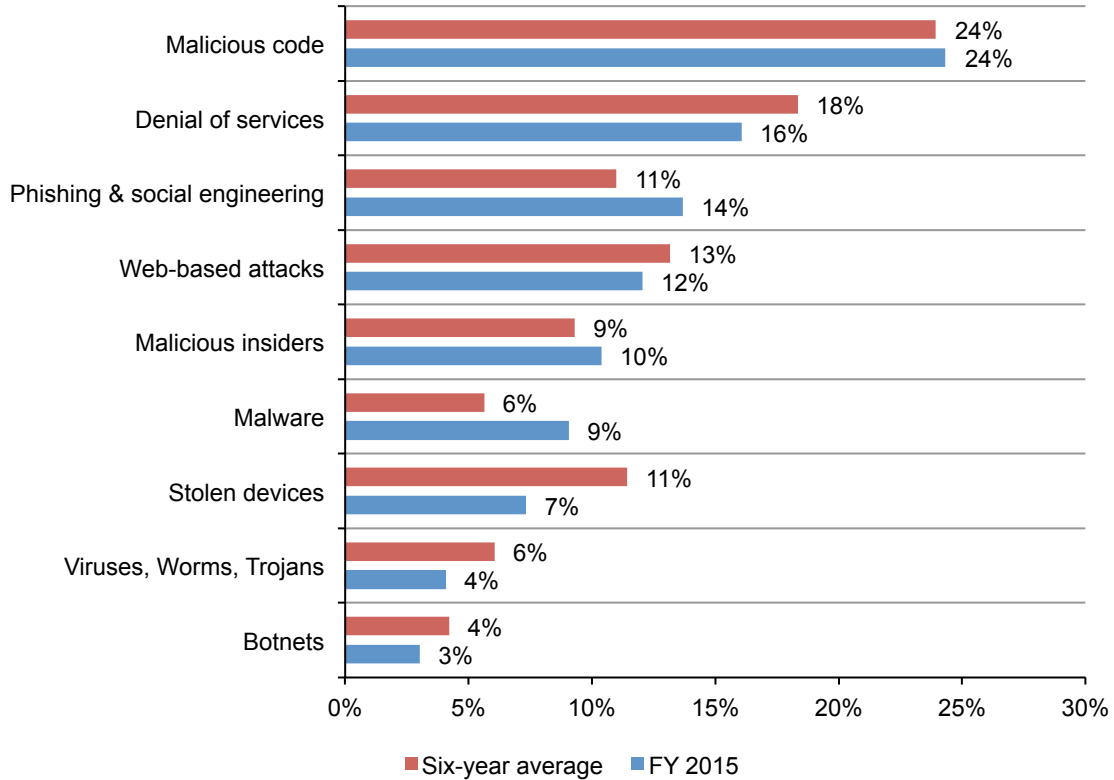
Figure 8. Types of cyber attacks experienced by 58 benchmarked companies



Costs vary considerably by the type of cyber attack. Figure 9 compares benchmark results of 2015 to the past six 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 50 percent of the total annualized cost of cyber crime experienced by 58 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 stolen devices.

Figure 9. Percentage annualized cyber crime cost by attack type

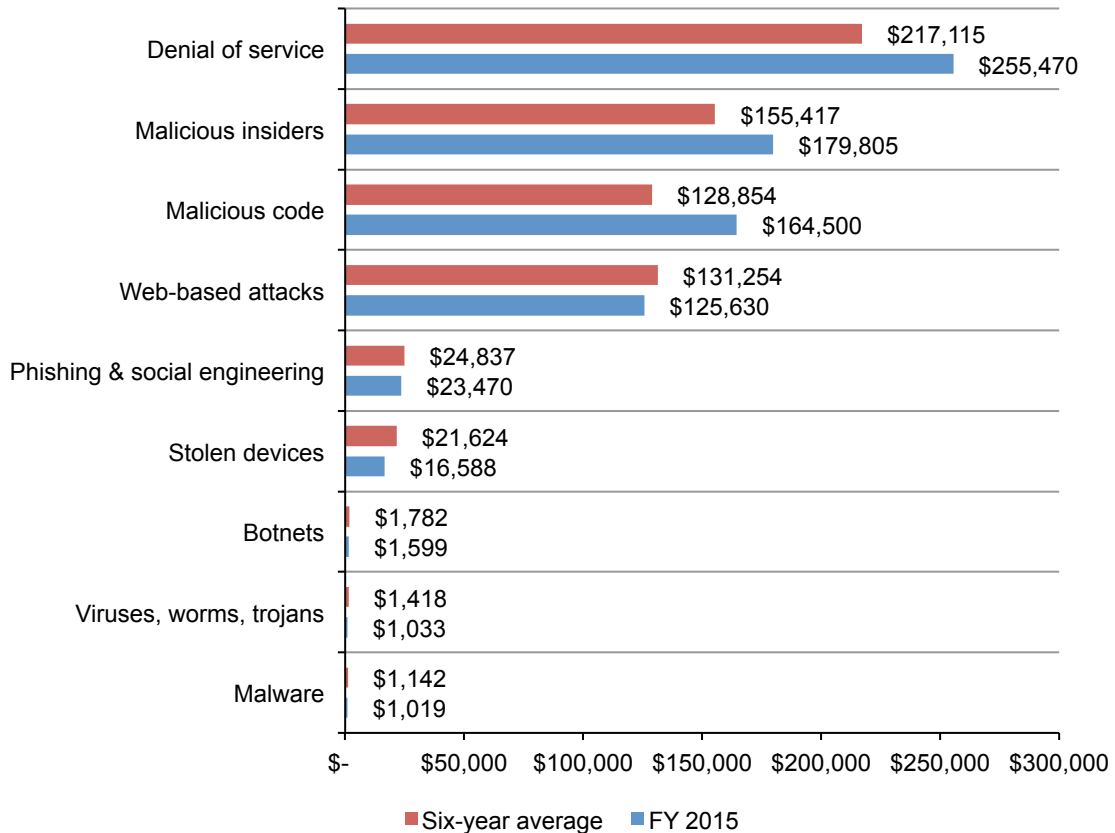


The cost of cyber crime is also influenced by the frequency of the different attack types.

