Ponemon INSTITUTE

Second Annual Cost of Cyber Crime Study

Benchmark Study of U.S. Companies

Sponsored by ArcSight, an HP Company

Independently conducted by Ponemon Institute LLC

Publication Date: August 2011

Second Annual Cost of Cyber Crime Study

Benchmark Study of U.S. Companies

Ponemon Institute August 2011

Part 1. Executive Summary

Sponsored by ArcSight, an HP company, we are pleased to present the Second Annual Cost of Cyber Crime Study. This year's study is based on a representative sample of 50 organizations in various industry sectors. While our research focused on organizations located in the United States, many are multinational corporations. For consistency purposes, our benchmark sample consists of only larger-sized organizations (i.e., more than 700 enterprise seats).

Despite widespread awareness of the impact of cybercrime, cyber attacks continue to occur frequently and result in serious financial consequences for businesses and government institutions. Key takeaways from this report include:

- Cyber crimes can do serious harm to an organization's bottom line. We found that the median annualized cost of cyber crime for 50 organizations in our study is $5.9 million per year, with a range of $1.5 million to $36.5 million each year per company. This represents an increase in median cost of 56 percent from our first cyber cost study published last year.[1]
- Cyber attacks have become common occurrences. The companies in our study experienced 72 successful attacks per week and more than one successful attack per company per week. This represents an increase of 44 percent from last year's successful attack experience.
- The most costly cyber crimes are those caused by malicious code, denial of service, stolen devices and web-based attacks. Mitigation of such attacks requires enabling technologies such as SIEM and enterprise governance, risk management and compliance (GRC) solutions.

Similar to last year, the purpose of this benchmark research 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 devastating consequences of an attack.

Cyber attacks generally refer to 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. Recent well-publicized cyber attacks – for instance, Wikileaks, Epsilion, Sony, Citibank, Boeing, Google, and RSA – have affected private and public sector organizations.

As described above, our goal is to be able to quantify with as much accuracy as possible the costs incurred by organizations when they have a cyber attack. In our experience, a traditional survey approach would not capture the necessary details required to extrapolate cyber crime costs. Therefore, we decided to pursue field-based research that involved interviewing senior-level personnel and collecting details about actual cyber crime incidents. Approximately nine months of effort was required to recruit companies, build an activity-based cost model, collect source information and analyze results.

This research culminated with the completion of case studies involving 50 organizations. The focus of our project was the direct, indirect and opportunity costs that resulted from the loss or theft of information, disruption to business operations, revenue loss and destruction of property, plant and equipment. In addition to external consequences of the cyber crime, the analysis attempted to capture the total cost spent on detection, investigation, containment, recovery and after-the-fact or "ex-post" response.

[1] See the First Annual Cost of Cyber Crime Study, Ponemon Institute, July 2010.

Summary of key findings

Following are the most salient findings of this year's study. In several places we compare the present finding compiled from a sample of 50 benchmark organizations to a separate sample of 45 organizations published in July 2010.[2]

Cyber crimes continue to be very costly for organizations. We found that the median annualized cost for 50 benchmarked organizations is $5.9 million per year, with a range from $1.5 million to $36.5 million each year per company. Last year's median cost per benchmarked organization was $3.8 million. Thus, we observe a $2.1 million (56 percent) increase in median values.

Cyber crime cost varies by organizational size. Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost. However, based on enterprise seats, we determine that smaller-sized organizations incur a significantly higher per capita cost than larger-sized organizations ($1,088 versus $284).

Cyber crimes are intrusive and common occurrences. The companies participating in our study experienced 72 successful attacks per week – or more than 1.4 successful attacks per organization. When compared to last year's study, this represents a 44 percent increase in successful attacks experienced by organizations.

The most costly cyber crimes are those caused by malicious code, denial of service, stolen or hijacked devices and malicious insiders. These account for more than 90 percent of all cyber crime costs per organization on an annual basis. Mitigation of such attacks requires enabling technologies such as SIEM 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. The average time to resolve a cyber attack is 18 days, with an average cost to participating organizations of $415,748 over this 18 day period. This represents a 67 percent increase from last year's estimated average cost of $247,744, which is compiled for a 14 day period. Results show that malicious insider attacks can take more than 45 days on average to contain.

Information theft continues to represent the highest external cost, followed by the costs associated with business disruption. On an annualized basis, information theft accounts for 40 percent of total external costs (down 2 percent from 2010). Costs associated with disruption to business or lost productivity account for 28 percent of external costs (up 6 percent from 2010).

Recovery and detection are the most costly internal activities. On an annualized basis, recovery and detection combined account for 45 percent of the total internal activity cost with cash outlays and labor representing the majority of these costs.

Enterprise deployment of SIEM makes a difference. The cost of cyber crime is moderated by the use of SIEM technologies. We found a percentage cost difference between SIEM and non-SIEM companies of 24 percent. Findings suggest companies using SIEM were better able to quickly detect and contain cyber crimes than those companies not using SIEM. As a result, SIEM companies experienced a substantially lower cost of recovery, detection and containment than non-SIEM companies. In addition, SIEM companies were more likely to recognize the existence of advance persistent threats (APTs) than non-SIEM companies.

[2]Observed differences in median or average value do not reflect a trend since it is calculated from two different samples of companies.

All industries fall victim to cybercrime, but to different degrees. The average annualized cost of cyber crime appears to vary by industry segment, where defense, utilities and energy, and financial service companies experience higher costs than organizations in retail, hospitality and consumer products.

A strong security posture moderates the cost of cyber attacks. We utilize a well-known metric called the Security Effectiveness Score (SES) to define an organization's ability to achieve reasonable security objectives.[3] 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.

Enterprise deployment of GRC practices moderates the cost of cyber crime. Findings suggest companies that have implemented GRC practices experience a lower cost of cyber crime than those that have not implemented these practices. Specifically, the percentage average cost of cyber crime for GRC companies is 38 percent higher than non-GRC companies.

[3]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.

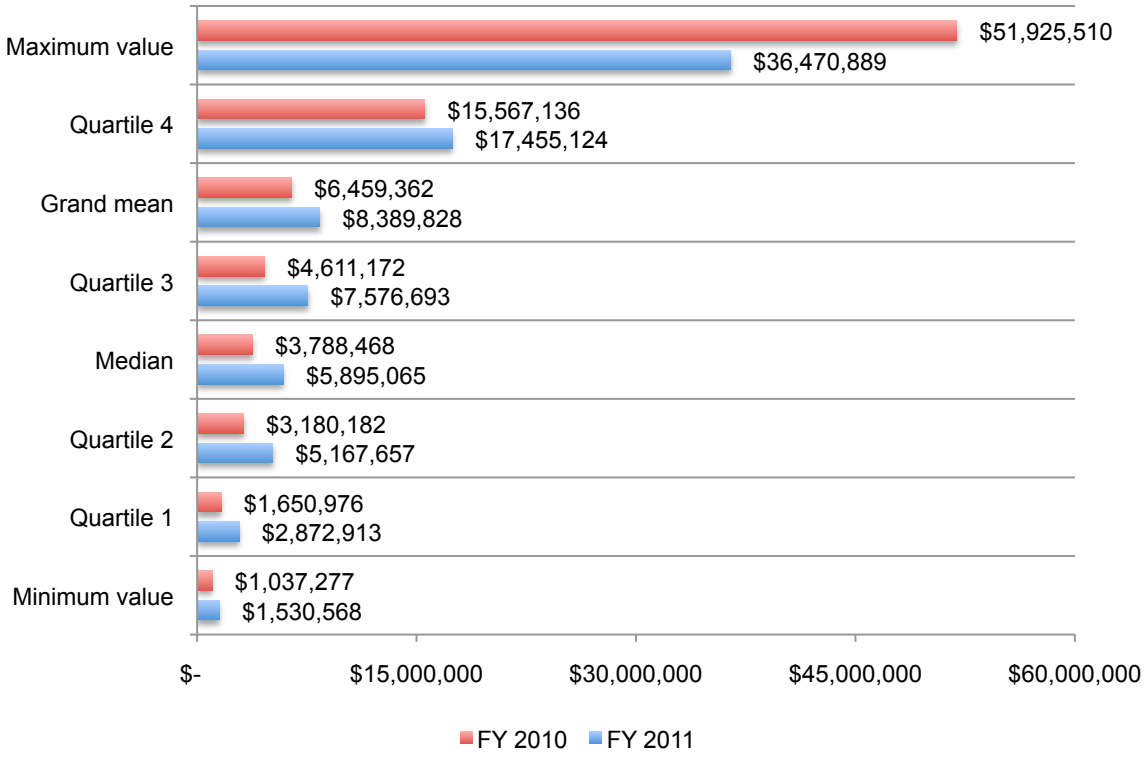
Part 2. Report Findings

Ponemon Institute's Cost of Cyber Crime Study examines the costs organizations incur when responding to cyber crime incidents. These costs do not include a plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

Cyber crimes are costly for participating organizations

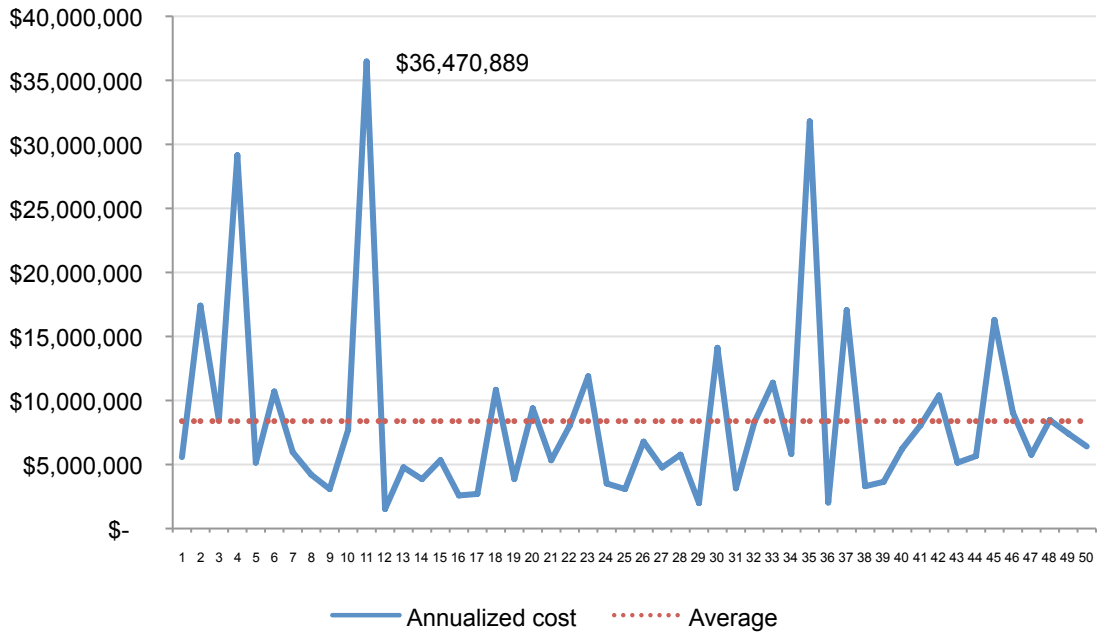
The total annualized cost of cyber crime for the benchmark sample of 50 organizations ranges from a low of $1.5 million to a high of nearly $36.5 million. Benchmark study participants were asked to report their expenditures for a four-week period. For ease of discussion, the reported figures were then extrapolated over a year's time. The median annualized cost of cyber crime in the study benchmark sample is $5.9 million – a 56 percent increase from last year's median value. The grand mean value is $8.4 million. Other key statistics on both the 2010 and 2011 cost of cyber crime are reported in Bar Chart 1.

