2015 Cost of Cyber Crime Study: Australia

Sponsored by Hewlett Packard Enterprise

Independently conducted by Ponemon Institute LLC

Publication Date: September 2015

2015 Cost of Cyber Crime Study: Australia

Benchmark Study of Australian Companies

Ponemon Institute September 2015

Part 1. Executive Summary

We are pleased to present the *2015 Cost of Cyber Crime Study: Australia*, the fourth annual study of Australian companies. Sponsored by Hewlett Packard Enterprise, this year's study is based upon a representative sample of 28 organisations in various industry sectors.

This is the sixth year Ponemon Institute conducted the cost of cyber crime study in the United States and the fourth year for companies in the United Kingdom, Germany and Japan. Last year we added the Russian Federation. This year, for the first time, we conducted the research in Brazil.

According to the Australian Signals Directorate, the most commonly targeted sectors are banking and finance, resources and energy, defence capability and telecommunications. Last year, the Australian government opened the Australian Cyber Security Centre to co-locate defence intelligence agencies, the Attorney-General and the Australian Federal Police cyber units.[1]

Australia Study at a Glance

28 AU companies, 252 companies in 7 countries
283 interviews with AU company personnel
200 total attacks used to measure total cost
$4.9 million is the average annualised cost
13% net increase in cost over the past year
16% average ROI for 7 security technologies

For purposes of this study, we refer to cyber attacks as criminal activity conducted via the Internet. These attacks can include stealing an organisation'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 organisations 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 organisations' actual cyber crime incidents. Approximately 10 months of effort is required to recruit companies, build an activity-based cost model to analyse the data, collect source information and complete the analysis.

For consistency purposes, our benchmark sample consists of only larger-sized organisations (i.e., with a minimum of appoximately 1,000 enterprise seats[2]). The study examines the total costs organisations 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 organisation's security posture or compliance with standards, policies and regulations.

[1] "Cyber Attacks on Australian businesses rose 20pc last year," by Emily Stewart, Australian Broadcasting Corporation, 23 April 2015

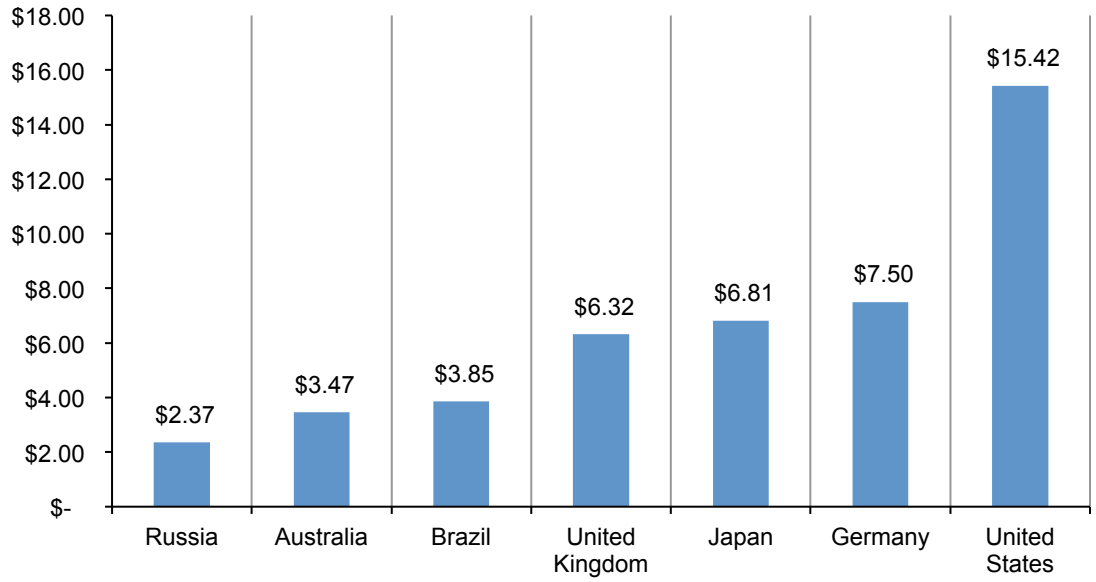
[2] Enterprise seats refer to the number of direct connections to the network and enterprise systems.