Figure 10 reveals the most to least expensive cyber attacks when analyzed on the frequency of incidents. The most expensive attacks continue to be denial of services, malicious insiders and malicious code. As discussed previously, these attacks represent 50 percent of total annualized cost (Figure 9).

Over the past six years, average costs increased significantly for the following attack categories: denial of service increased by \$38,355, malicious code rose by \$35,646 over the six-year average and malicious insiders increased \$24,388. In the context of our study, malicious insiders include employees, temporary employees, contractors and, possibly, business partners. The other attack categories decreased slightly in cost.

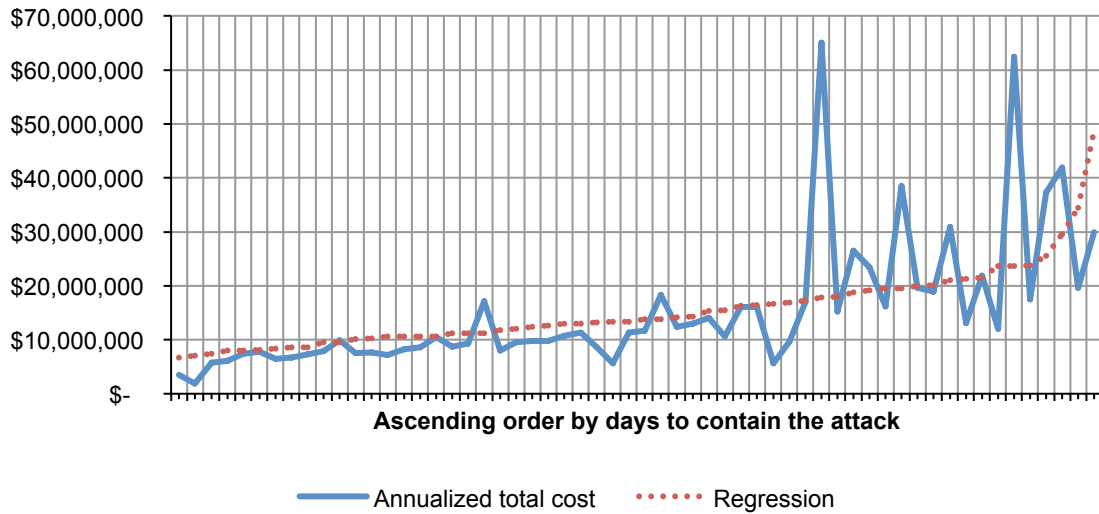
Figure 10. Average annualized cyber crime cost weighted by attack frequency



Time to resolve or contain cyber crimes increases the cost. The mean number of days to resolve cyber attacks is 46 with an average cost of \$43,327 per day – or a total cost of approximately \$2 million the 46-day remediation period. This represents a 22 percent increase from last year’s cost estimate of \$1.6 million for a 45-day resolution period. 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.

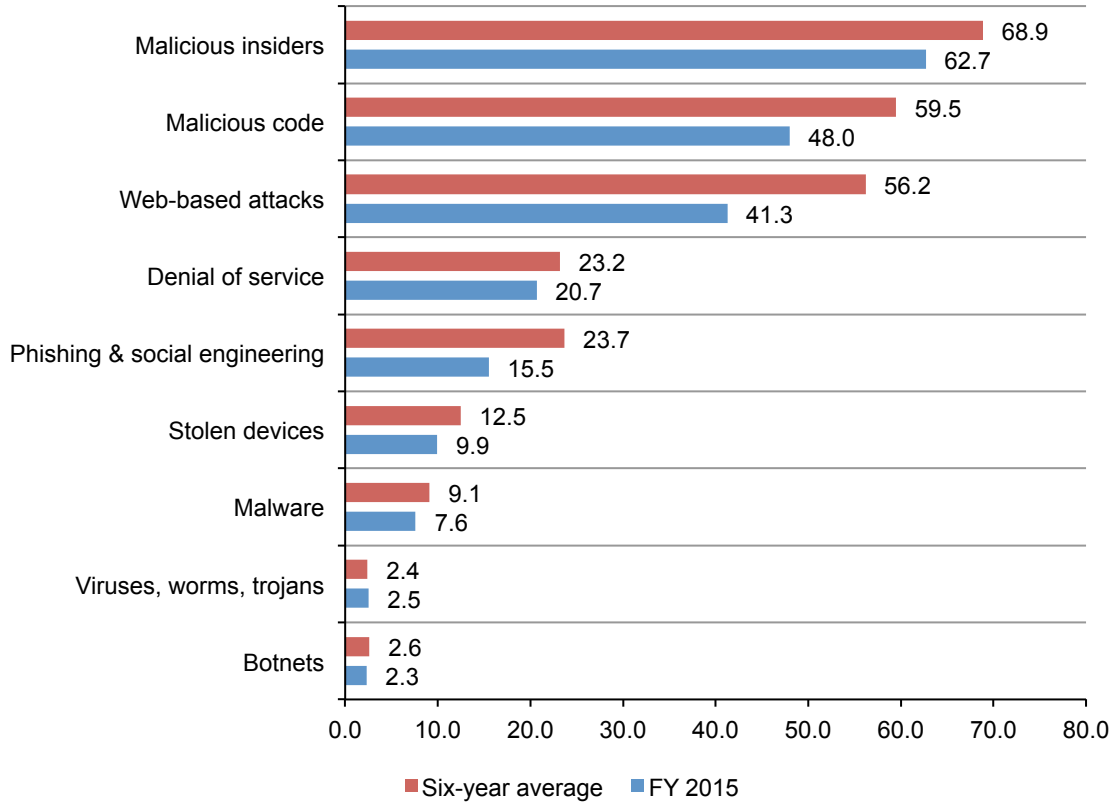
Figure 11. Total annualized cost by the number of days to contain the attack



