First Annual Cost of Cyber Crime Study

Benchmark Study of U.S. Companies

Sponsored by ArcSight

Independently conducted by Ponemon Institute LLC
Publication Date: July 2010

Ponemon Institute© Research Report

First Annual Cost of Cyber Crime Study

Benchmark Study of U.S. Companies

Conducted by Ponemon Institute July 2010

Part 1. Executive Summary

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 of the 45 organizations in our study is $3.8 million per year, but can range from $1 million to $52 million per year per company.
- Cyber attacks have become common occurrences. The companies in our study experienced 50 successful attacks per week and more than one successful attack per company per week.
- The most costly cyber crimes are those caused by web attacks, malicious code and malicious insiders, which 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 threat and risk management solutions.

The purpose of this benchmark study is twofold. First, we wanted to quantify the economic impact of a cyber attack. Second, we believed 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. Well-publicized cyber attacks have affected private and public sector organizations such as Google, TJX Companies, TD Ameritrade and Heartland Payment Systems.

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. The total time invested in recruiting companies, building an activity-based cost model, collecting source information and analyzing results required nine months of effort.

This research resulted in the completion of case studies involving 45 organizations located in the United States. 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.

High-Level Findings

Listed below are what we believe to be the major findings of this research.

Cyber crimes are costly. Cyber crimes can do serious harm to an organization's bottom line. We found that the median annualized cost of the 45 organizations in our study is $3.8 million per year, but can range from $1 million to $52 million per year per company.

Cyber crimes are intrusive and common occurrences. The companies in our study experienced 50 successful attacks per week and more than one successful attack per company per week.

The most costly cyber crimes are those caused by web attacks, malicious code 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 threat and risk management solutions.

Cyber attacks can get costly if not resolved quickly. In this benchmark study sample, the average number of days to resolve a cyber attack was 14 days with an average cost to the organization of $17,696 per day. The survey revealed that malicious insider attacks can take up to 42 days or more to resolve. These costs demonstrate that quick resolution is needed for today's sophisticated attacks.

Information theft represents the highest external cost, followed by the costs associated with the disruption to business operations. On an annualized basis, information theft accounts for 42 percent of total external costs. Costs associated with disruption to business or lost productivity accounts for 22 percent of external costs.

Detection and recovery are the most costly internal activities. On an annualized basis, detection and recovery combined account for 46 percent of the total internal activity cost with labor representing the majority of these costs. Specific cost components include direct labor (36 percent), indirect labor (13 percent), overhead (8 percent), amortized system costs (30 percent) and lost productivity (13 percent). These cost elements highlight a significant cost-reduction opportunity for organizations that are able to automate detection and recovery through technologies like security information and event management (SIEM) systems.

All industries fall victim to cybercrime. The average annualized cost of cyber crime appears to vary by industry segment, where defense, energy and financial services companies experience higher costs than organizations in retail, services and education.

A strong security posture reduces the impact and cost of cyber attacks. In this benchmark study, we utilize a statistic known as the Security Effectiveness Score (SES) to measure an organization's ability to meet reasonable security objectives.[1] The higher the SES score, 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. The cost of cyber crime is moderated by "good" governance practices. The appointment of a CISO, the creation and rollout of an enterprise security strategy, adherence to a voluntary certification program (such as ISO) and deployment of SIEM appear to lessen the total cost of cyber crime. Companies that had deployed a SIEM system achieved a 24 percent cost savings when dealing with cyber attacks versus those that had not.

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

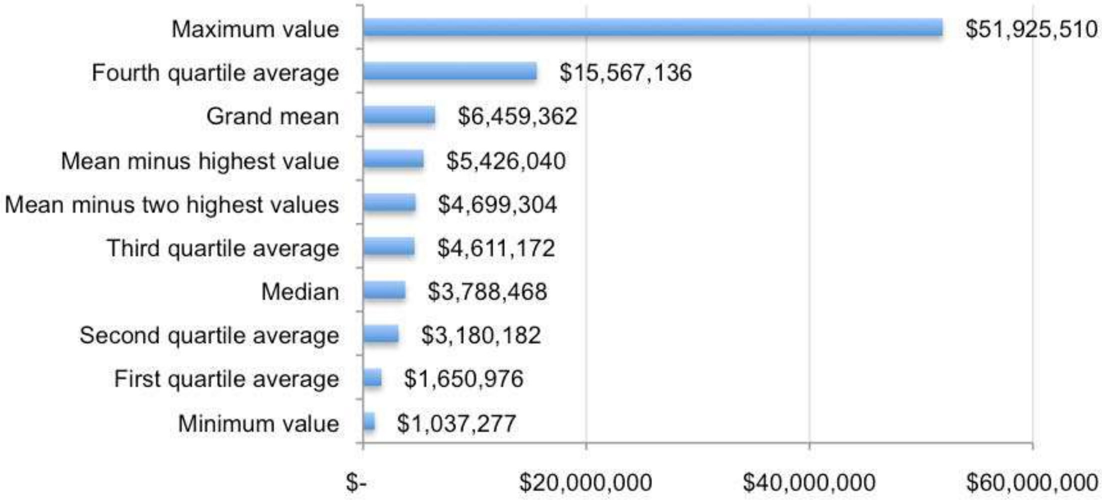
Part 2. Key Report Findings

Ponemon Institute's First Annual Cost of Cyber Crime Study examines the costs organizations incur when responding to cyber crime incidents.

Cyber Crimes are Costly

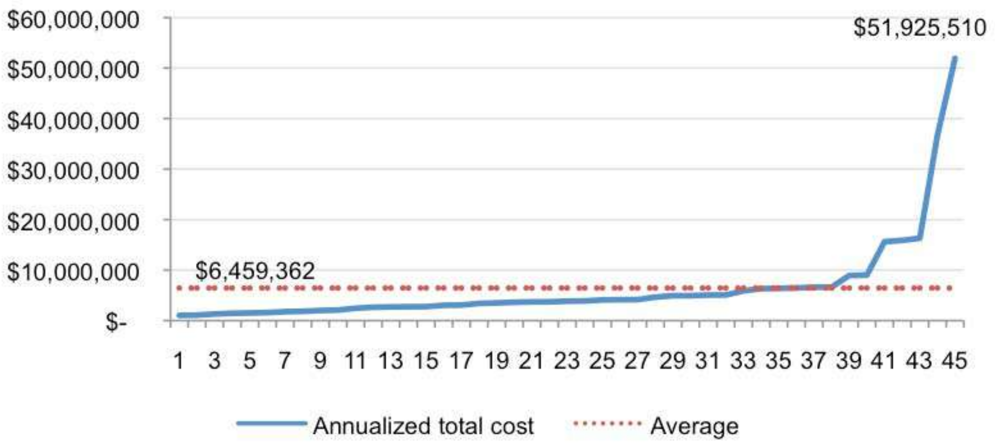
The total annualized cost of cyber crime for the benchmark sample of 45 organizations ranges from a low of $1 million to a high of nearly $52 million. Benchmark study participants were asked to report their expenditures for a four-week period. For ease of discussion, the reported figures were then extrapolated over a year's time. The median annualized cost of cyber crime in the study benchmark sample is $3.8 million. The grand mean value is $6.5 million. Other key statistics on the annualized 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, 38 participants spent $6 million or less and eight respondents spent between $6 million and $52 million. While the highest cost estimate of $51 million may appear to be an outlier, it is proof that cyber crime costs can be very significant.