Global at a glance

This year's annual study was conducted in the United States, United Kingdom, Germany, Australia, Japan, the Russian Federation, and for the first time, Brazil, with a total benchmark sample of 252 organisations. 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 million[3].

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.

Cost of Cyber Crime FAQs

What is a cyber attack? A cyber attack is any type of offensive maneuver employed by individuals or whole organisations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices 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.[4] The cost of cyber crime can vary according to the cause and the safeguards in place at the time of attack.

How do you collect the data? Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a 10-month period. Field research for the 2015 study began in January 2015 and was completed in August 2015. In this year's study we interviewed 283 IT, compliance and information security practitioners who are knowledgeable about their organisation's costs associated with resolving the cyber attack. For privacy purposes we do not collect any organisation-specific information.

How do you calculate the cost of cyber crime? To calculate the average cost of cyber crime, we analysed 200 attacks experienced by the organisations and both the direct and indirect expenses incurred in dealing with the attacks. 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 organisational 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 organisation. In survey research, the unit of analysis is the individual. We recruited 28 organisations to participate in this study and conducted 283 interviews.

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 data breaches because these are not typical of the attacks most organisations experience. In order to be representative of the population of Australian organisations and draw conclusions from the research that can be useful in understanding costs when protected information is lost or stolen, we do not include cyber attacks involving organisations with fewer than approximately 1,000 enterprise seats, which refers to the number of direct connections to the network and enterprise systems.

Are you tracking the same organisations each year? Each annual study involves a different sample of companies. In other words, we are not tracking the same sample of organisations over time. To be consistent, we recruit and match organisations with similar characteristics such as the company's industry, headcount and geographic footprint. Since starting this research more than four years ago, we have studied the cyber crime experiences of 124 Australian organisations.

[4] Source: Wikipedia

Summary of Australian findings

Following are the most salient findings for a sample of 28 Australian-based organisations requiring 283 separate interviews to gather cyber crime cost results. In several places in this report, we compare the present findings to previous studies.

Cyber crimes continue to be very costly for organisations. We found that the mean annualised cost for 28 benchmarked organisations is $4.9 million per year, with a range from $792,932 to $18 million. Last year's mean cost per benchmarked organisation was $4,270,804. Thus, we observe a 13 percent increase in mean value.

Cyber crime cost varies by organisational size. Results reveal a positive relationship between organisational size (as measured by enterprise seats) and annualised cost.[5] However, based on enterprise seats, we determined that small organisations incur a significantly higher per capita cost than larger organisations ($1,919 versus $372).

All industries fall victim to cybercrime, but to different degrees. The average annualised cost of cyber crime appears to vary by industry segment, where energy & utilities, financial services and technology experience substantially higher cyber crime costs than organisations in media, consumer products and retail.

The most costly cyber crimes are those caused by malicious insiders, denial of services, and malicious code. These account for more than 45 percent of all cyber crime costs per organisation on an annual basis.[6] 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 organisational 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 31 days, with an average cost to participating organisations of $419,542 during this 31-day period. This represents a 41 percent increase from last year's estimated average cost of $276,323, which was based upon a 23-day resolution period. Results show that malicious insider attacks can take about 50 days on average to contain.

Business disruption continues to represent the highest external cost, followed by the costs associated with information loss.[7] On an annualised basis, business disruption accounts for 38 percent of total external costs (down 2 percent from last year). Costs associated with information and revenue loss account for 58 percent of external costs, an increase from 54 percent last year.

Detection and recovery are the most costly internal activities. On an annualised basis, detection and recovery combined account for 48 percent of the total internal activity cost with productivity and direct labour representing the majority of these costs.