Some attacks take longer to resolve and as a result are more costly. While the average number of days to resolve a cyber attack is 46 days, Figure 12 reports certain attacks take much longer to remediate. These include malicious insiders and malicious code. On a positive note, companies are becoming more effective in reducing the number of days to deal with a cyber attack for most nine attack types.

Figure 12. Average days to resolve attack by attack type

Estimated average time is measured for each attack type in days

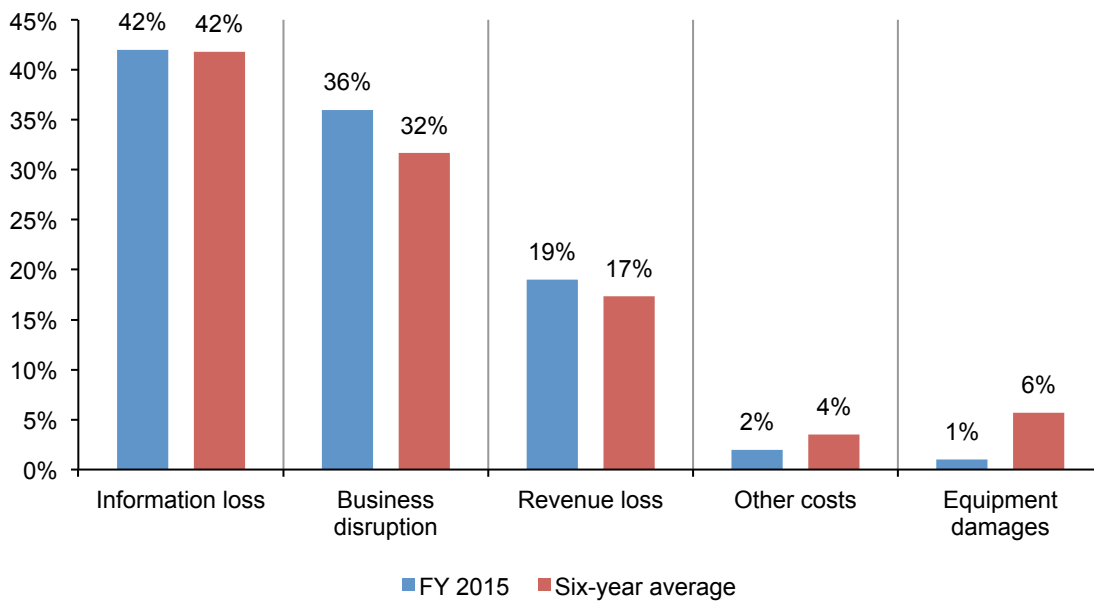


An analysis of the cost components of cyber crime

Information theft remains the most expensive consequence of a cyber crime. In this research we look at four primary consequences of a cyber attack: 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 (42 percent) of the total cost to an organization that has a cyber attack. This is consistent with the six-year average of 42 percent.

Business disruption or loss of productivity has increased slightly to 36 percent from the six-year average of 32 percent of total costs. Revenue losses (19 percent) and equipment damages (1 percent) yield a much lower cost impact.

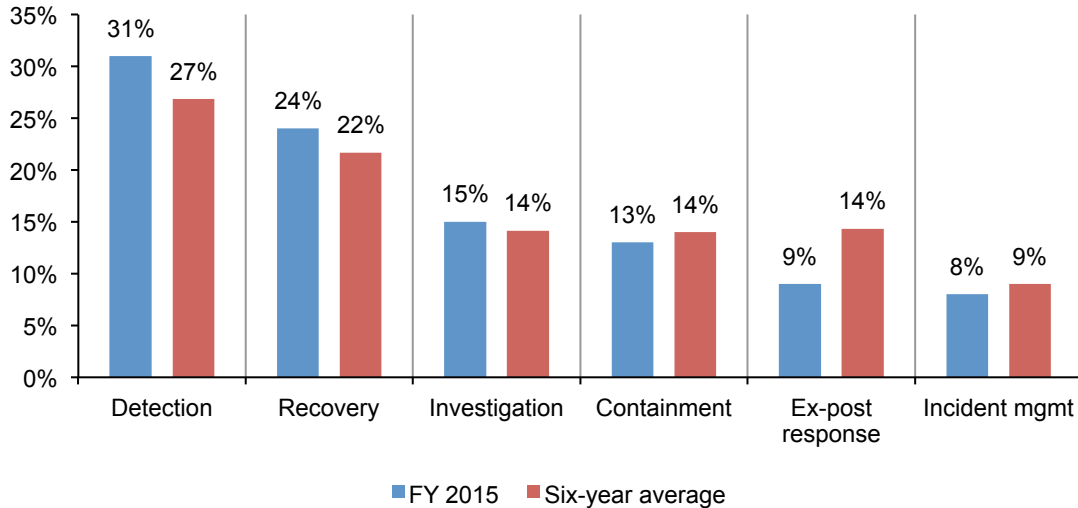
Figure 13. Percentage cost for external consequences



Companies spend the most on recovery and detection. Cyber crime detection and recovery activities account for 55 percent of total internal activity cost (49 percent is the six-year average), as shown in Figure 14. This is followed by investigation and containment (15 percent and 13 percent, respectively).