Bar Chart 1
Key benchmark sample statistics on the annualized cyber crime cost



As shown in Line Graph 1, 16 companies incurred more than the mean value of $8.4 millions and, hence, 34 organizations incurred less than the mean value. The highest cost estimate of $36.5 million is not considered an outlier given that there are two other organizations that experienced an annualized cost above $29 million.

Line Graph 1
Annualized total cost of cyber crime for 50 participating companies

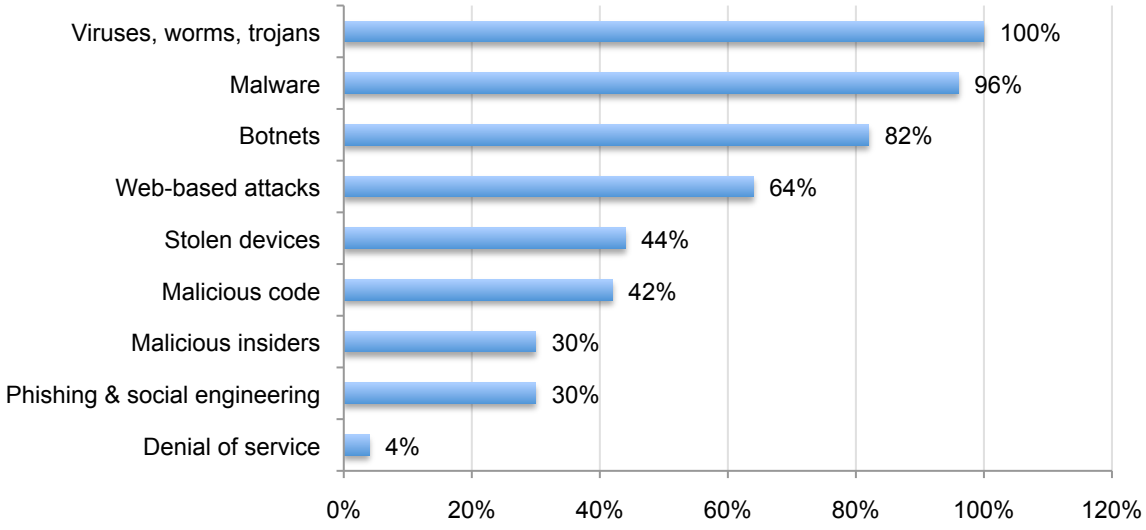


Cyber crimes are intrusive and frequent

The benchmark sample of 50 organizations experienced 72 discernible and successful cyber attacks per week, which translates to 1.4 successful attacks per benchmarked organization each week. The comparable rate for 45 organizations in FY 2010 was 50 discernible cyber attacks each week. This represents a 44 percent increase in successful attacks experienced last year.

Bar Chart 2 summarizes the types of attack methods experienced by participating companies. Virtually all organizations experienced attacks relating to viruses, worms and/or trojans over the four-week benchmarking period. Ninety-six percent experienced malware attacks[4], 82 percent experienced botnets, 64 percent experienced Web-based attacks, 44 percent experienced stolen or hijacked computing devices, 42 percent experienced malicious code, and 30 percent experienced malicious insiders. Another 30 percent experienced phishing and social engineering (including spear phishing) and only four percent experienced denial of service attacks.

Bar Chart 2
Frequency of cyber attacks experienced by benchmark sample
The percentage frequency defines a type of attack categories experienced.

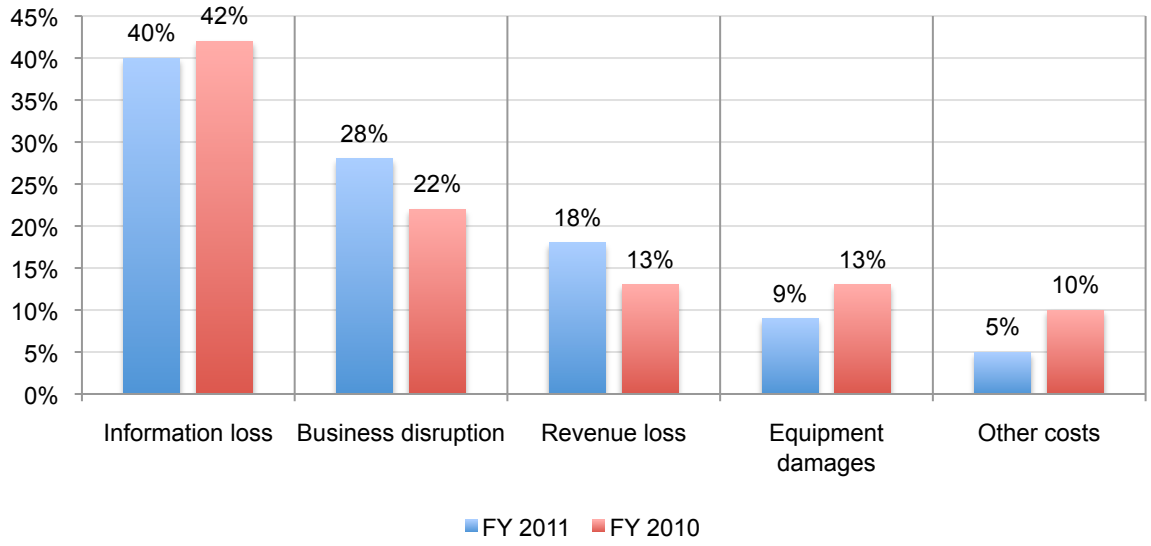


[4]Malware attacks and malicious code attacks are inextricably linked. We classified malware attacks that successfully infiltrated the organizations' networks or enterprise systems as a malicious code attack.

Information theft represents the highest external cost

At the top end of the external cyber crime cost spectrum is information loss. On an annualized basis, information loss accounts for 40 percent of total external costs, which is a decrease of two percent from our FY 2010 study. In contrast, business disruption or loss of productivity account for 28 percent of total external costs, an increase of six percent from FY 2010. Revenue loss (18 percent) and equipment damages (9 percent) yield a much lower cost impact.

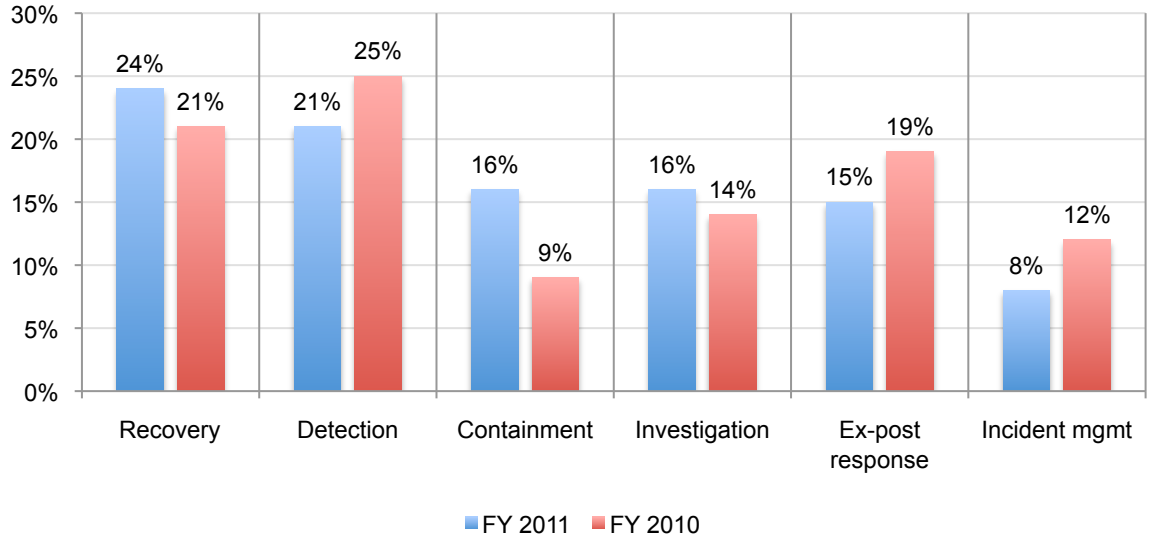
Bar Chart 3
Percentage cost for external consequences
Other cost includes direct and indirect costs that could not be allocated to a main external cost category.