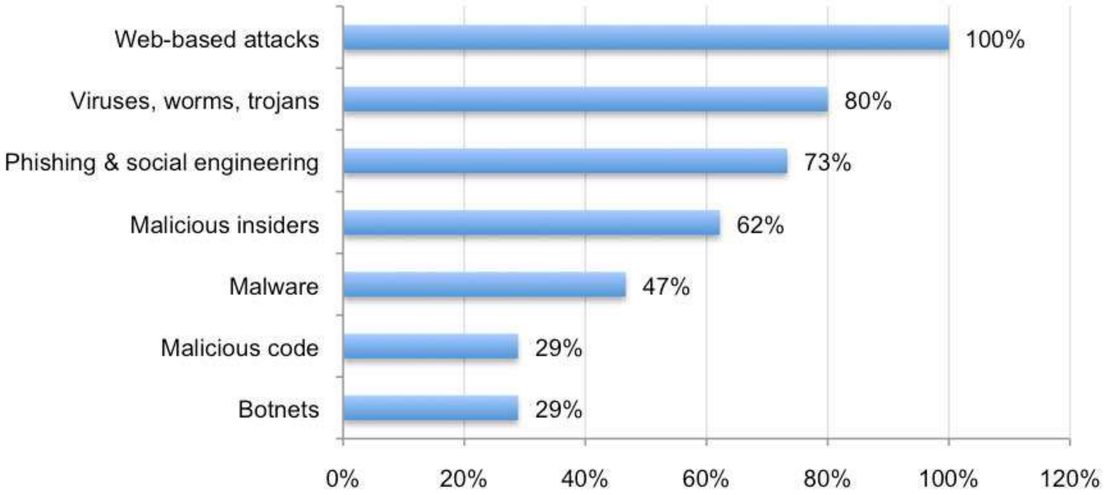
Line Graph 1
Annualized total cost of cyber crime for the 45 participating companies



Cyber Crimes are Intrusive and Frequent

The benchmark sample of 45 organizations experienced 50 discernible and successful cyber attacks per week, which translates to more than one successful attack per company per week.

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

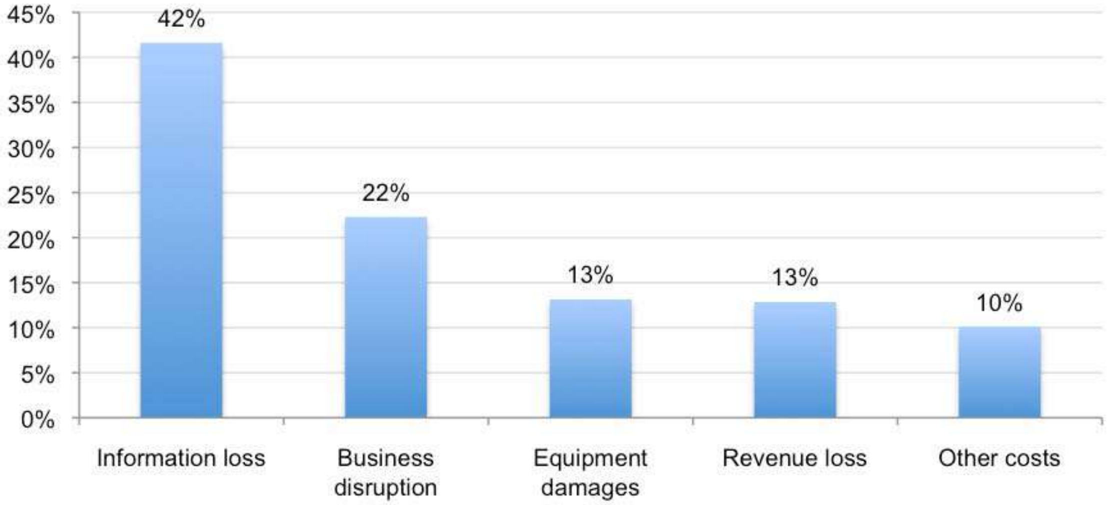


Bar Chart 2 summarizes the types of attack methods experienced by participating companies. All organizations experienced attacks relating to web-based attacks over the four-week benchmark period. Eighty percent experienced cyber attacks associated with viruses, worms and trojans while 73 percent experienced phishing and social engineering attacks. Sixty-two percent experienced attacks relating to malicious insiders while 47 percent experienced malware and 29 percent experienced attacks associated with malicious code and botnets.

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 42 percent of total external costs. In contrast, costs associated with business disruption or loss of productivity account for just 22 percent of total external cyber crime costs. Revenue loss and equipment damages yield a much lower cost impact, each coming in at 13 percent.

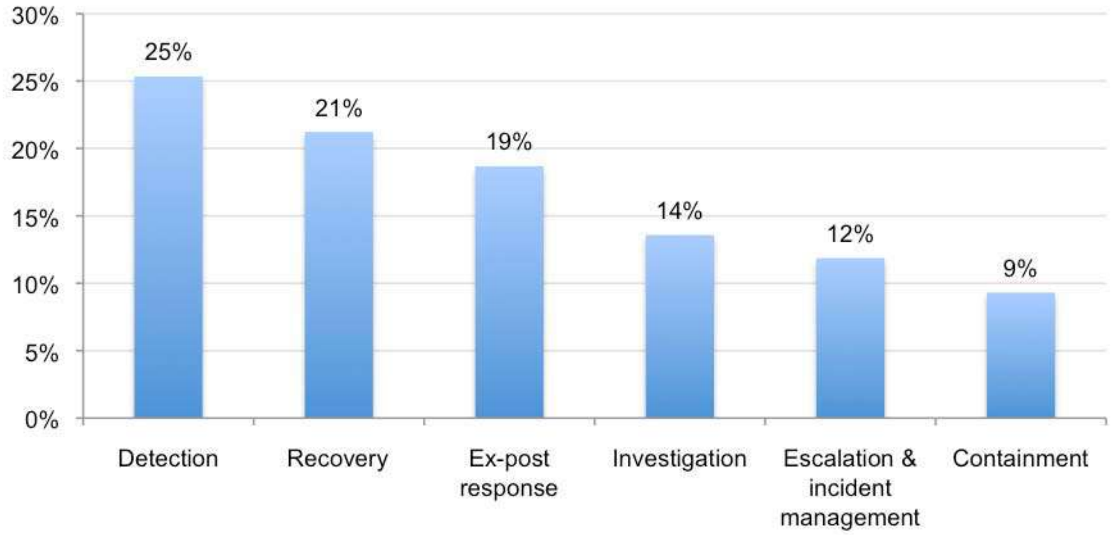
Bar Chart 3
Percentage cost for external consequences
Other cost includes direct and indirect costs that could not be allocated to a main external cost category.