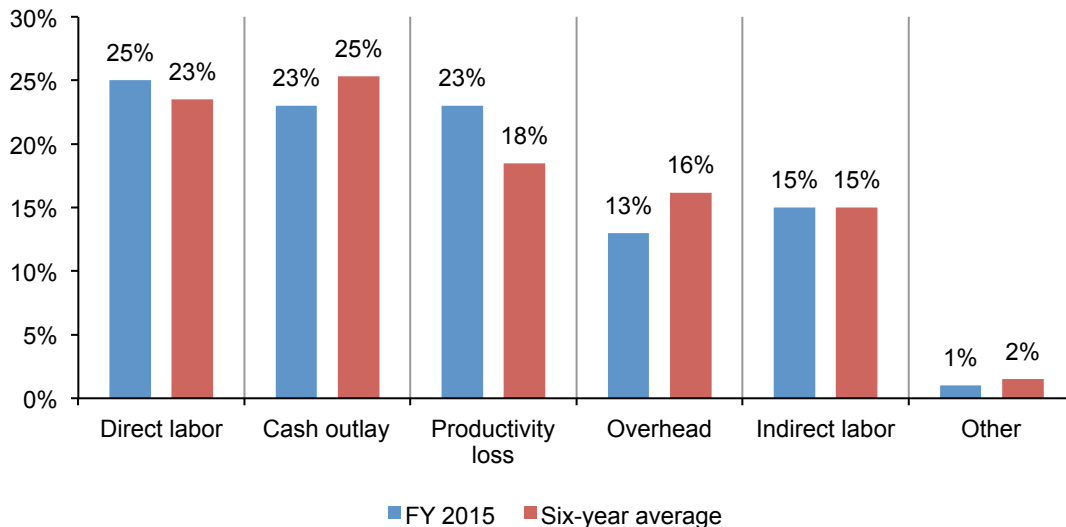
Detection and recovery cost elements highlight a significant cost-reduction opportunity for organizations that are able to systematically manage recovery and deploy enabling security technologies to help facilitate the detection process.

Figure 14. Percentage cost by internal activity center



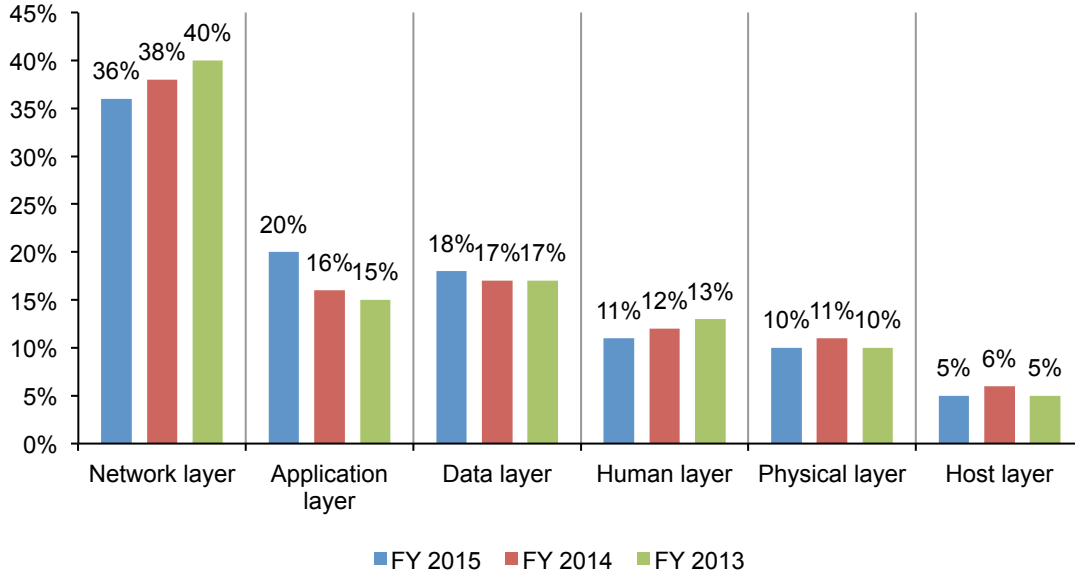
The percentage of annualized costs can be further broken down into specific expenditure components, which include: direct labor (25 percent), cash outlays (23 percent), productivity losses (23 percent), overhead (13 percent) and indirect labor (15 percent). Costs not included in these components are represented in “other”. As shown in Figure 15, the cash outlays and overhead costs have decreased over six years. In contrast, direct labor and productivity losses have increased over six years.

Figure 15. Percentage activity cost by 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 of spending dedicated to each layer. The network layer receives the highest allocation at 36 percent of total dedicated IT security funding. At only 5 percent, the host layer receives the lowest funding level.

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



Organizations deploying security intelligence technologies realize a lower annualized cost of cyber crime. Figure 17 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 (50 percent) deploy security intelligence tools such as SIEM, IPS with reputation feeds, network intelligence systems, big data analytics and others.

In every case, 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 (\$5.70 vs. \$3.80) and incident management (\$1.55 vs. \$0.54).