Recovery and detection are the most costly internal activities

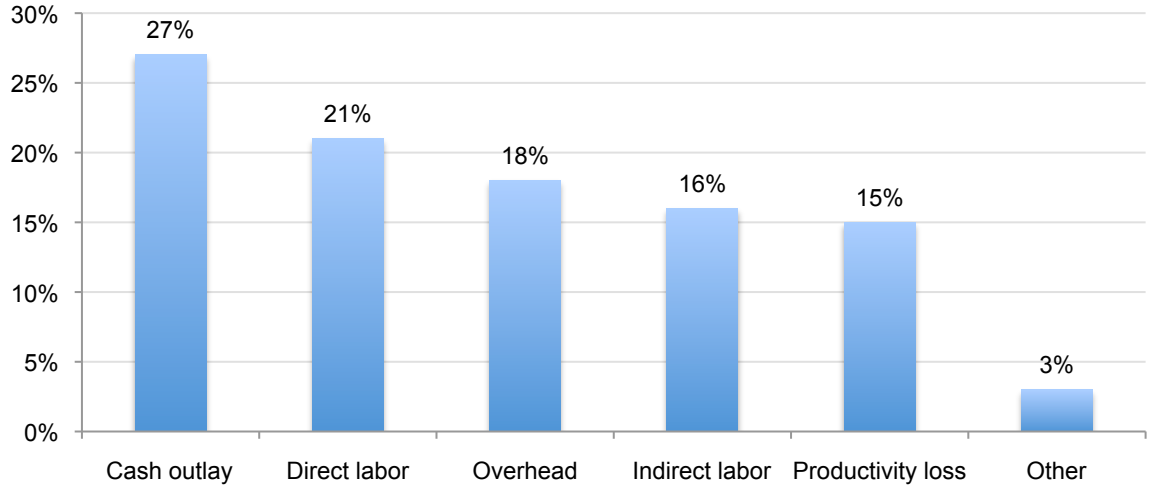
In our present study, cyber crime recovery and detection activities account for 45 percent of total internal activity cost (46 percent in FY 2010). Containment and investigation each represent 16 percent of internal activity cost. Ex-post response (i.e., after the fact response, or remediation) represents the lowest internal activity cost at 15 percent (down 4 percent from FY 2010). These cost elements highlight a significant cost-reduction opportunity for organizations that are able to automate recovery and detection activities through enabling security technologies.

Bar Chart 4
Percentage cost by internal activity center
Investigation includes escalation activities



Internal activity costs can be further broken down into specific cost components, which include cash outlays (27 percent), direct labor (21 percent), overhead (18 percent), indirect labor (16 percent), and lost productivity (15 percent).

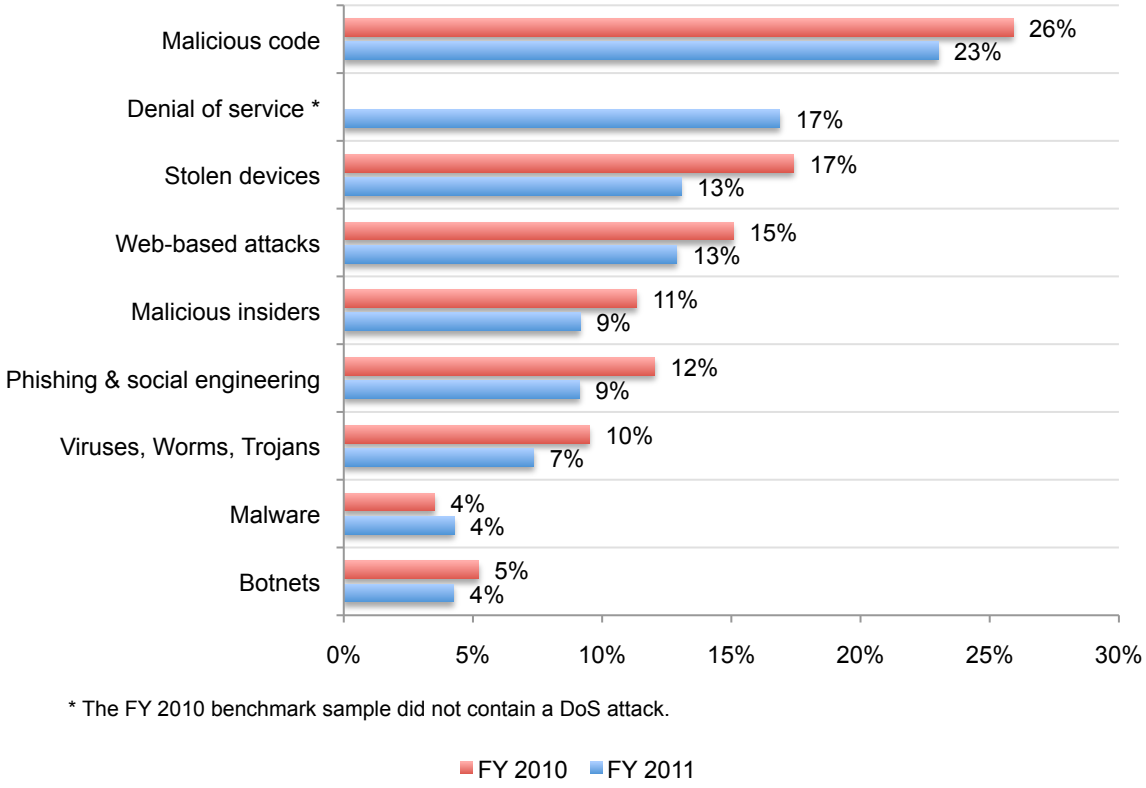
Bar Chart 5
Percentage internal activity cost by six specific cost components



Costs vary considerably by the type of cyber attack

Bar Chart 6 compares 2010 and 2011 results, showing the percentage of annualized cyber crime cost allocated to nine attack types compiled from all benchmarked organizations. Malicious code and denial of service (DoS) account for the two highest percentage cyber cost types. The least costly concern botnets, malware, viruses, worms and trojans.

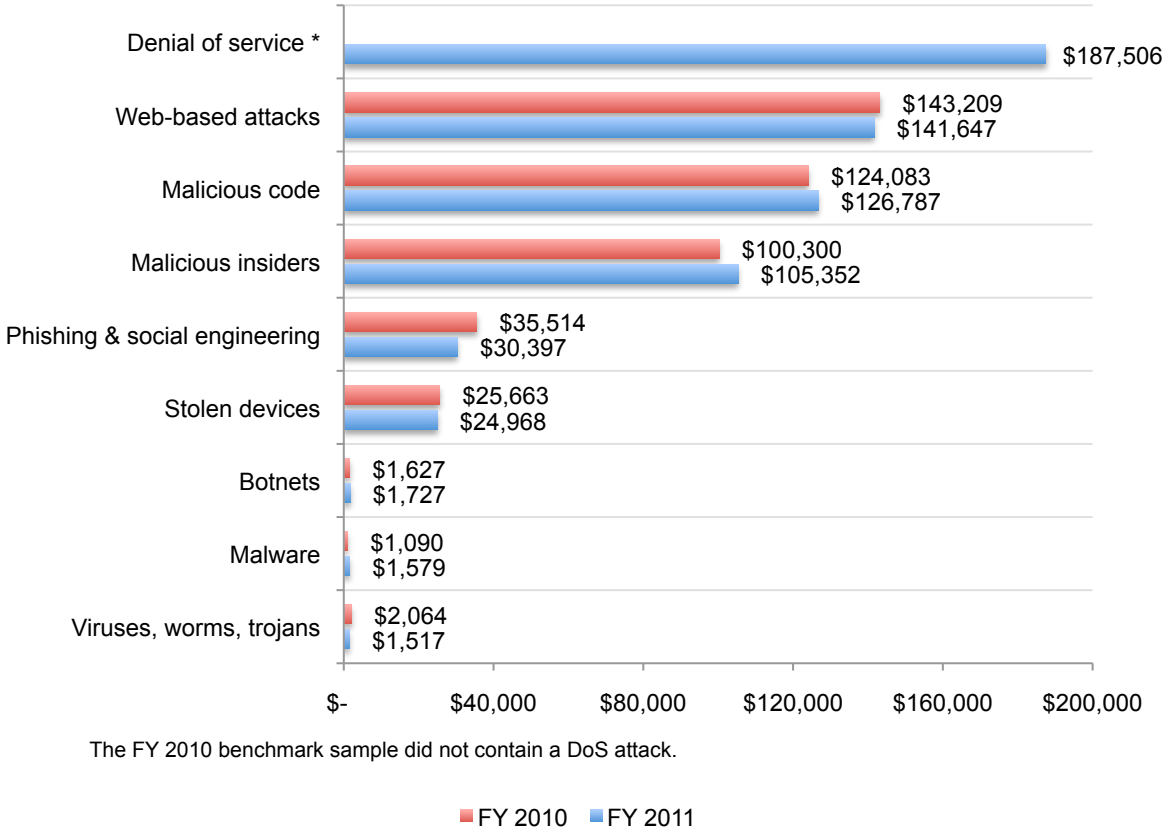
Bar Chart 6
Percentage annualized cyber crime cost by attack type



* The FY 2010 benchmark sample did not contain a DoS attack.

Bar Chart 7 compares 2010 and 2011 results, and illustrates how cyber crime costs vary by the method of attack. The chart highlights the average annualized cyber crime cost weighted by the frequency of attack incidents for all benchmarked companies. Clearly, the most expensive cyber crimes are denial of service, Web-based attacks, malicious code and malicious insiders. In total, these attacks account for more than 90 percent of all cyber crime costs experienced.

Bar Chart 7
Average annualized cyber crime cost weighted by attack frequency

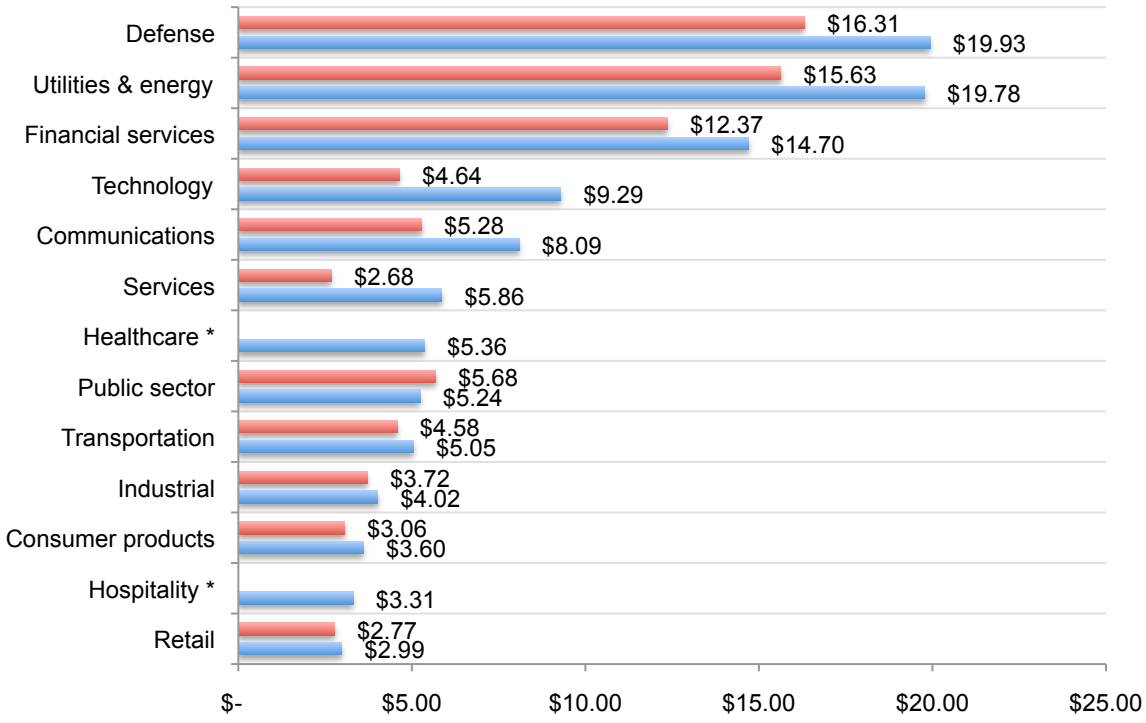


The FY 2010 benchmark sample did not contain a DoS attack.