Detection and Recovery are the Most Costly Internal Activities

On an annualized basis, cyber crime detection and recovery activities account for 46 percent of total internal activity cost. Ex-post response (i.e., after the fact response, or remediation) is a close third, garnering 19 percent. And at 9 percent, containment of the cyber crime incident represents the lowest internal activity cost. Detection costs can be further broken down into specific cost components, which include direct labor (36 percent), indirect labor (13 percent), overhead (8 percent), amortized system costs (30 percent) and lost productivity (13 percent). These cost elements highlight a significant cost-reduction opportunity for organizations that are able to automate detection and recovery through technologies like security information and event management (SIEM) systems.

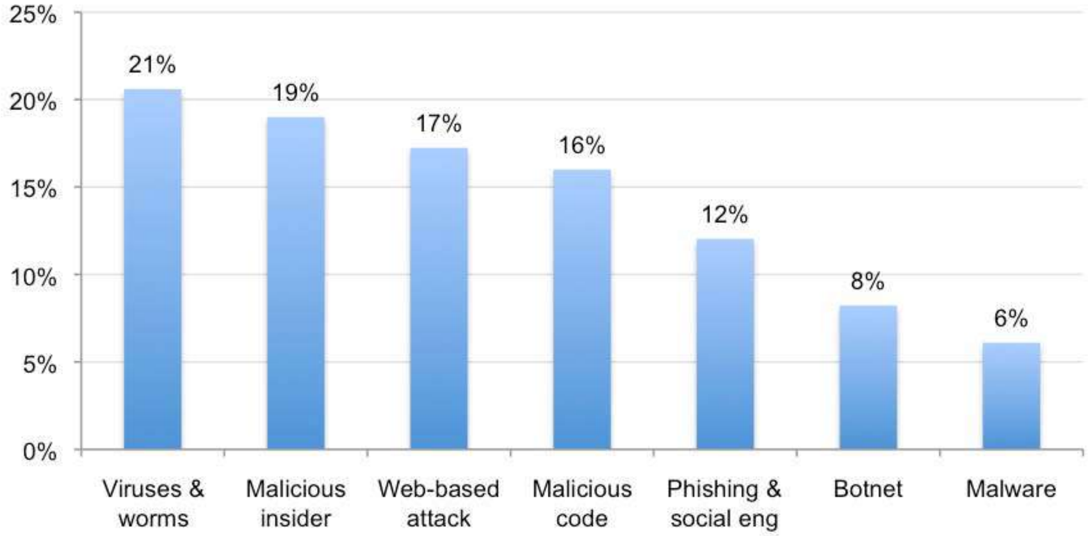
Bar Chart 4
Percentage cost by internal activity center
Investigation and escalation activities are shown separately because their underlying cost drivers are different.



Costs Vary Considerably by Attack Type

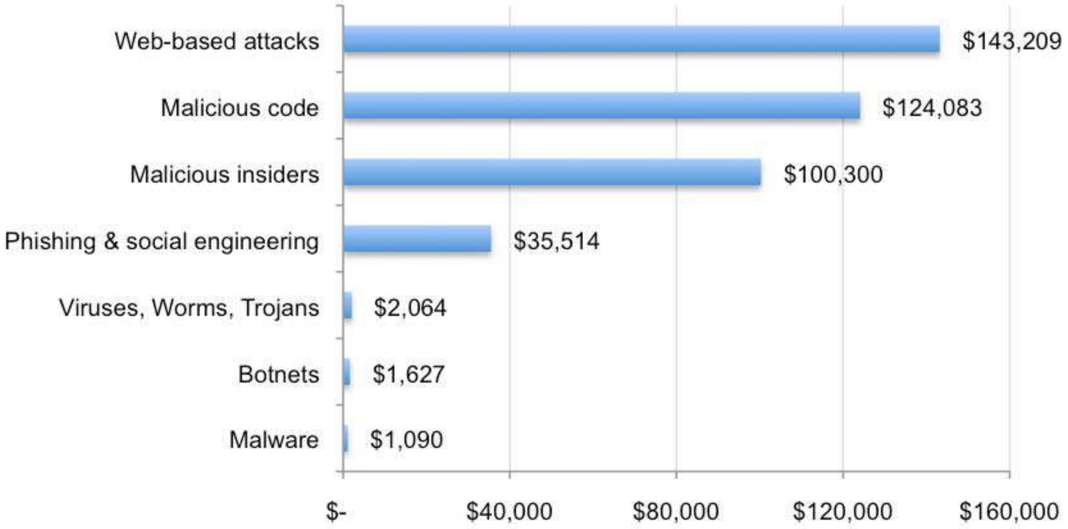
Bar Chart 5 reports the percentage of annualized cyber crime cost allocated to seven attack types for the 45 benchmark study participants. The cost of viruses, worms and Trojans and malicious insiders account for the highest annualized cyber attack cost.

Bar Chart 5
Percentage annualized cyber crime cost by attack type



Bar Chart 6 further 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 the 45 benchmarked companies. Clearly, the most expensive cyber crimes are web-based, malicious code and malicious insider attacks, activities which account for 90 percent of all cyber crime costs per organization on an annual basis.