Figure 17. Activity cost comparison and the use of security intelligence technologies
 \$1,000,000 omitted

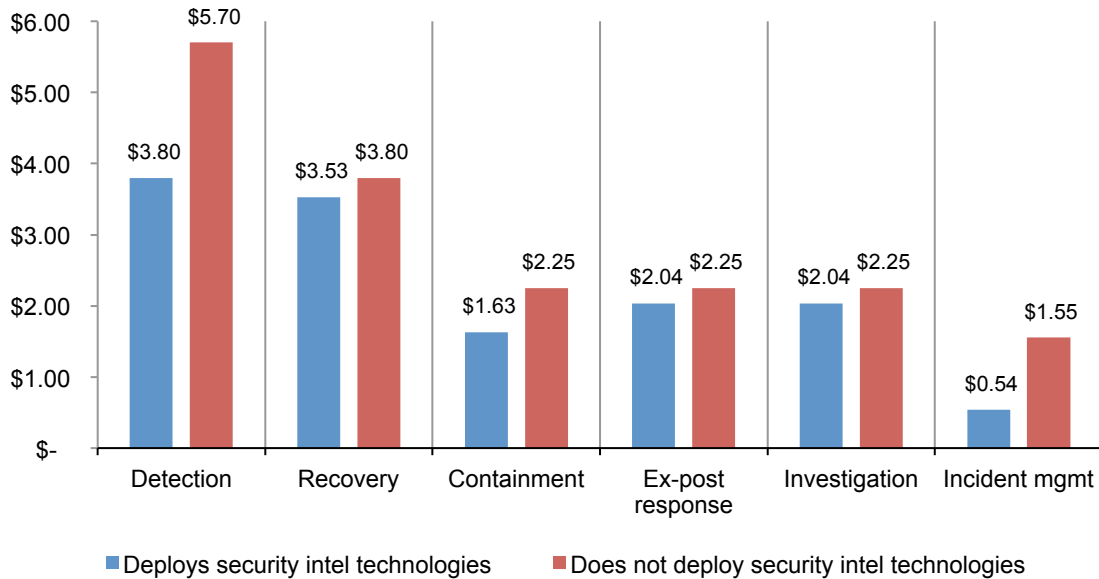


Figure 18 shows seven enabling security technology categories experienced by a subset of benchmarked companies. Each bar represents the percentage of companies fully deploying each given security technology. The top three technology categories include: advanced perimeter control and firewall technologies (64 percent), enterprise encryption technologies (57 percent), and security intelligence systems (50 percent).

Figure 18. Seven enabling security technologies deployed

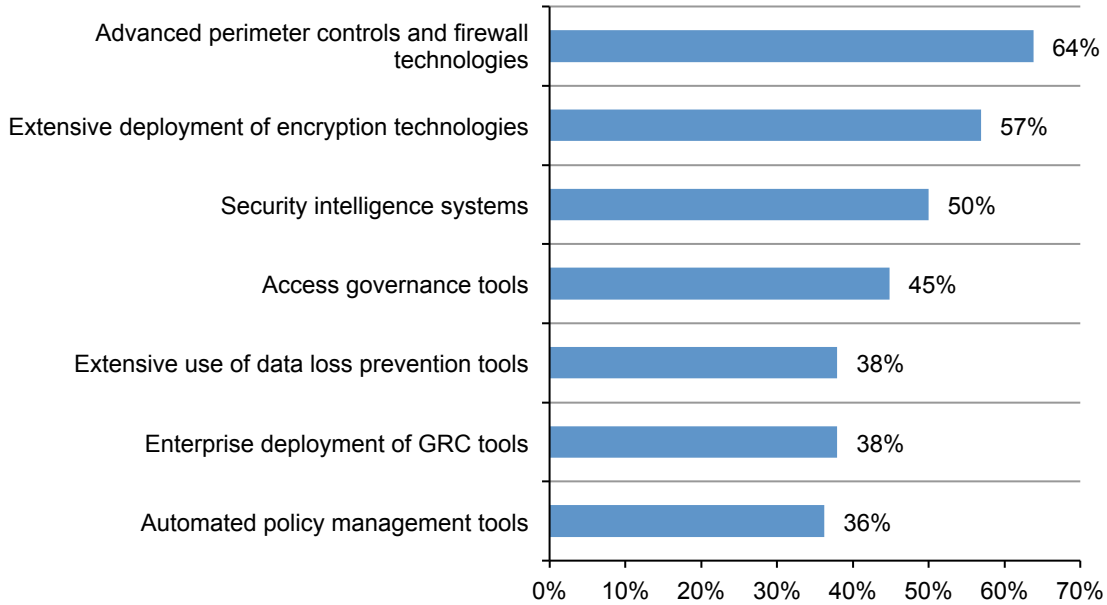
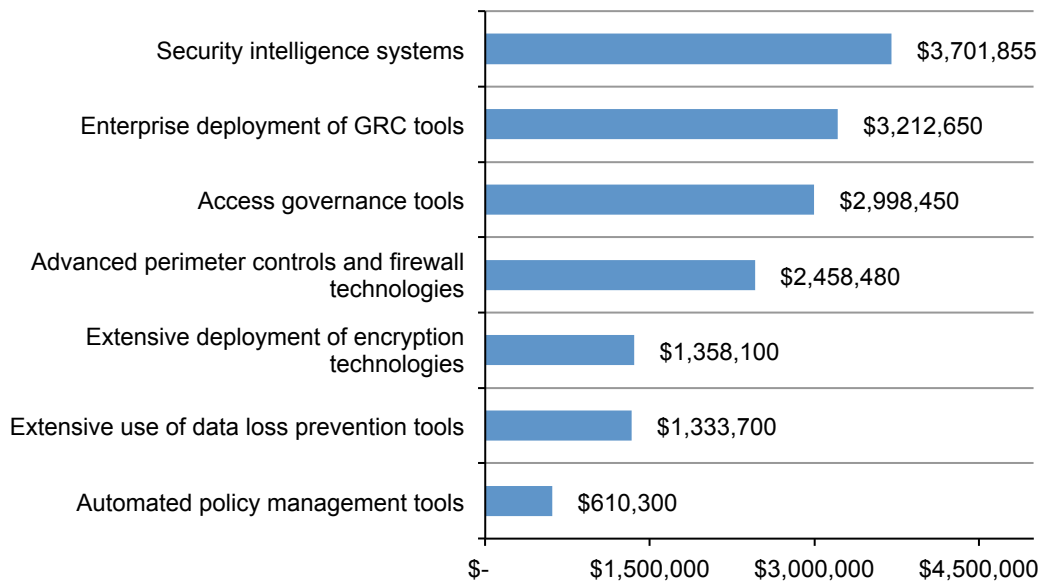