The cost of cyber crime impacts all industries

The average annualized cost of cyber crime appears to vary by industry segment and shows a consistent pattern comparing 2010 and 2011 results. As seen in Bar Chart 8, defense, utilities & energy, and financial service companies experience substantially higher costs in both the 2010 and 2011 studies. Organizations in retail, hospitality and consumer products appear to have a lower overall cyber crime cost.[5]

Bar Chart 8
Average annualized cost by industry sector
$1,000,000 omitted



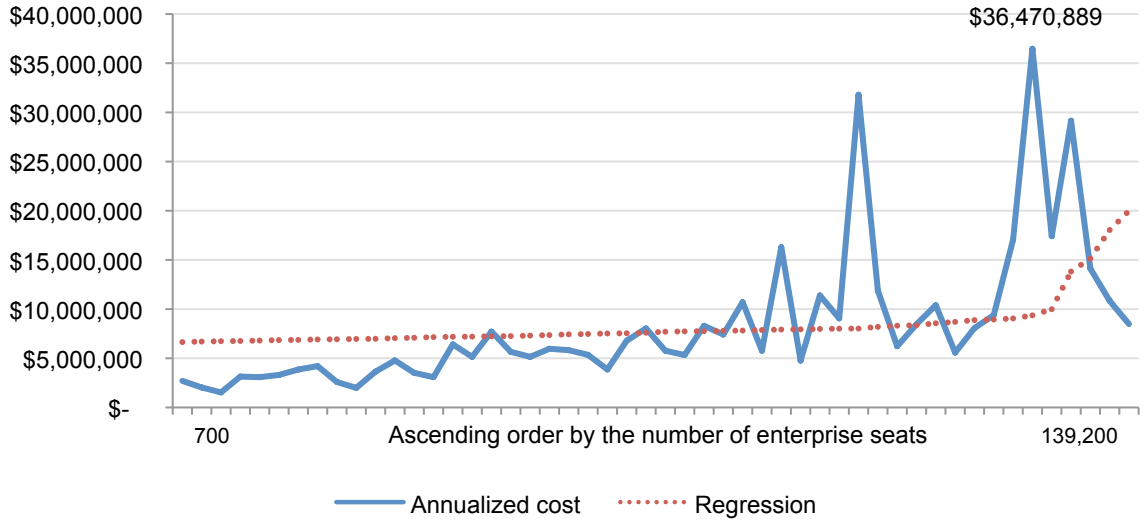
*Industry was not represented in the FY2010 benchmark sample.

[5]Despite similarities between the FY 2010 and FY 2011 results, this analysis is for illustration purposes only. The sample sizes in both years are too small to draw definitive conclusions about industry segment differences.

The cost of cyber crime varies by organizational size

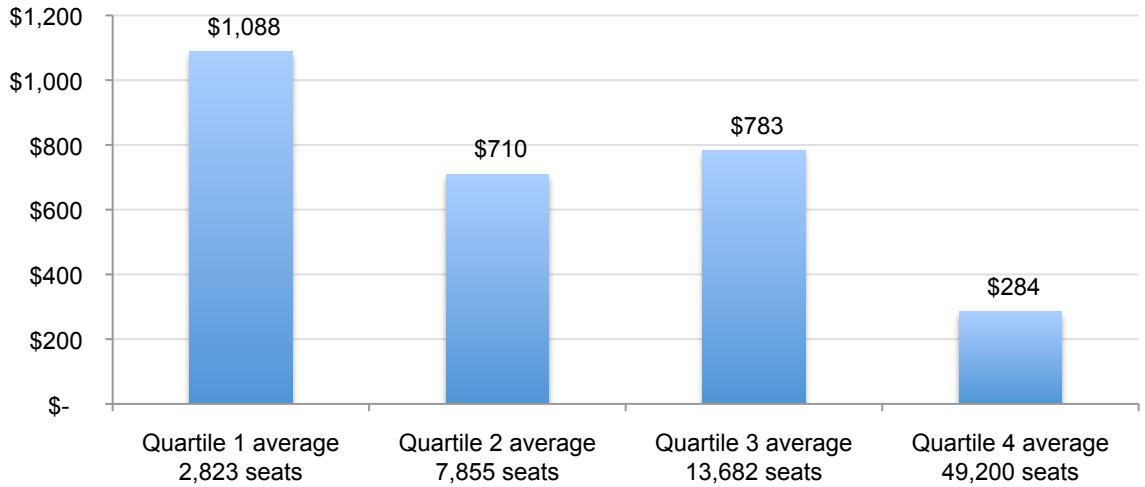
As shown in Line Graph 2, organizational size, as measured by the number of enterprise seats or nodes, is positively correlated to annualized cyber crime cost. This positive correlation is indicated by the upward slopping regression line.

Line Graph 2
Annualized cost in ascending order by the number of enterprise seats
Regression performed on enterprise seats ranging from 700 to 139,200.



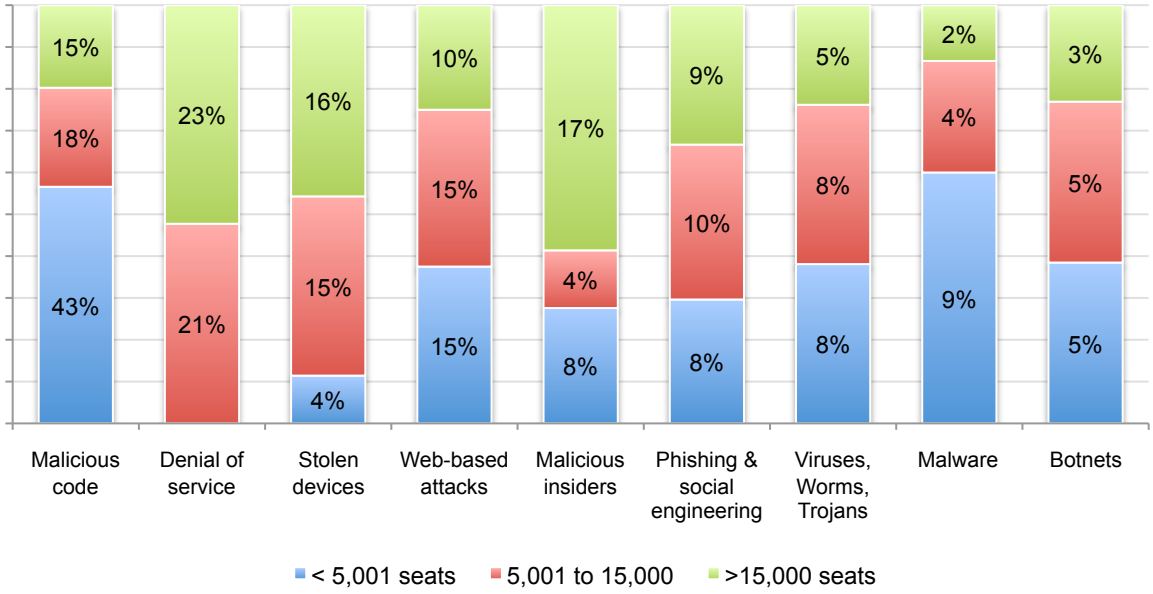
Bar Chart 9 summarizes the analysis of annualized cost on an enterprise seat basis. Accordingly, the average cost is compiled for each one of four quartiles ranging from the smallest sub-sample (Quartile 1 = $1,088) to the largest sub-sample (Quartile 4 = $284). As can be seen, the quartile average costs for organizations with the lowest number of enterprise seats is 3.8 times higher than the quartile average for organizations with the highest number of seats.

Bar Chart 9
Average annualized cost per enterprise seat



As revealed in Bar Chart 10, a comparison of small, medium and large-sized organizations reveals that the cost mix for specific cyber attacks varies by organizational size. Specifically, small organizations (less than 5,001 seats) experience a higher proportion of cyber crime costs relating to malicious code and malware. In contrast, large organizations (greater than 15,000 seats) experience a higher proportion of costs relating to malicious insiders, stolen or hijacked devices, and denial of service.

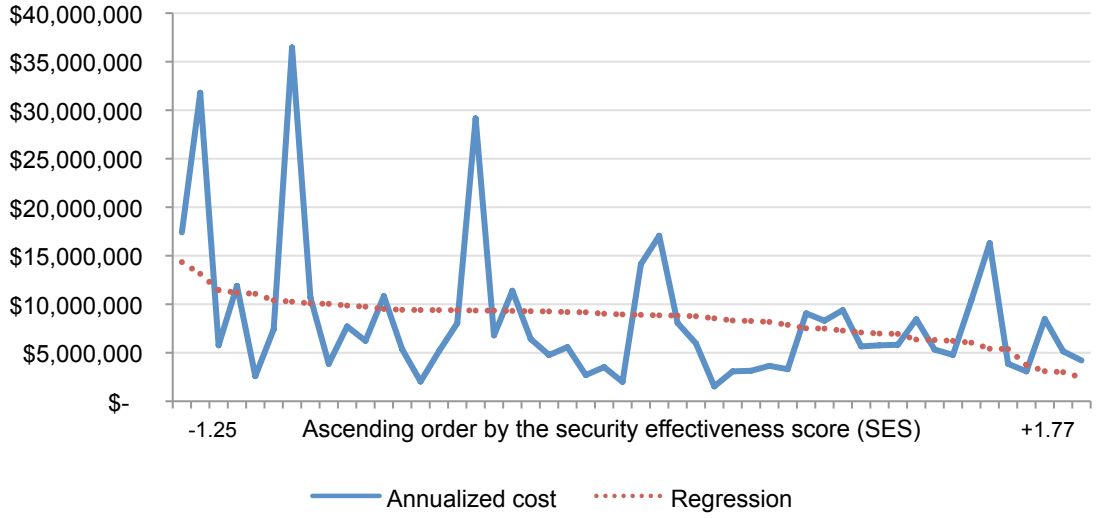
Bar Chart 10
The cost mix of attacks by organizational size
Size measured according to the number of enterprise seats within the participating organizations.