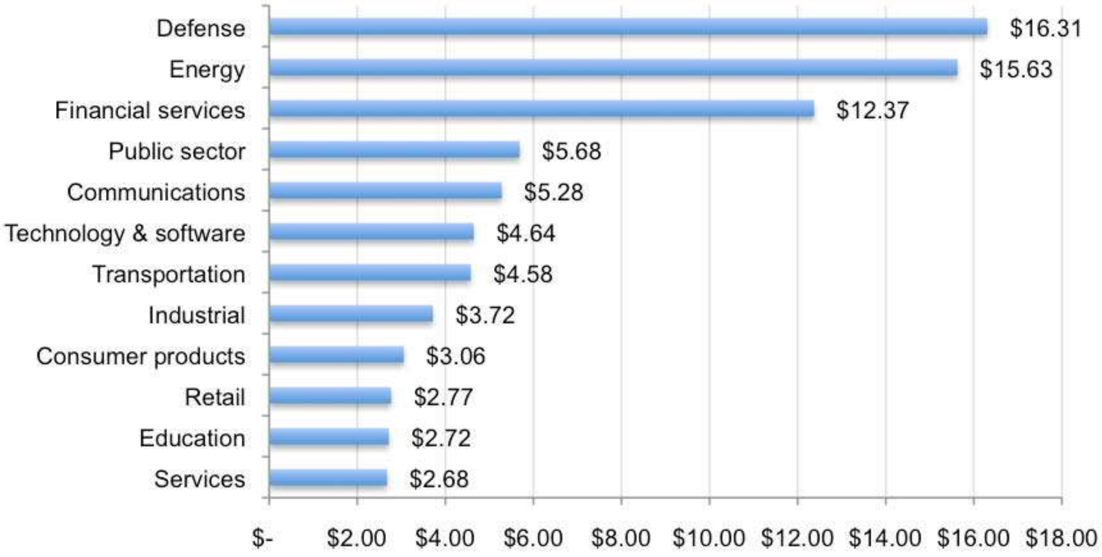
Bar Chart 6
Average annualized cyber crime cost weighted by attack frequency



The Cost of Cyber Crime Affects All Industries

The average annualized cost of cyber crime appears to vary by industry segment. As seen in Bar Chart 7, defense, energy and financial service companies experience substantially higher costs ($16.31 million, $15.63 million and $12.37 million, respectively) than organizations in retail, services and education (all under $6 million).

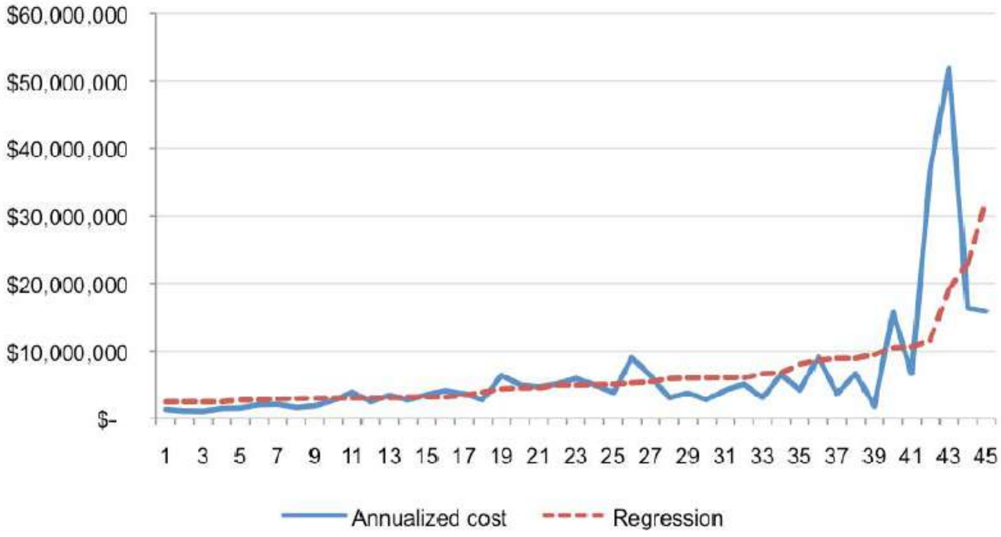
Bar Chart 7
Average annualized cost by industry sector
Reported in $ millions. Some of the industry segments are too small to make empirical inferences.



The Cost of Cyber Crime Varies by Organizational Size

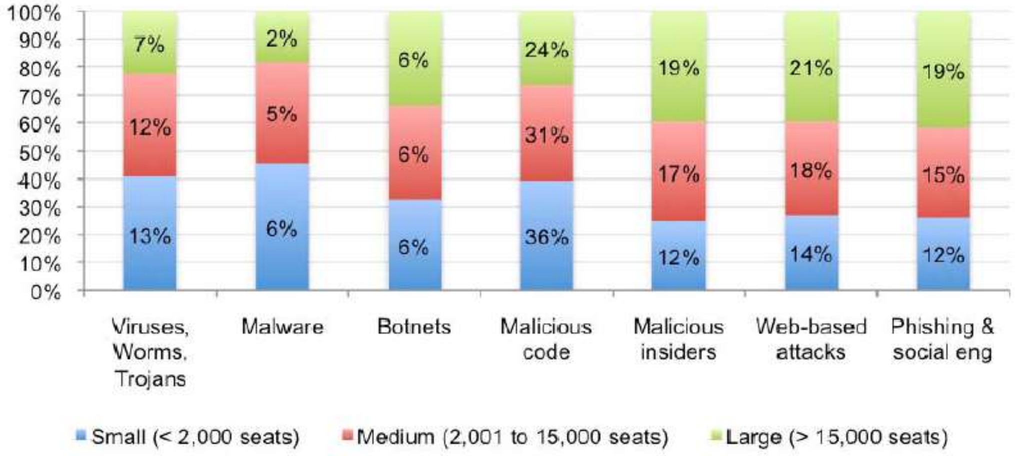
As shown in Line Graph 2, organizational size, as measured by the number of enterprise seats or nodes, is positively correlated to annualized cyber crime cost.

Line Graph 2
Annualized cost in ascending order by the number of enterprise seats
Regression performed on enterprise seats ranging from 500 to 105,000.



A comparison of smaller to larger-sized organizations reveals that the cost mix for given attacks varies by size of organization.

Bar Chart 8
The cost mix of attacks by organizational size
Size measured according to the number of enterprise seats within the participating organizations.