Figure 19 shows the money companies can save by deploying each one of seven enabling security technologies. For example, companies deploying security intelligence systems, on average, experience a substantial cost savings of \$3.7 million. Similarly, companies deploying enterprise GRC tools save \$3.2 million on average. Please note that these extrapolated cost savings are independent of each other and cannot be added together.

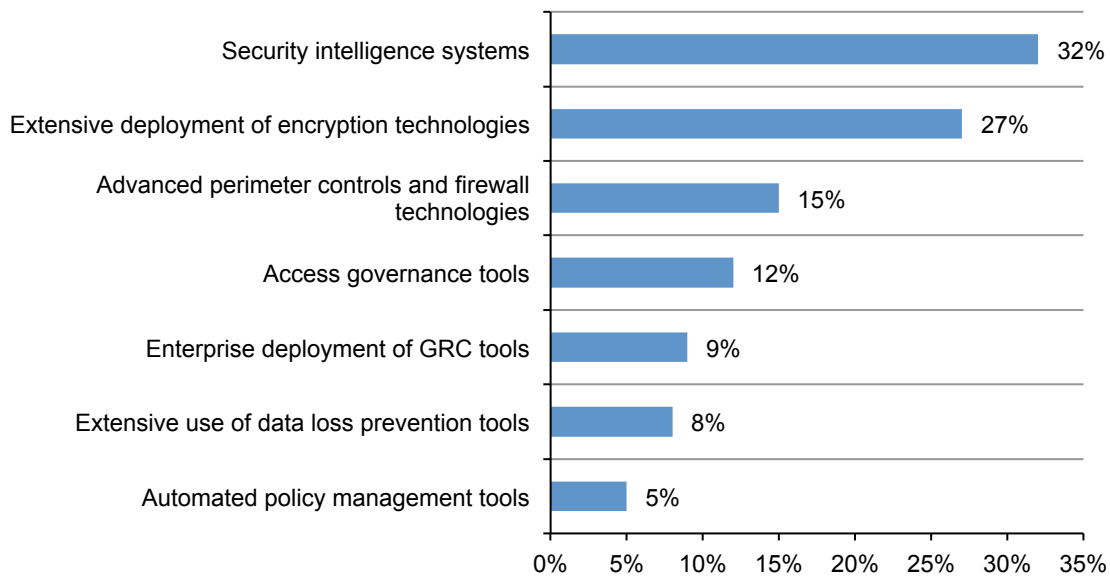
Figure 19. Cost savings when deploying seven enabling security technologies



Security intelligence systems have the biggest return on investment. Figure 20 summarizes the estimated return on investment (ROI) realized by companies for each one of the seven categories of enabling security technologies indicated above.⁹ At 32 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 (27 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 20. Estimated ROI for seven categories of enabling security technologies



⁹The 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 21 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: appointment of a high-level security leader (57 percent), certification against industry-leading standards (53 percent) and formation of a senior-level security council (52 percent).