The organization's security posture Influences the cost of cyber crime

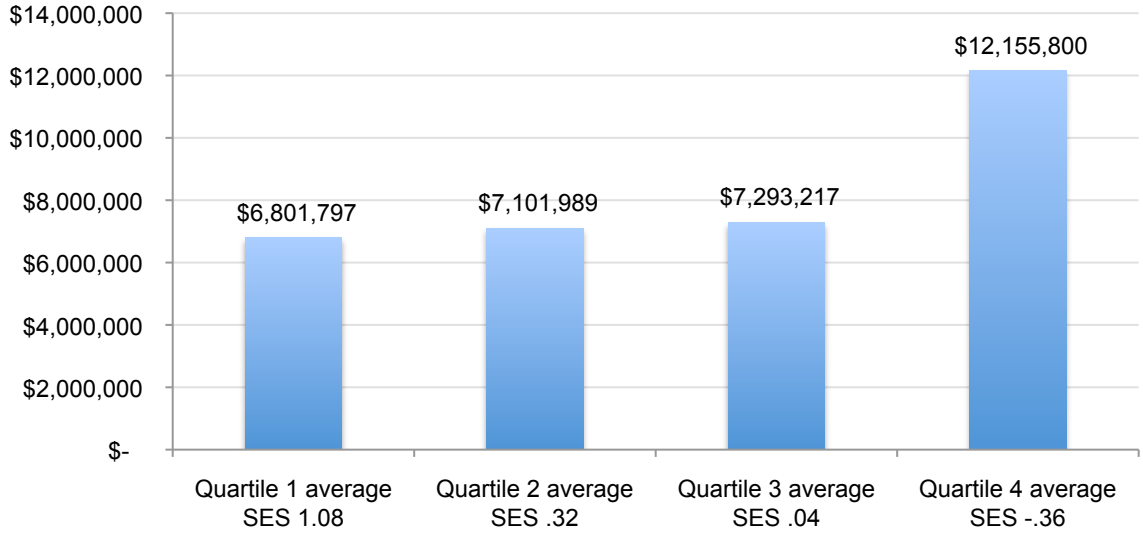
In our present study, we measure the security posture of participating organizations as part of the benchmarking process. Line Graph 3 reports the annualized cost and regression forecast of companies in ascending order of security effectiveness as measured by the SES (see footnote 3). The graph shows a downward sloping regression, suggesting security posture is inversely related to 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 +1.77 to a low of -1.25, with a mean value at +.26.

Line Graph 3
Annualized cost in descending order by SES
Reported in $ millions. Regression performed on SES ranging from +1.77 to -1.25.



A comparison of organizations grouped into four quartiles based on SES reveals average cost differences. As noted in Bar Chart 11, the average cost for companies in quartile 1 is $6.8 million, while the average cost for quartile 4 is substantially higher at $12.2 million. This analysis shows that organizations with the lowest SES results are more likely to incur a higher cost.

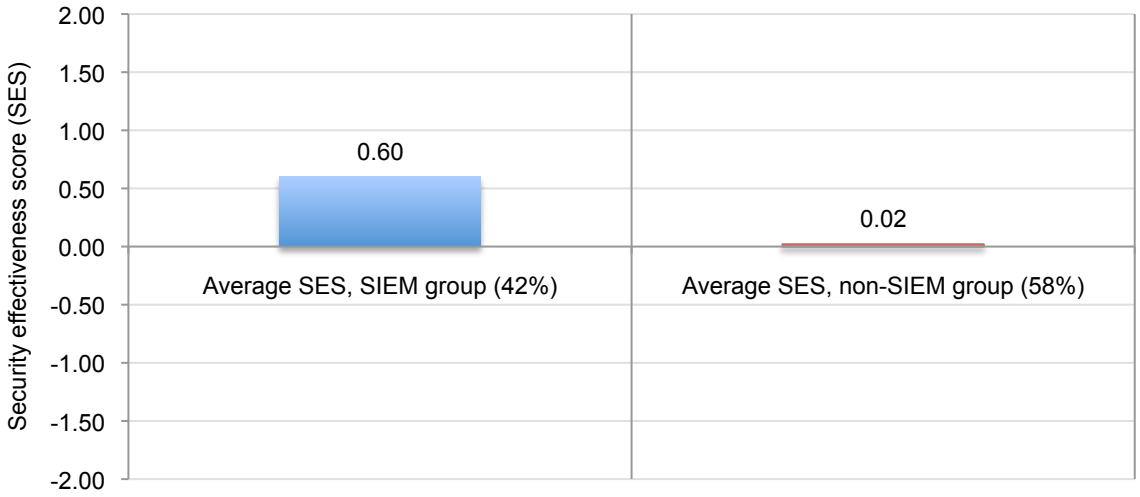
Bar Chart 11
Quartile comparison of annualized cost by SES



Organizations that have SIEM technologies realize a higher level of security effectiveness

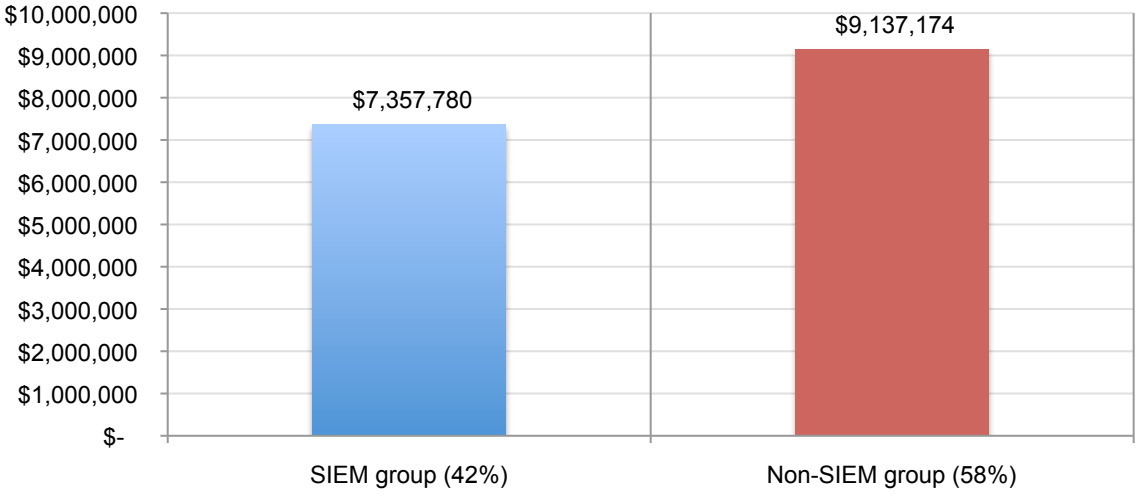
Bar Chart 12 reports the average SES score of companies with SIEM and non-SIEM. As can be seen, users of SIEM technologies realize a higher SES score than those in the non-SIEM sub-sample.

Bar Chart 12
Comparison of SIEM and non-SIEM sub-sample on security effectiveness
SES is defined for the range of +1.77 to -1.25.



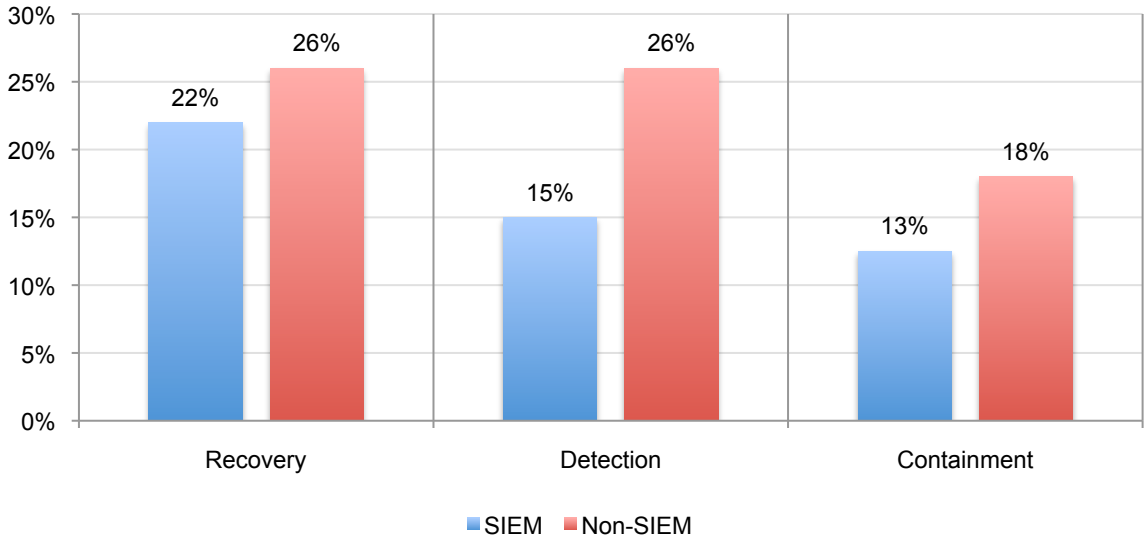
Bar Chart 13 shows organizations deploying SIEM achieve a lower overall cost (24 percent difference) than organizations that do not deploy SIEM. This result suggests SIEM improves a company's security posture, thereby reducing its overall cost of cyber crime.

Bar Chart 13
Comparison of SIEM and no-SIEM sub-sample on average cost of cyber crime



Bar Chart 14 reports the percentage cost for recovery, detection and containment cost centers for the SIEM and non-SIEM groups, respectively. As can be seen, companies deploying SIEM technologies experience a substantially lower cost of detection (difference = 11%). Other significant differences include containment (5%) and recovery (4%) operations.