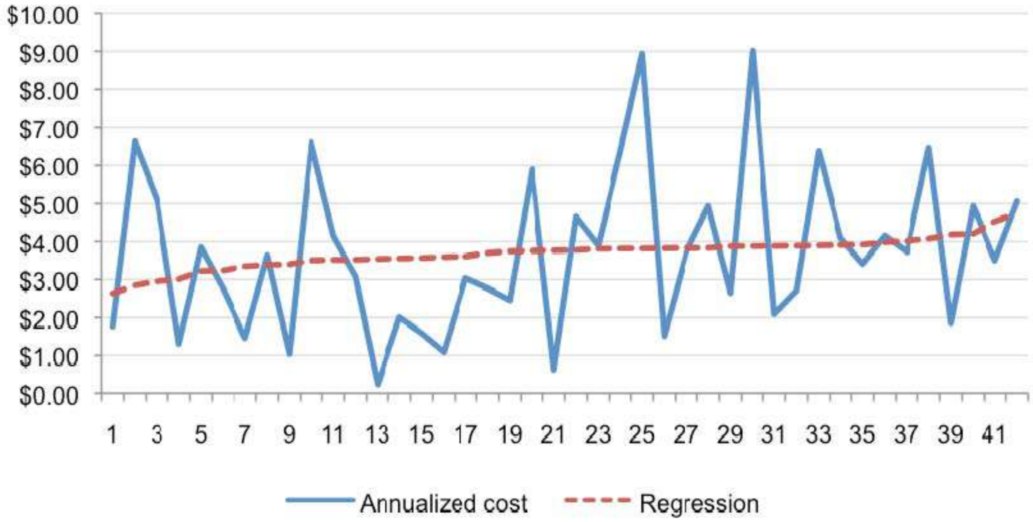


Bar Chart 8 reports the percentage distribution of cyber crime cost across the seven attack types. It reveals differences in the cost mix, wherein smaller companies experience a higher percentage of costs associated to malicious code and virus attacks than medium and larger-sized companies. In contrast, larger-sized companies experience a higher percentage for insider and phishing attacks than medium or smaller-sized companies.

The Organization's Security Posture Influences the Cost of Cyber Crime

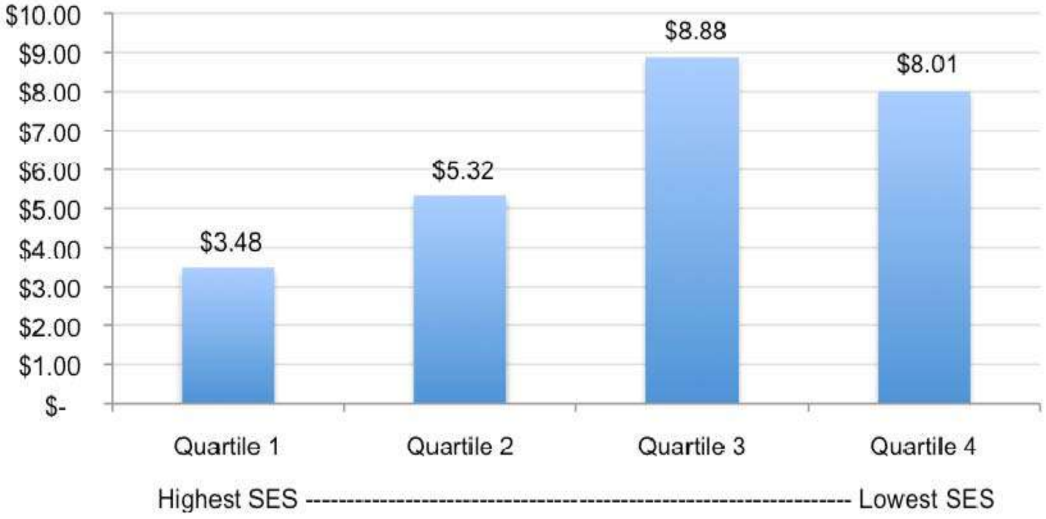
As with prior Ponemon Institute research, we measured the security posture of participating organizations as part of the benchmarking process for this study. Line Graph 3 reports the annualized cost and regression forecast of companies in descending order of security effectiveness, as measured by the SES (see footnote 2). 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 +1.9 to -1.28, with a mean value at .29.

Line Graph 3
Annualized cost in descending order by SES
Reported in $ millions. Regression performed on SES ranging from +1.9 to -1.28 with six outliers removed.



A comparison of organizations grouped into four quartiles based on SES reveals average cost differences. As noted in Bar Chart 9, the average cost for companies in quartile 1 is $3.45 million, while the average cost for quartile 3 is highest at $8.88 million.

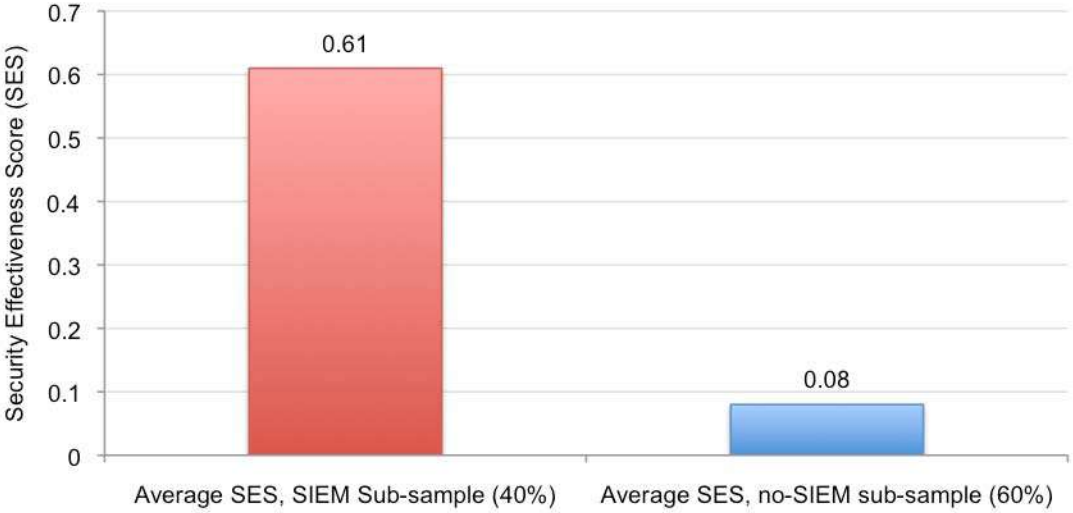
Bar Chart 9
Quartile comparison of annualized cost by SES
Reported in $ millions. Average SES for Quartile 1 = 1.08, Quartile 2 = .36, Quartile 3 = .09 and Quartile 4 = -.31



Organizations that have SIEM Technologies Realize a Higher Level of Security Effectiveness

Bar Chart 10 reports the average SES score companies with SIEM and no-SIEM. As can be seen, users of SIEM technologies realize a higher SES score than those in the no-SIEM sub-sample. Companies that had deployed a SIEM system achieved a 24 percent cost savings when dealing with cyber attacks versus those that had not.

Bar Chart 10
Comparison of SIEM and no-SIEM sub-sample on security effectiveness
SES is defined for the range of +1.9 to -1.28.