Figure 21. Seven enterprise security governance activities deployed

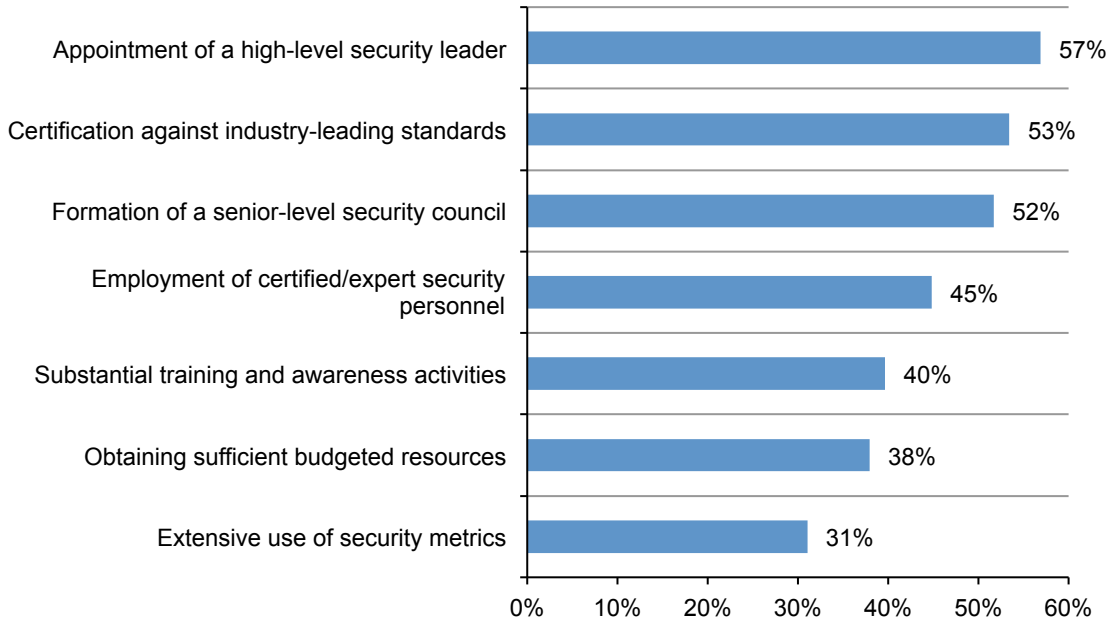
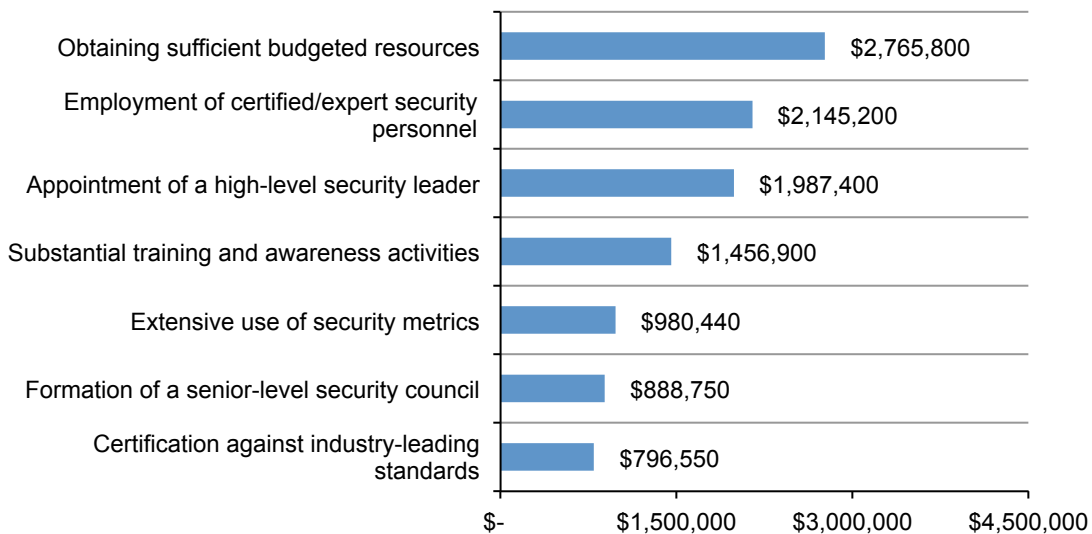


Figure 22 shows the incremental cost savings for each one of seven enterprise governance activities. As shown, companies with sufficient budget save an average of \$2.8 million. On average, companies employing certified and expert security personnel can save \$2.1 million. Similar to security technology categories, cost savings resulting from improved governance activities are independent of each other and cannot be added together.

Figure 22. Cost savings when executing seven enterprise security governance activities



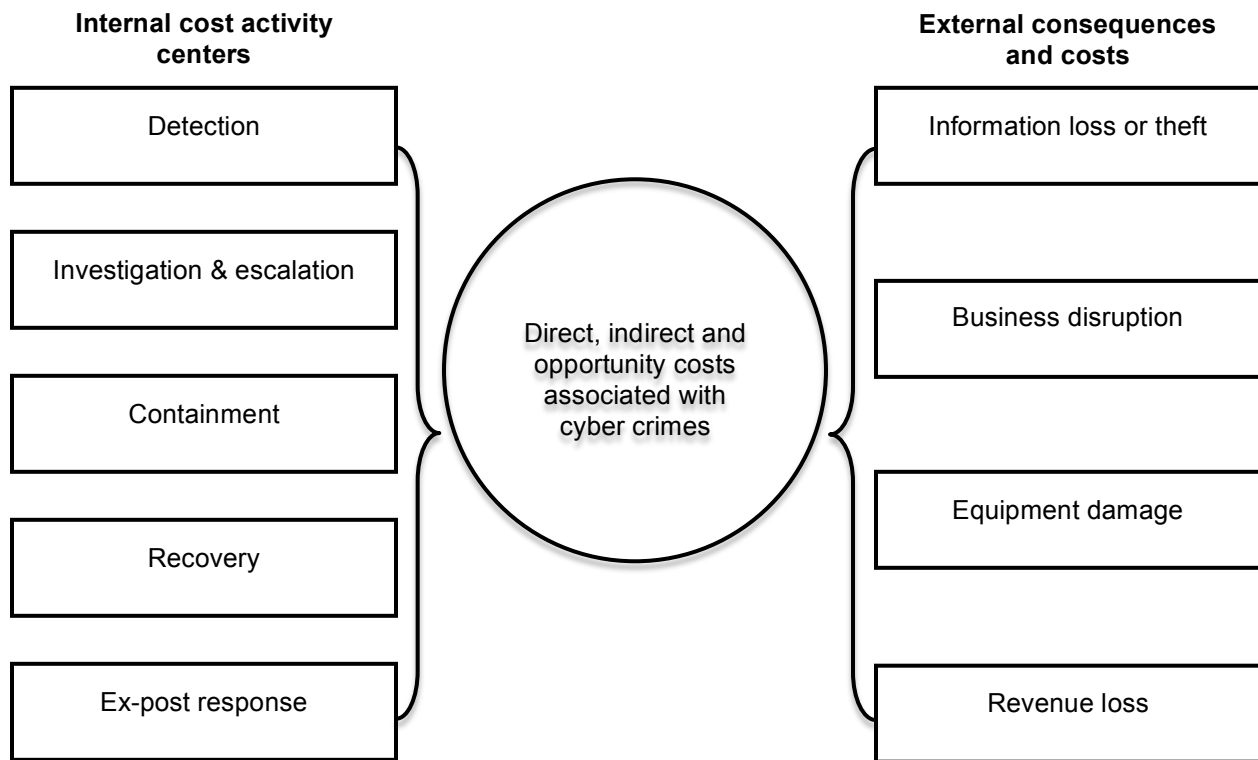
Part 3. Framework

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 23 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 23. 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 and damaged devices; malicious code (including SQL injection); and denial of services.¹⁰

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:¹¹

- 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.