[5]In this study, we define an enterprise seat as one end-user identity/device connected to the company's core networks or enterprise systems.
[6]This year the category malicious insider includes the cost of stolen devices.
[7]In the context of this study, an external cost is one that is created by external factors such as fines, litigation, marketability of stolen intellectual properties and more.

Activities relating to IT security in the network layer receive the highest budget allocation (30 percent). In contrast, the host layer receives the lowest funding level at 6 percent.

Deployment of security intelligence systems makes a difference. In total, 15 companies (53 percent) deploy security intelligence tools such as SIEM, IPS with reputation feeds, network intelligence systems, big data analytics and others. The largest cost differences in millions pertain to recovery ($.96 vs. $1.43) and incident management ($.33 vs. $.69).

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

Deployment of enterprise security governance practices moderates the cost of cyber crime. Findings show companies that employ certified expert security personnel and appoint a high-level security leader have cyber crime costs that are lower than companies that have not implemented those practices.

Part 2. Key findings

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

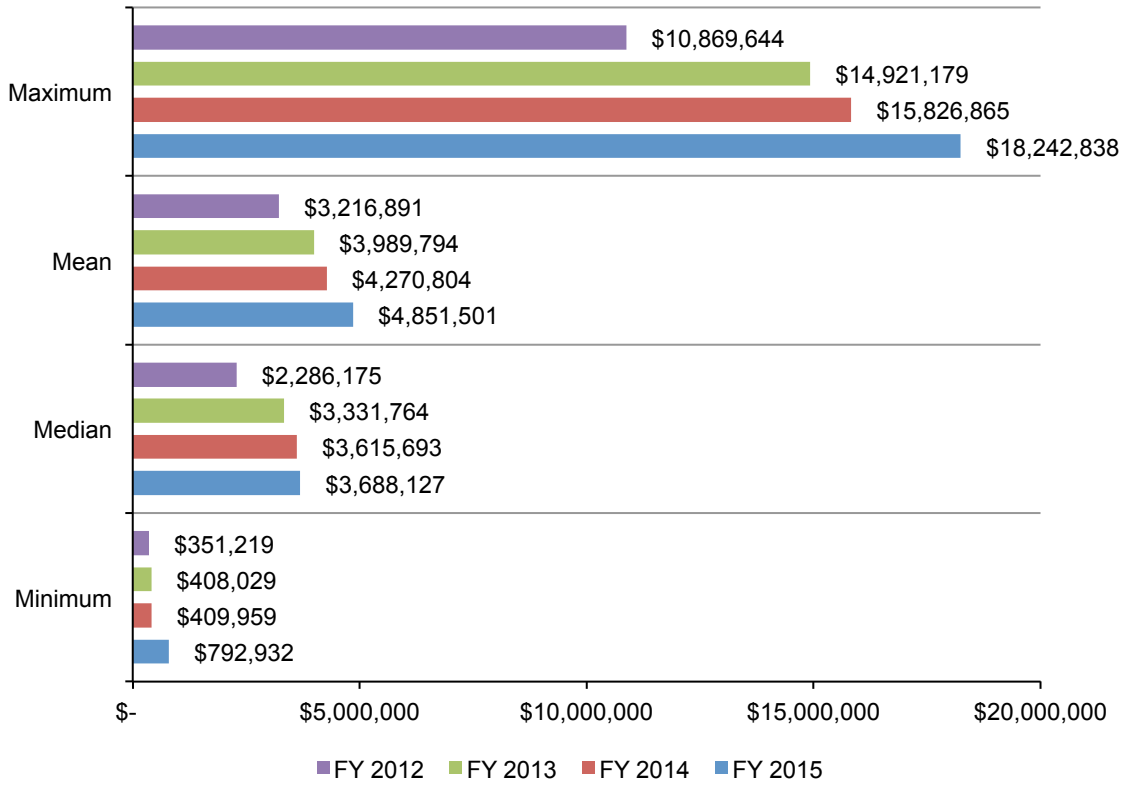
- **The average cost of cyber crime by organisational size and industry**
- **The type of attack influences the cost of cyber crime**
- **An analysis of the cost components of cyber crime**