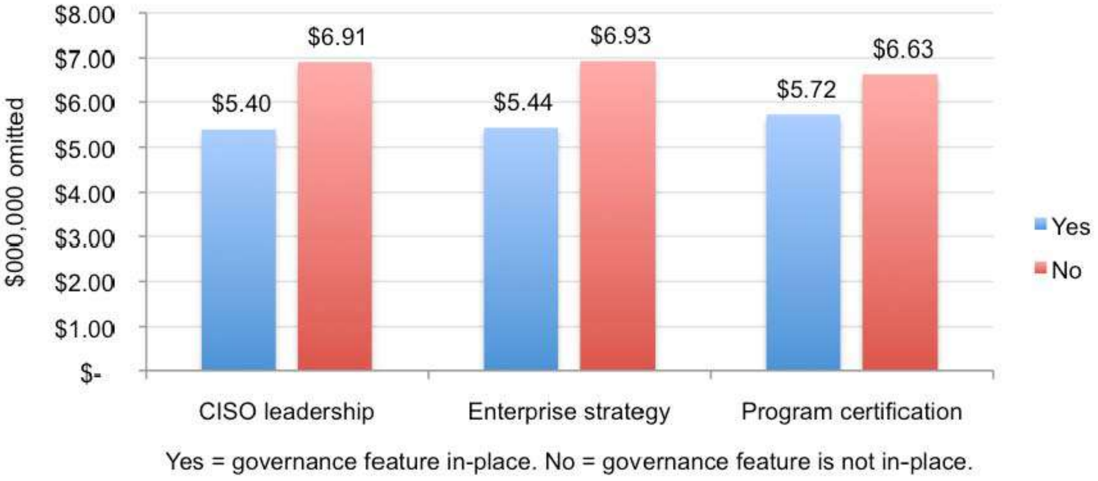


Good Governance Practices Moderate the Cost of Cyber Crime

The appointment of a CISO, the creation and rollout of an enterprise security strategy and adherence to a voluntary certification program (such as ISO) appear to lessen the total cost of cyber crime. Accordingly, 44 percent of companies have a fully dedicated information security leader or CISO. Forty-nine percent of companies have an enterprise strategy for information security, data protection, privacy and other related features. Forty-seven percent of companies voluntarily comply with a security certification body such as ISO, NIST or a comparable benchmark program.

Bar Chart 11 reports the total annualized cyber crime cost for organizations with and without the stated governance feature. Clearly, extrapolated costs are substantially lower for each one of the three governance features examined.

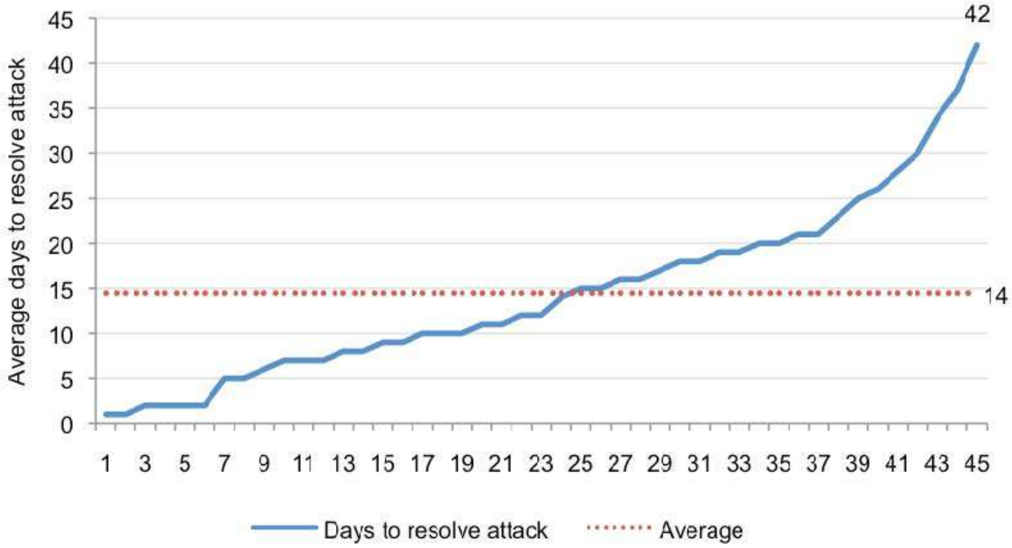
Bar Chart 11
Cost differences for three governance features
Reported in $ millions.



Time to Resolve or Contain Cyber Crimes Increases the Cost

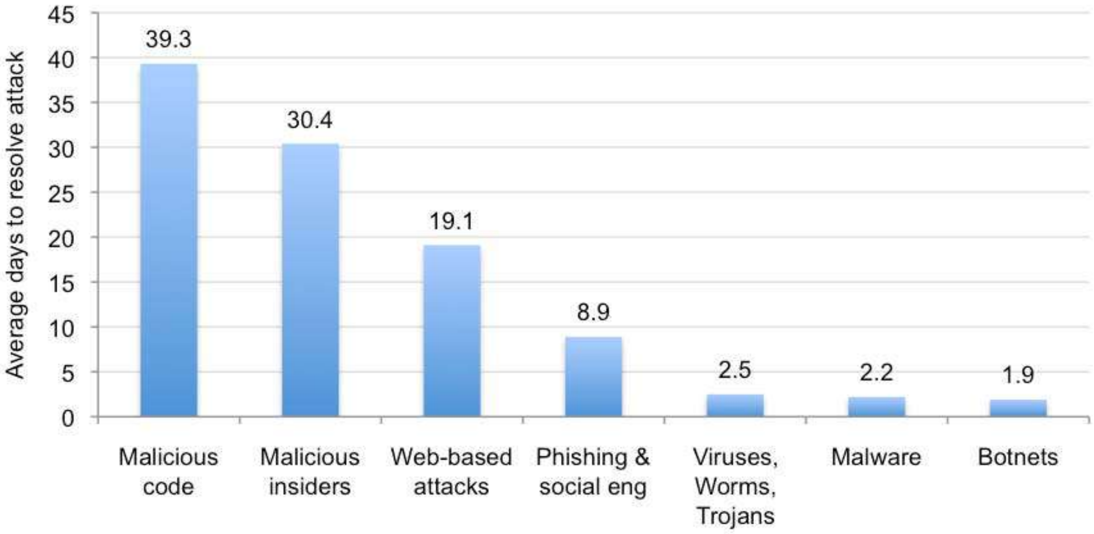
In the present sample, the average number of days to resolve cyber attacks is 14 days. The range of time to resolve or contain a cyber crime ranges from less than 24 hours to over 42 days. Our results suggest the average number of days to resolve cyber crime corresponds to the costs of cyber crime.