¹⁰ 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.

¹¹ 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 US study. As can be seen, this year’s study involved 553 interviews for each benchmarked company.¹²

Table. Functional areas of interview participants	FY 2015	Pct%
IT security	113	20%
IT operations	88	16%
Compliance	65	12%
Data center management	50	9%
Legal	44	8%
Network operations	28	5%
IT risk management	23	4%
Accounting & finance	23	4%
Physical security/facilities mgmt	18	3%
Internal or IT audit	17	3%
Human resources	16	3%
Enterprise risk management	15	3%
Procurement/vendor mgmt	15	3%
Quality assurance	13	2%
Application development	13	2%
Industrial control systems	12	2%
Total	553	100%
Interviews per company on average	9.37	

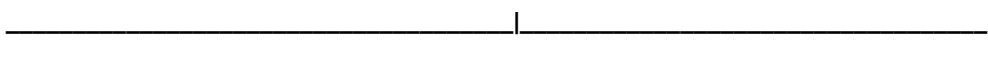
Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant. Within each category, cost estimation was a two-stage process. First, the benchmark instrument required

¹²Last year’s study involved 544 individuals or an average of 9.22 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.

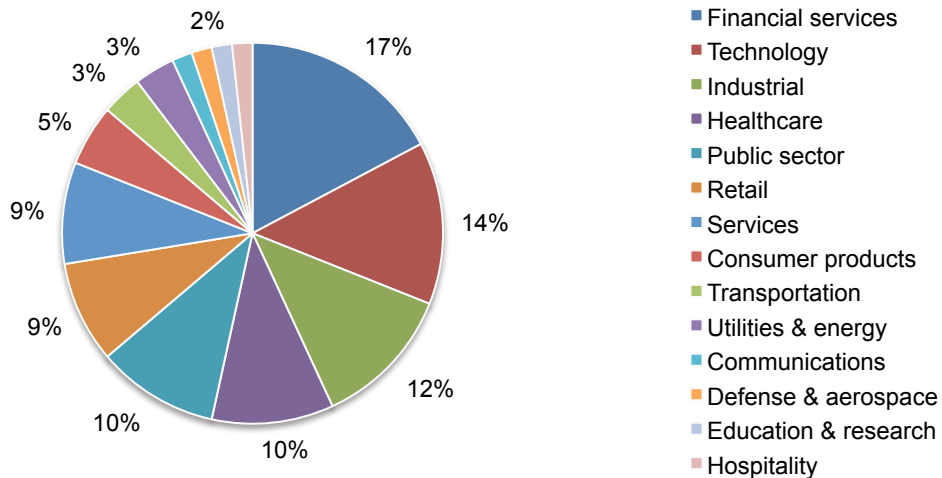
Field research was conducted over several months concluding in August 2015. To maintain consistency for all benchmark companies, information was collected about the organizations' cyber crime experience was limited to four consecutive weeks. This time frame was not necessarily the same time period as 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 458 U.S.-based organizations for possible participation and ¹³58 organizations permitted Ponemon Institute to perform the benchmark analysis.

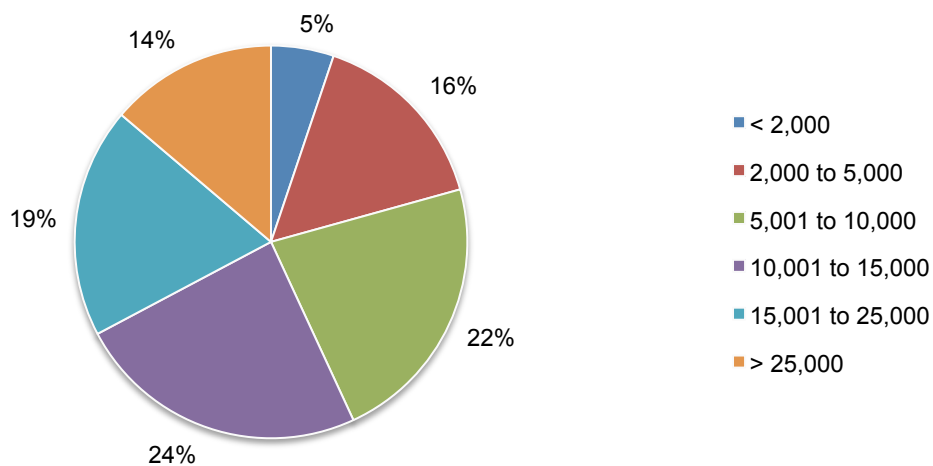
Pie Chart 1 summarizes the current (FY 2015) sample of participating companies based on 14 primary industry classifications. As can be seen, financial services (17 percent) represent the largest segment. This includes retail banking, insurance, brokerage and credit card companies. The second largest segments are technology and industrial (at 14 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)



¹³Approximately, 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 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-eight 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.