The average cost of cyber crime by organisational size and industry

To determine the average cost of cyber crime, the 28 organisations 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 annualised cost.[8]

As shown in Figure 2, the total annualised cost of cyber crime in 2015 ranges from a low of $792,932 million to a high of $18 million. The mean annualised cost of cyber crime in the benchmark sample is $4.9 million – an increase from last year's mean value of $4.3 million. This is an increase of 13 percent from last year.

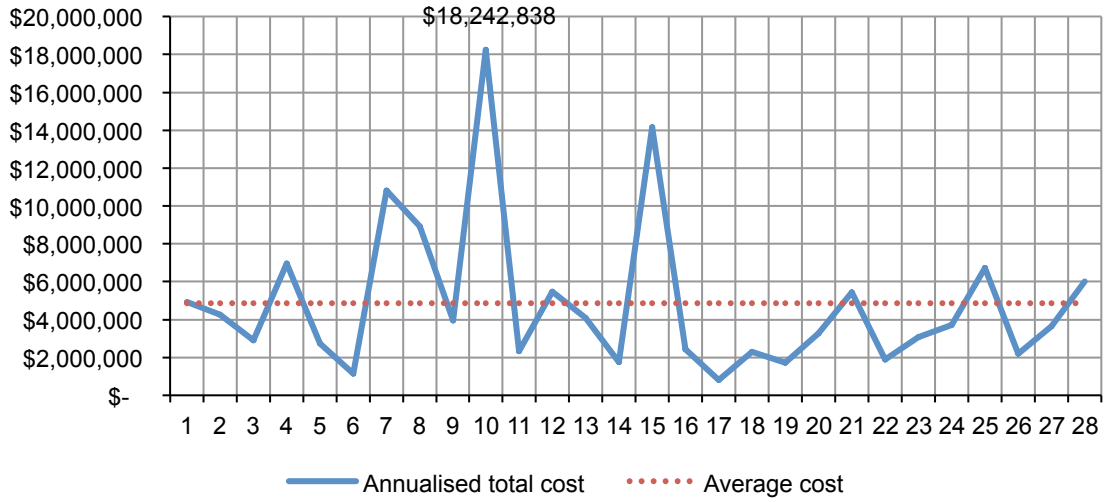
Figure 2. The cost of cyber crime



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

Figure 3 reports the distribution of annualised total cost for 28 companies. As can be seen, 18 companies in our sample incurred total costs below the mean value of $4.9 million, thus indicating a skewed distribution. The highest cost estimate of $18 million was determined not to be an outlier based on additional analysis. Ten other organisations experienced an annualised total cost of cyber crime above the average.

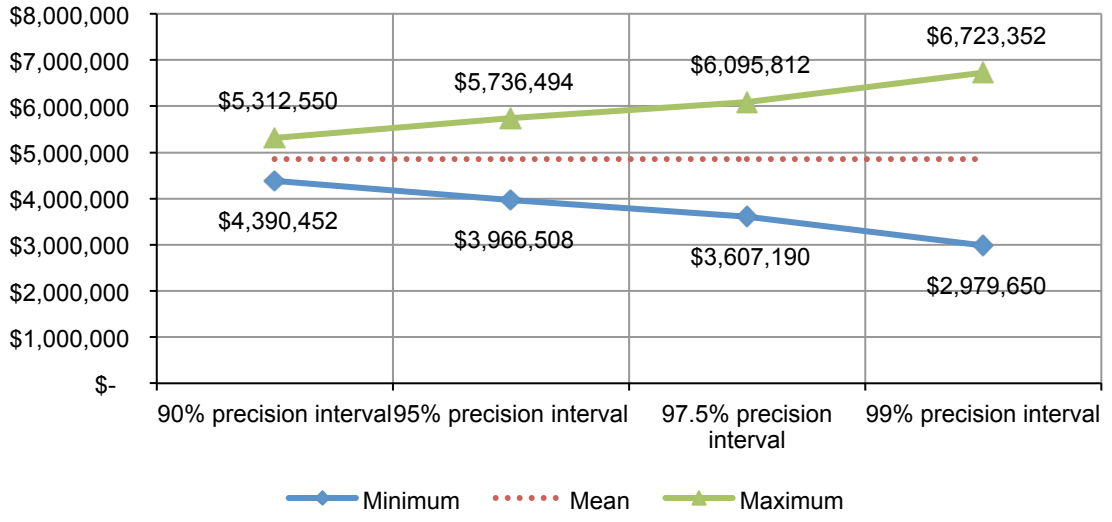
Figure 3. Annualised total cost of cyber crime for 28 participating companies