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



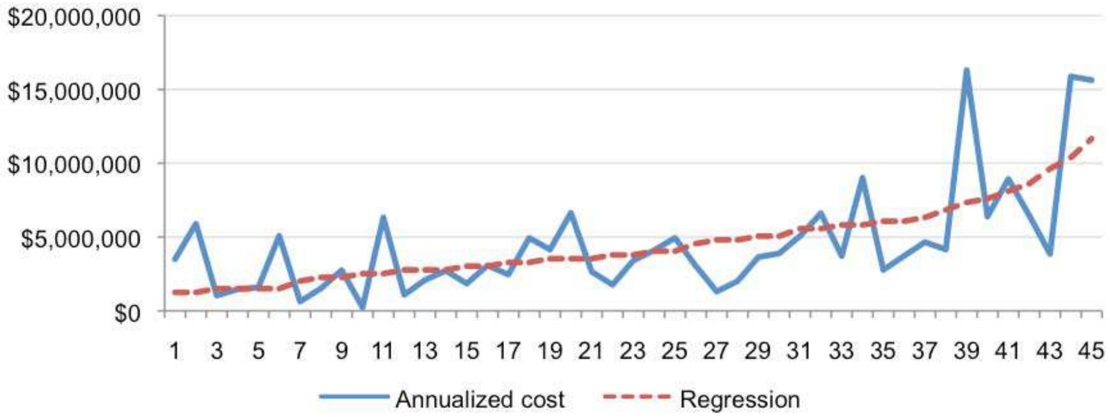
Bar Chart 12 reports the average days to resolve cyber attacks for seven different attack types studied in this report. It is clear from this chart that it takes substantially more time, on average, to resolve malicious insider, malicious code and web-based attacks than botnets, malware and viruses. In other words, the elapsed time to resolve a cyber attack is very likely to be associated, or correlated, with total costs.

Bar Chart 12
Average days to resolve attack for seven attack types



Line Graph 5 reports the annualized cost and regression forecast for companies in ascending order of days to resolve cyber attack. This graph clearly shows that delays in resolving or containing cyber attacks substantially increases costs for the benchmark sample. On average, companies expend $247,757 every 14 days or $17,696 per day per attack.

Line Graph 5
Annualized cost in ascending order by days to resolve attack
Regression performed on days ranging from 1 to 42 days.



.

Part 3. Study Overview and Methodology

The cost of cyber crime benchmark instrument is designed to collect descriptive information from data protection or information security practitioners about the costs incurred either directly or indirectly as a result of cyber attacks. The survey design relies upon a shadow costing method used in applied economic research. This method does not require subjects to provide actual accounting results, but instead relies on broad estimates based on the experience of the subject.

Within each category, cost estimation is a two-stage process. First, the survey requires individuals to provide direct cost estimates for each privacy cost category by checking a range variable. A range variable is used rather than a point estimate to preserve confidentiality (in order to ensure a higher response rate). Second, the survey requires participants to provide a second estimate for both indirect cost and opportunity cost, separately. These estimates are calculated based on the relative magnitude of these costs in comparison to a direct cost within a given category. Finally, we conduct a follow-up interview to obtain additional facts, including estimated revenue losses as a result of the cyber crime.

The size and scope of survey items is 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 use 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 use in our benchmark study. As can be seen, we examine 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 contains descriptive cost for each one of the five cost activity centers. Within each cost activity center, the survey requires 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 does not capture company-specific information of any kind. Subject materials contain 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 consider crucial to the measurement of cyber crime cost. Based on discussions with learned experts, the final set of items focus on a finite set of direct or indirect cost activities. After collecting benchmark information, each instrument is examined carefully for consistency and completeness. In this study, seven companies were rejected because of incomplete, inconsistent or blank responses.

The study was launched in January 2010. The recruitment started with a personalized letter and a follow-up phone call to 311 organizations for possible participation in our study. While 54 organizations initially agreed to participate, 47 organizations permitted researchers to complete the benchmark analysis. Two cases were removed from our final analysis because they fell below our minimum size requirement of 500 or more enterprise seats. 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, and 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 45 benchmark companies, we collected information over four consecutive weeks. Field research was conducted over a five-month period concluding on June 23, 2010. Hence, the four consecutive weeks for any given organization was not necessarily the same time period. 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).

Sample of Participating Companies

Pie Chart 1 and Table 1 summarize the sample of participating companies based on 12 primary industry classifications. As can be seen, financial services (22 percent) represent the largest segment. This includes retail banking, insurance, brokerage and credit card companies. The second and third largest segments are technology and communication companies, respectively (both at 11 percent).

Pie Chart 1
Sample distribution by industry

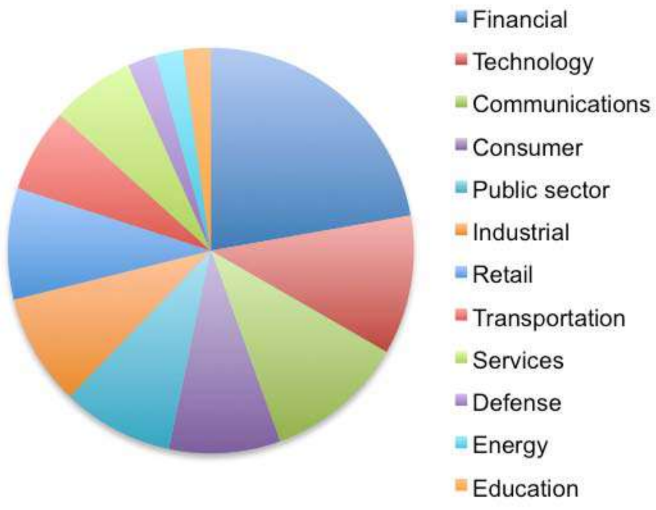
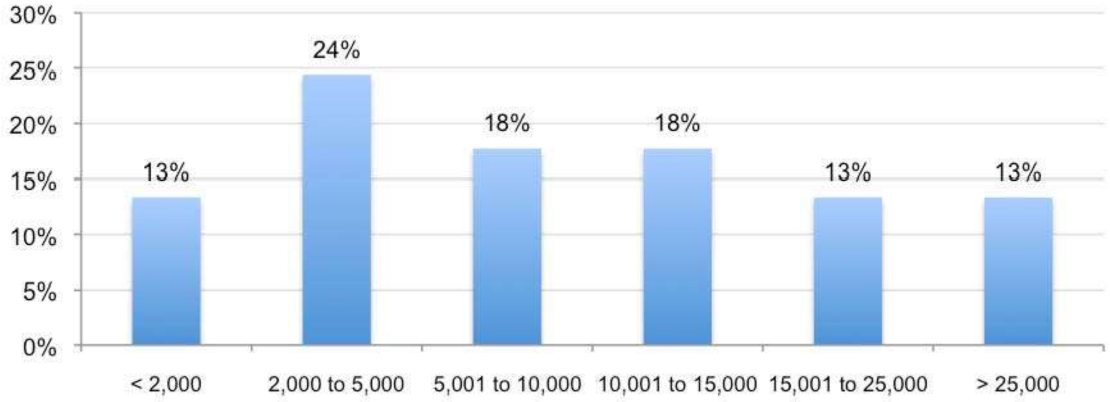