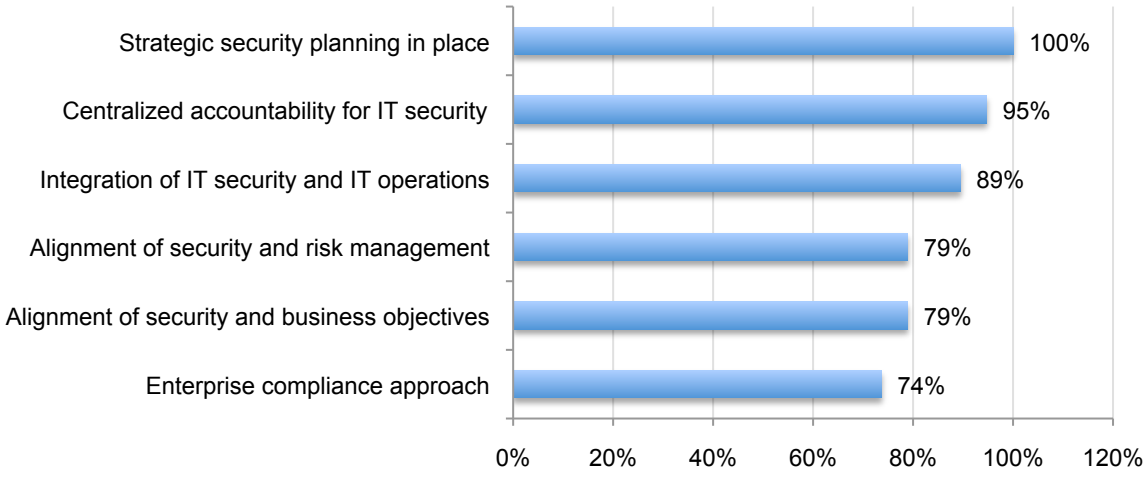
Bar Chart 14
Comparison of SIEM and no-SIEM sub-sample for three internal cost activity centers



Governance, risk management and compliance (GRC) practices moderate the cost of cyber crime

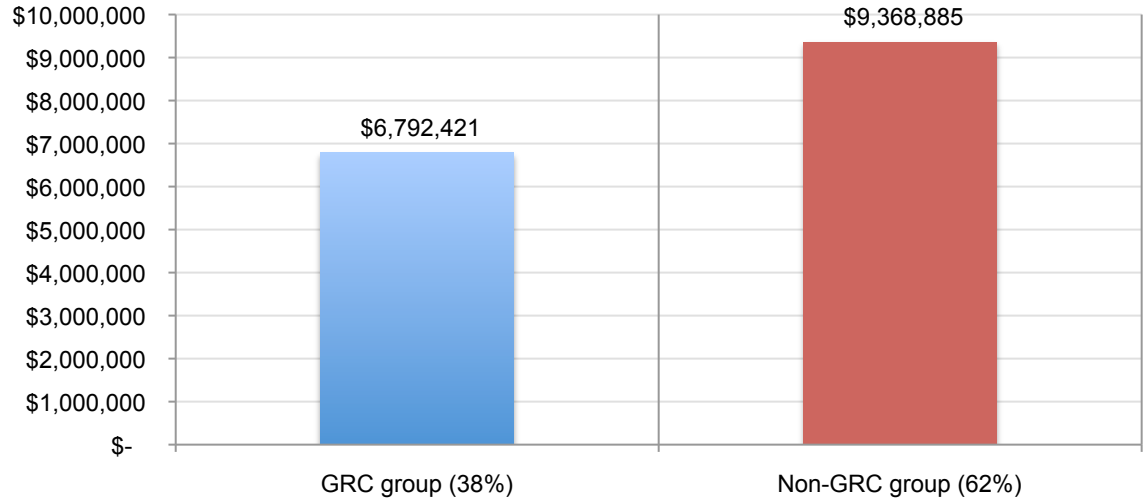
Bar Chart 15 reports six attributes used in our analysis for defining enterprise GRC activities. Using these attributes we categorize two subsamples – namely, the GRC group (38 percent) and non-GRC group (62 percent).

Bar Chart 15
Six attributes that define organizations' core GRC activities
Percentages defined for 19 organizations that have a GRC program



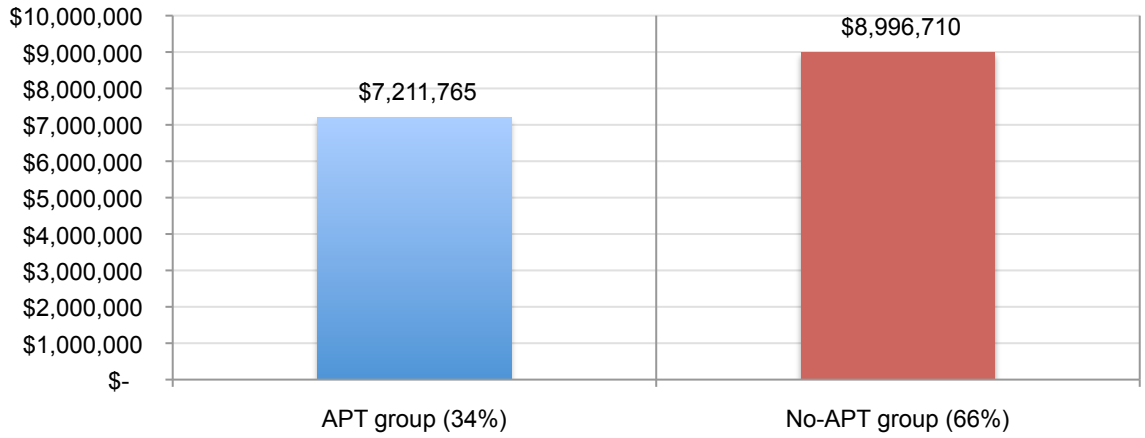
Bar Chart 16 reports the total annualized cyber crime cost for organizations with and without the above-mentioned GRC features. As shown, the extrapolated average costs are substantially lower for companies that deploy enterprise GRC practices versus companies that do not.

Bar Chart 16
Comparison of GRC and no-GRC sub-sample on average cost of cyber crime



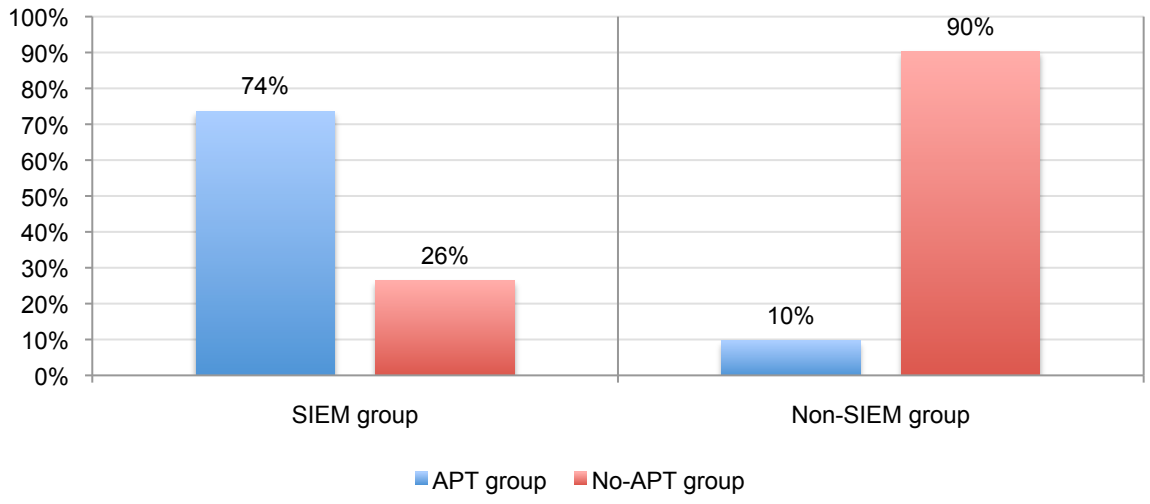
Bar Chart 17 reports the total annualized cyber crime cost according to organizations recognizing or not recognizing advance persistent threats (APT) during the four-week benchmarking period. As shown, organizations that recognized APTs (34 percent) seem to achieve a lower overall cost than those that did not recognize APTs (66 percent).[6]

Bar Chart 17
Comparison of APT and no-APT sub-sample on average cost of cyber crime



Bar Chart 18 analyzes the relationship between APT recognition and the use of SIEM technologies. As shown below, there seems to be a significant relationship between companies that use SIEM and their ability to recognize APTs. Accordingly, 74 percent of SIEM companies recognized the existence of APTs during the four-week benchmark period versus only 26 percent of SIEM companies that failed to recognize APTs. In sharp contrast, only 10 percent of non-SIEM companies recognized APTs during a four-week benchmark period. The ability to recognize and defend the organization from APTs may explain why, at least in part, SIEM deployment lowers the overall cost of cyber crime.

Bar Chart 18
Comparison of APT and No-APT by SIEM and non-SIEM sub-samples



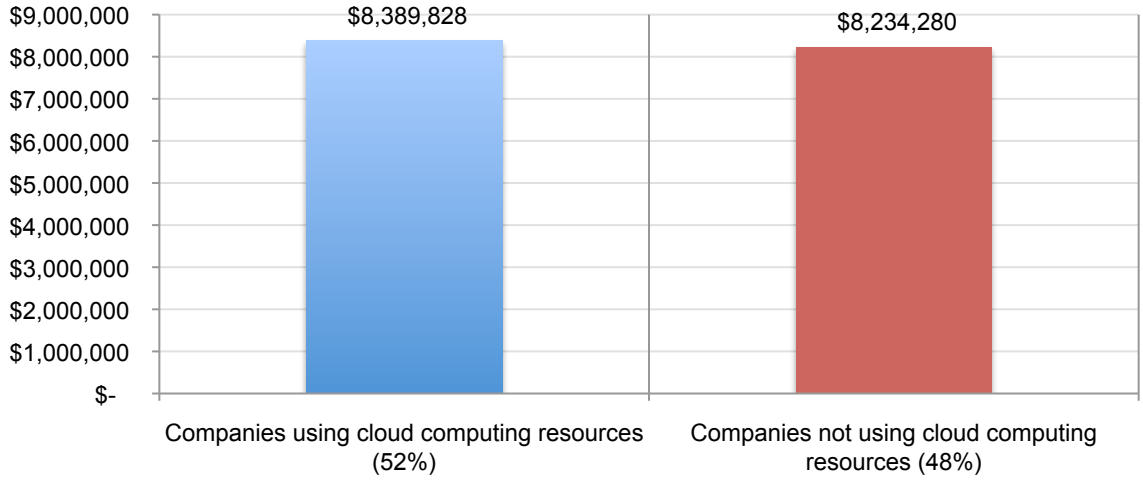
[6]See The Growing Risk of Advanced Threats, Ponemon Institute, June 2010. This study shows that APTs are a possible driver or antecedent to cyber crime costs.