As part of our analysis we calculated a precision interval for the average cost of $4.9 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.

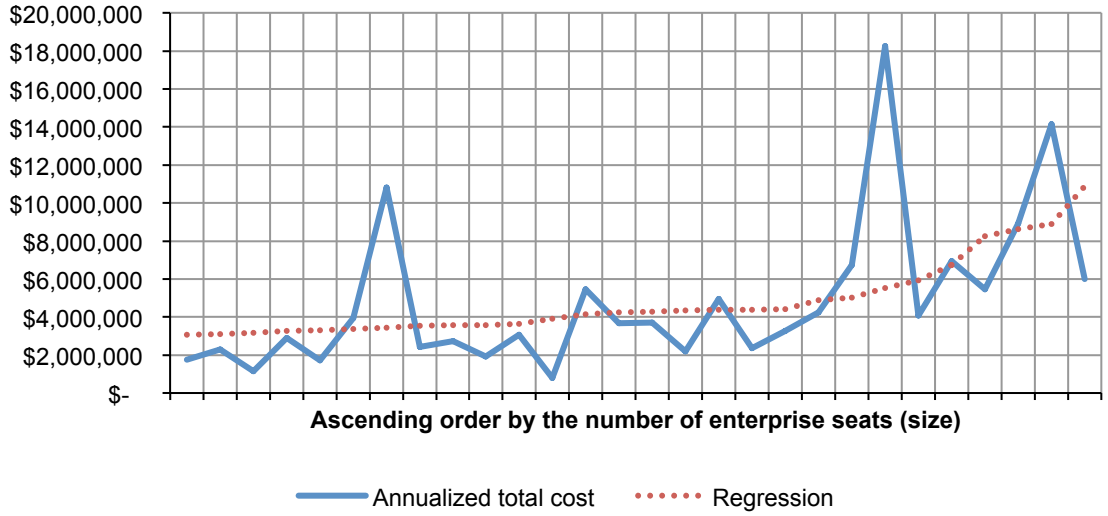
The range of possible cost estimates widens at increasingly higher levels of confidence, as shown in Figure 4. Specifically, at a 90 percent level of confidence we expect the range of cost to be between $4.4 million and $5.3 million.

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



The cost of cyber crime varies by organisational size. As shown in Figure 5, organisational size, as measured by the number of enterprise seats or nodes, is positively correlated to annualised cyber crime cost. This positive correlation is indicated by the upward slopping regression line. In this year's study, the number of enterprise seats ranges from 890 to 39,554.

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



Organisations 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 organisational size and the cost of cyber crime. Table 1 shows the quartile average cost of cyber crime for four years. There are approximately seven companies in each quartile.