Table 1
Percentage frequency by industry

Industry	Pct%
Financial	22%
Technology	11%
Communications	11%
Consumer	9%
Public sector	9%
Industrial	9%
Retail	9%
Transportation	7%
Services	7%
Defense	2%
Energy	2%
Education	2%

Bar Chart 13 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 500 seats. The largest enterprise has 105,000 seats.

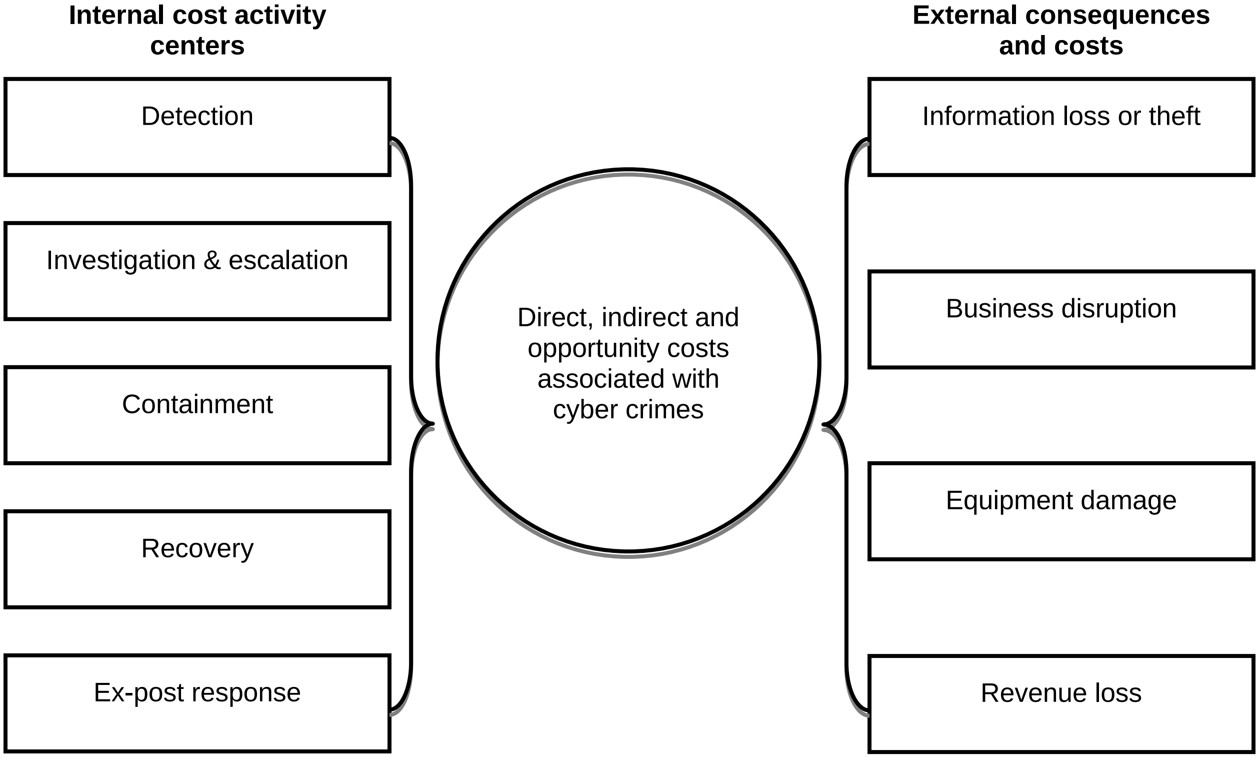
Bar Chart 13
Percentage distribution of participating organizations by enterprise seats (size)



Part 4. Cost of Cyber Crime Benchmark Framework

We are pleased to present the summarized findings of our first benchmark study that seeks to examine the inherent cost structure that organizations may incur as a result of cyber attacks against endpoints, networks and enterprise systems. Our benchmark results of 45 organizations are intended to provide a meaningful baseline for companies experiencing a wide array of cyber attacks including viruses, malware, Trojans, worms, SQL injections, botnets, malicious employees and others.

Figure 1
Activity-based Costing Framework for Cyber Crime


Internal cost activity centers
Detection
Investigation & escalation
Containment
Recovery
Ex-post response
Direct, indirect and opportunity costs associated with cyber crimes
External consequences and costs
Information loss or theft
Business disruption
Equipment damage
Revenue loss

The benchmark 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 methodology contains questions designed 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.

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:[2]

- Detection: Activities that enable an organization to reasonably detect and possibly deter cyber attacks or advanced threat. This includes allocated (overhead) costs of certain enabling technologies that enhance mitigation or early detection.

[2] Internal costs are extrapolated using labor (time) as a surrogate for indirect and indirect costs. This is also used to allocate an overhead component for fixed costs such as multiyear investments in technologies.

- 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).[3]

[3] 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 over the past 12 months. 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 reference group of over 311 separate organizations, all believed to have experienced one or more cyber attacks over the past 12 months. Forty-five 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 direct and indirect expenses. 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 $3.8 million per year, but can range from $1 million to $52 million per year per company.

- Cyber attacks have become common occurrences. The companies in our study experienced 50 discernible and successful cyber attacks per week which translates to more than one successful attack per company per week.

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

- Detection and recovery are the most costly internal cost activities with labor representing the majority of costs at 49 percent. This highlights a significant cost-reduction opportunity for organizations that are able to automate detection and recovery through technologies like security information and event management (SIEM) systems.

- Mitigation, detection and recovery costs from cyber attacks can be mitigated by deploying enabling technologies such as SIEM and enterprise threat and risk management solutions. In our benchmark study, companies that had deployed a SIEM system achieved a 24 percent cost saving when dealing with cyber attacks versus those that had not.

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.