Cyber crime costs are not influenced by companies' use of public or hybrid cloud computing resources

We captured information from each participating company concerning their use of public or hybrid cloud computing resources. Our research classified 26 companies as significant users of public or hybrid cloud resources including software, infrastructure, and platform services. The remaining 24 companies were not significant users of public or hybrid cloud services.[7]

Based on previous research, we hypothesized that companies deploying cloud resources would experience a higher cost of cyber crime (by virtue of heightened security risks experienced in the cloud ecosystem).[8] However, evidence of higher cyber crime costs is not indicated in this study. Specifically, Bar Chart 19 shows about the same average cost of cyber crime for companies deploying or not deploying public or hybrid cloud resources.

Bar Chart 19
Comparison of companies by their use of public or hybrid cloud computing resources

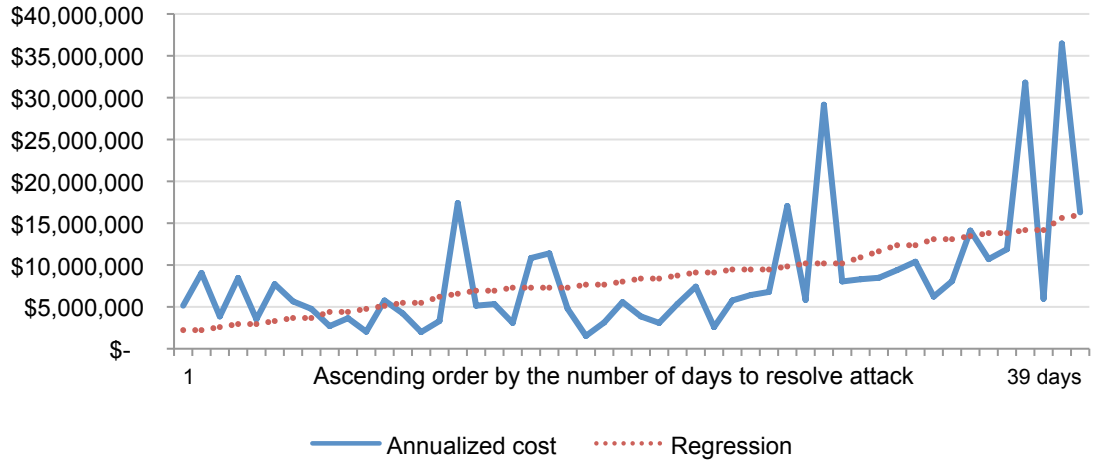


[7]Please note that five of these companies were deploying private cloud systems.
[8]See Security of Cloud Computing Providers, Ponemon Institute, April 2011.

Time to resolve or contain cyber crimes increases the cost

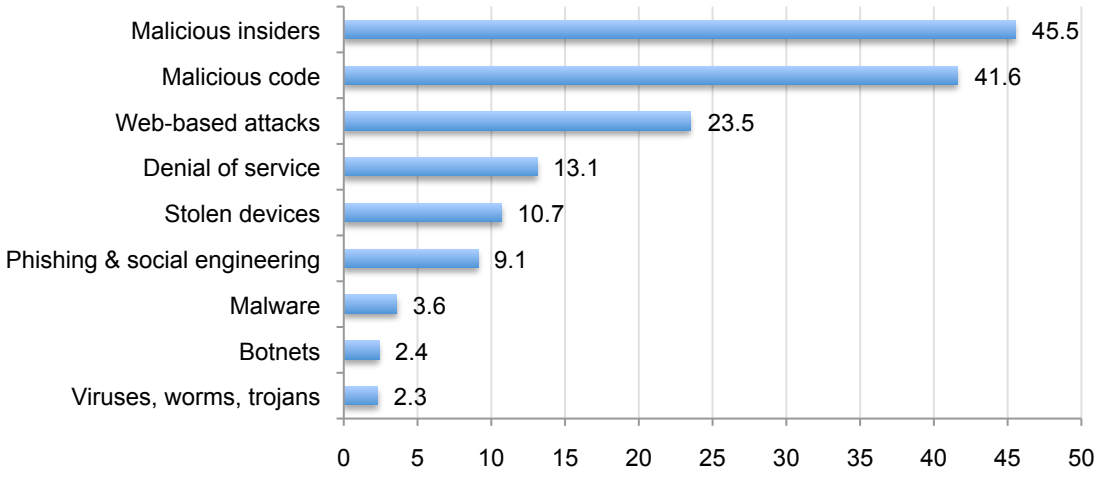
In the present sample, the average number of days to resolve cyber attacks is 18 with an average cost of $22,986 per day – or a total cost of $413,784 over the 18 day period. This represents a 67 percent increase from last year's cost estimate.[9] The time range to resolve attacks is from less than 24 hours to over 39 days. Line Graph 4 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.

Line Graph 4
Average days to resolve attack in ascending order
Estimated average time is measured for each given organization in days.



Bar Chart 20 reports the average days to resolve cyber attacks for seven different attack types studied in this report. It is clear from this chart that it takes substantially more time, on average, to resolve malicious insider, malicious code and Web-based attacks than botnets, malware and viruses.

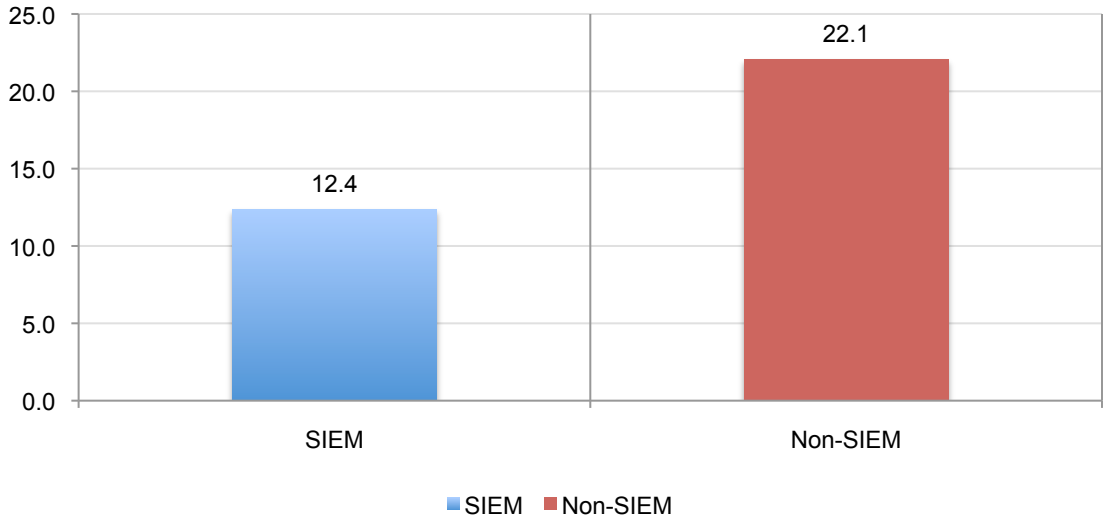
Bar Chart 20
Average days to resolve attack for seven attack types



[9]Our 2010 study found the average days to resolve an attack was 14 with a range of 1 to 42 days. This produced an average cost of $17,696 per day or $247,744 over the 14 day resolution period.

Bar Chart 21 once again demonstrates the importance of SIEM in minimizing the cost of cyber crime for participating companies. Accordingly, organizations deploying SIEM experience a 12.4 day average time to resolve cyber attacks as compared to the non-SIEM group that, on average, experienced 22.1 days to resolve attacks (nearly a 10 day difference).

Bar Chart 21
Average days to resolve attack for SIEM and Non-SIEM groups



Part 3. Overview & Methods

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 1 reports the frequency of individuals by their approximate functional discipline that participated in this year's study. As can be seen, this year's study involved 379 individuals or an average of 7.6 interviews for each benchmarked company.

Table 1: Functional areas of interview respondents	Frequency	Pct%
IT operations	50	100%
IT security	49	98%
Compliance	47	94%
Data center management	45	90%
Network operations	37	74%
Accounting & finance	29	58%
Internal or IT audit	28	56%
Data protection	23	46%
Quality assurance	19	38%
Other	15	30%
Legal	14	28%
Human resources	12	24%
Development & testing	11	22%
Total	379	

Using a series of structured interview questions, key individuals provided direct cost estimates for each cyber crime cost category by selecting a range variable. A range variable rather than a point estimate was used to preserve confidentiality and to ensure a higher response rate. Second, the structured interview required key individuals to provide a second series of cost estimates for all indirect cost and opportunity losses by cost component category.

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.

Figure 1 (shown in Part 4) illustrates the activity-based costing schema we used in our benchmark study. As can be seen, we examined internal cost centers sequentially – starting with incident discovery to escalation to containment to recovery to ex-post response and culminating in diminished business opportunities or revenues. The cost driver of ex-post response and lost business opportunities is business disruption resulting from the attack.

In total, the benchmark instrument contained descriptive costs for each one of the five cost activity centers. Within each cost activity center, the survey required respondents to estimate the cost range to signify direct cost, indirect cost and opportunity cost, 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.

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.

To keep the benchmark instrument to a manageable size, we carefully limited items to only those cost activities we considered crucial to the measurement of cyber crime cost. 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, seven companies were rejected because of incomplete, inconsistent or blank responses.

The present study was launched in January 2011. The recruitment started with a personalized letter and a follow-up phone call to 401 organizations for possible participation in our study.[10] While 63 organizations initially agreed to participate, 50 organizations permitted our researchers to complete the benchmark analysis.

Utilizing activity-based costing (ABC), cost estimates were captured using a standardized instrument for direct and indirect cost categories. Specifically, labor (productivity) and overhead costs were allocated to five internal activity centers (see Figure 1). 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 eight discernible attack vectors.

To maintain consistency across all benchmarked companies, we collected information over four consecutive weeks. Field research was conducted over a five-month period concluding on June 24, 2011. The four consecutive weeks for any given organization was not necessarily the same time period as every other organization is 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).