Table 1. Quartile analysis				
Quartile 1	$1,259,489	$1,611,092	$1,515,063	$1,689,169
Quartile 2	$1,970,364	$3,630,898	$3,072,993	$2,913,541
Quartile 3	$3,028,308	$4,354,655	$5,215,855	$4,550,160
Quartile 4	$6,311,444	$6,098,893	$7,052,968	$10,253,134

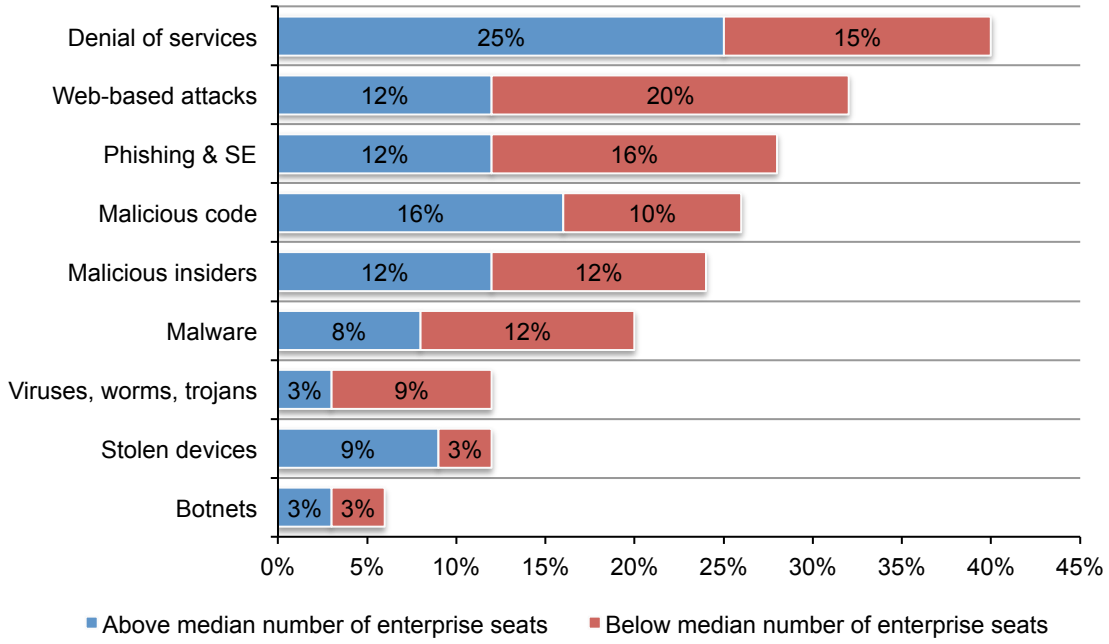
Table 2 reports the average cost per enterprise seat (a.k.a. per capita cost) compiled for four quartiles ranging from the smallest (Quartile 1) to the largest (Quartile 4). Consistent with prior years, the 2015 average per capita cost for organisations with the fewest seats is 2.7 times higher ($1,919) than the average per capita cost for organisations with the most seats ($372).

Table 2. Quartile analysis				
Quartile 1 (smallest)	$651	$974	$755	$1,919
Quartile 2	$276	$567	$589	$621
Quartile 3	$193	$367	$513	$481
Quartile 4 (largest)	$140	$251	$282	$372

Certain attacks are more costly based on organisational 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.