[10]More than half of the organizations contacted for possible participation in this year's study are members of Ponemon Institute's benchmarking community. This community of companies is composed of organizations that have participated in one or more benchmarking studies sometime over the past nine years.

Sample of participating companies

Pie Chart 1 and Table 2 summarize the sample of participating companies based on 12 primary industry classifications. As can be seen, financial services (18 percent) represent the largest segment. This includes retail banking, insurance, brokerage and credit card companies. The second largest segment is technology (12 percent), including organizations in software and IT management.

Pie Chart 1
Sample distribution by industry

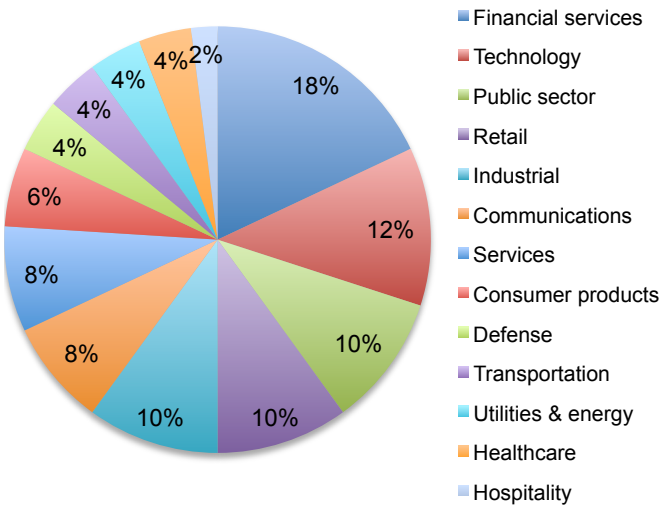
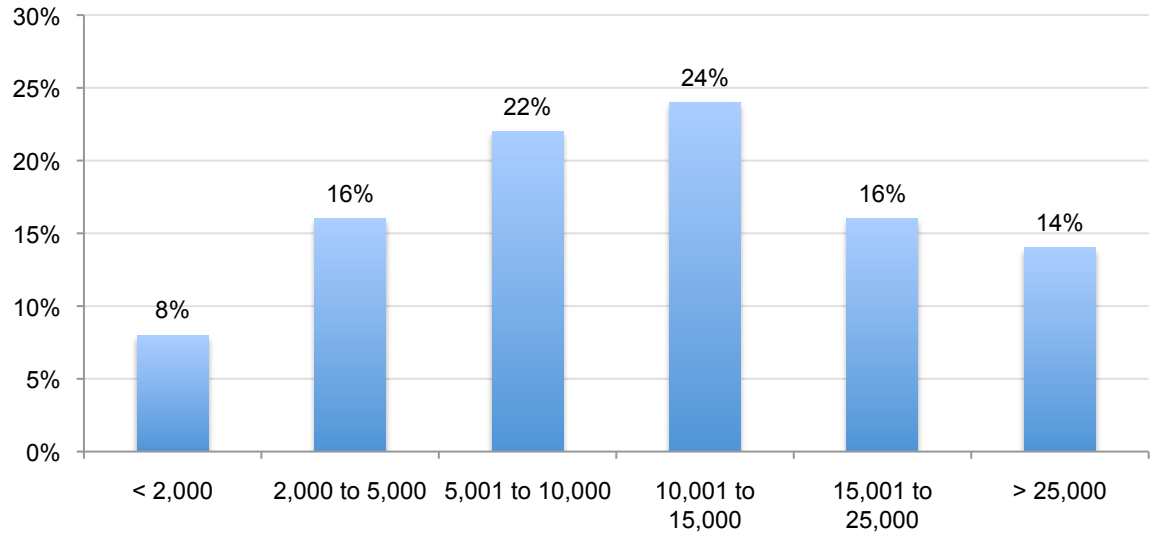


Table 2
2011 and 2010 samples by industry

Industries	2011	2010
Financial services	9	10
Technology	6	5
Public sector	5	4
Retail	5	4
Industrial	5	4
Communications	4	5
Services	4	3
Consumer products	3	4
Defense	2	1
Transportation	2	3
Utilities & energy	2	1
Healthcare	2	0
Hospitality	1	0
Education	0	1
Total	50	45

Bar Chart 22 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 700 seats. The largest enterprise has 139,200 seats.

Bar Chart 22
Percentage distribution of participating organizations by enterprise seats (size)

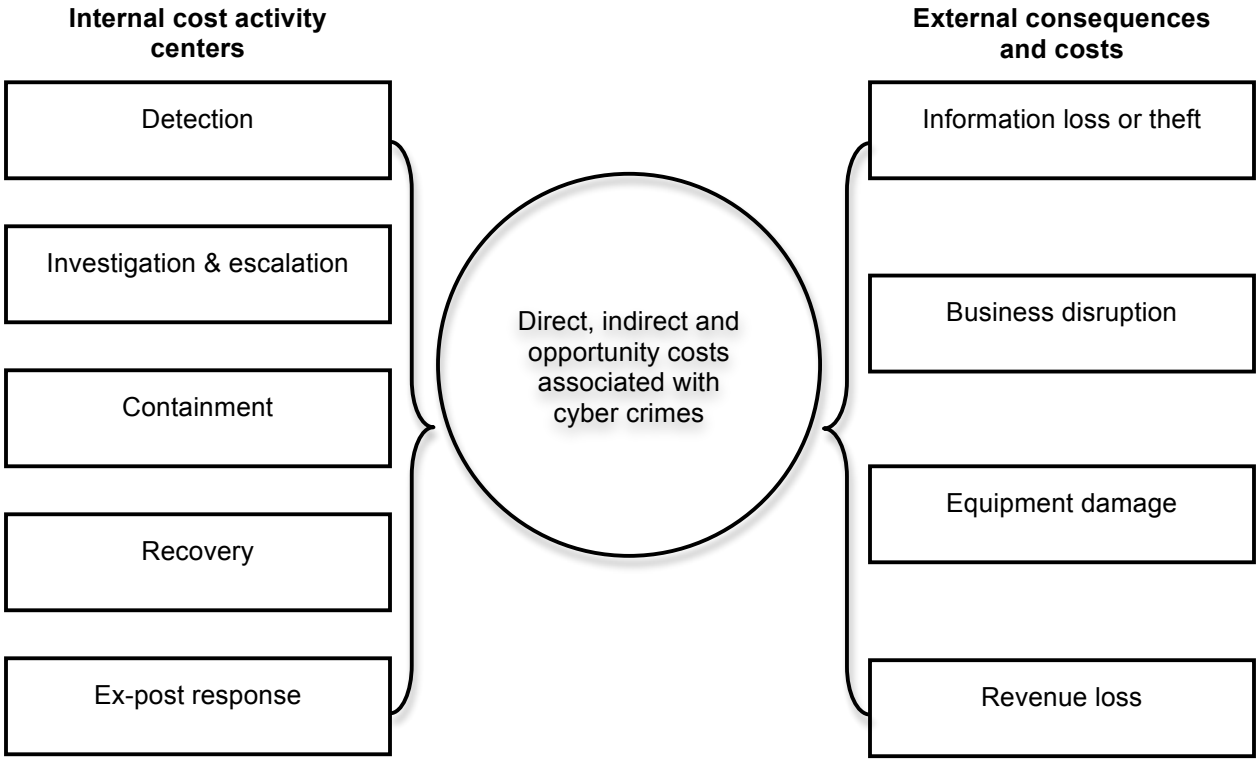


Part 4. Benchmark Framework

Benchmark results of 50 organizations are intended to provide a meaningful baseline for companies experiencing a wide array of cyber attacks including viruses, malware, Trojans, worms, malicious code, botnets, malicious insiders, denial of services and others.

The costing framework in Figure 1 presents the two separate cost streams used to measure total cyber crime cost for each participating organization. These two cost streams pertain to internal security-related activities and the external consequences experienced by organizations after experiencing an attack. Our benchmark methods attempt to elicit the actual experiences and consequences of cyber attacks. 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.

Figure 1
Costing Framework for Cyber Crime



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 to minimize potential future attacks. These include 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 Institute's 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.
- 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.

While not shown in Figure 1, the nature of attacks that underlie cost in our framework include the following seven attack types: viruses, worms, Trojans; malware; botnets; web-based attacks; phishing and social engineering; malicious insiders (including stolen devices); and malicious code (including SQL injection).[12]

[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.
[12] 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.

Part 5. Caveats

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 U.S.-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 401 separate organizations, all believed to have experienced one or more cyber attacks (see footnote 8). Fifty 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.

Part 6. Report Conclusions

The findings of this benchmark study suggest companies that experience cyber attacks do incur significant costs. The most salient costs result from the loss or theft of information, as well as disruption to business operations. Our research supports the notion that "an ounce of prevention is worth a pound of cure." Despite its stated limitations, the research is encouraging to those who believe the proposition that good security practices have a positive return on investment.

Other key takeaways from this report include:

- Cyber crimes can do serious harm to an organization's bottom line. We found that the median cost is $5.9 million per year, but can range from $1.5 million to $36 million per year per company. This represents a 56 percent average cost increase from last year's benchmark results.

- Cyber attacks have become common occurrences. The companies in our study experienced 72 discernible and successful cyber attacks per week, which represents a 44 percent increase in successful attacks over the number experienced by organizations in last year's study.

- The most costly cyber crimes are those caused by Web-based attacks, denial of service, malicious code and malicious insiders, which account for more than 90 percent of all cyber crime costs per organization on an annual basis.

- Recovery and detection are the most costly internal cost activities with labor representing nearly half of all internal cost activities. This highlights a significant cost-reduction opportunity for organizations that are able to automate detection and recovery through enabling security technologies.

- SIEM makes a difference. Specifically, companies deploying SIEM technologies across the enterprise experience a lower overall cost of cyber crime. Further, findings show that SIEM substantially reduces the time to resolve attacks and heightens awareness about serious threats and emerging attack vectors (such as advance persistent threats).

- GRC practices also moderate the cost of cyber crime. Companies that embrace key GRC practices such as strategic security planning, centralized accountability, integration of security and IT operations, alignment of security and risk management, and an enterprise compliance approach enjoy a lower cost of cyber crime than those that do not.

- The fact that discernible attacks in this year's study have increased – coupled with the fact that the time to resolve attacks has also increased – suggests the cyber crime landscape continues to evolve in terms of attack severity and frequency. In other words, results of the present study suggest things might be getting worse.

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.