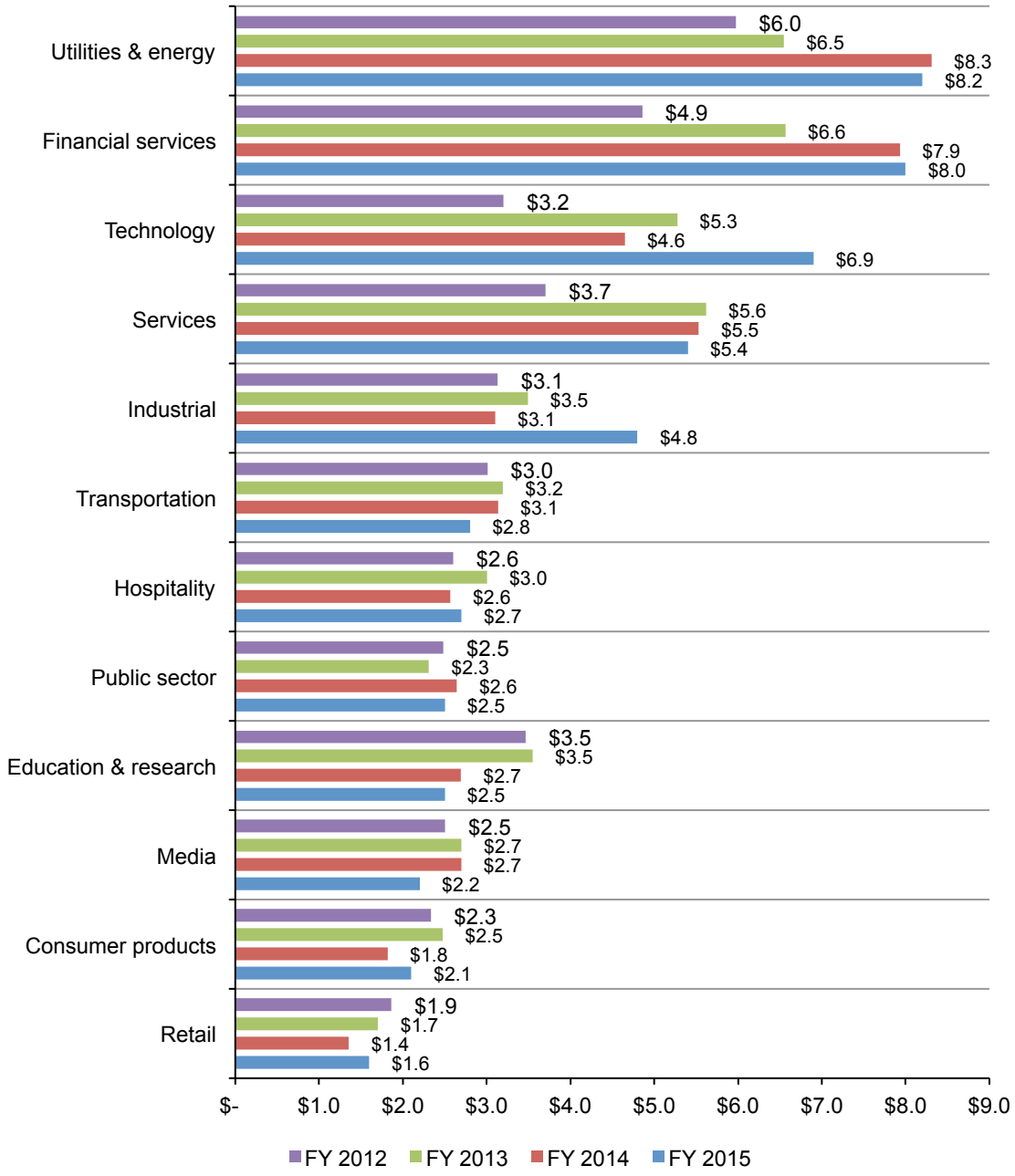
In Figure 6, we compare smaller and larger-sized organisations based on the sample median of 6,847 seats. Smaller organisations (below the median) experience a higher proportion of cyber crime costs relating to web-based attacks, phishing & social engineering, malware and viruses, worms and trojans. In contrast, larger organisations (above the median) experience a higher proportion of costs relating to denial of services, malicious code and stolen devices.

Figure 6. Percentage of total cost for nine attack types by organisational size
Size measured according to the number of enterprise seats within the participating organisations



The cost of cyber crime impacts all industries. The average annualised cost of cyber crime appears to vary by industry segment. In this year's study we compare the 2015 results to the past three years the study was conducted. As seen in Figure 7, the cost of cyber crime in the technology sector rose significantly. This sector includes organizations in software and IT management. Organisations in media, consumer products and retail appear to have a lower overall cyber crime cost over four years.[9]

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



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

The type of cyber attack influences the cost of cyber crime

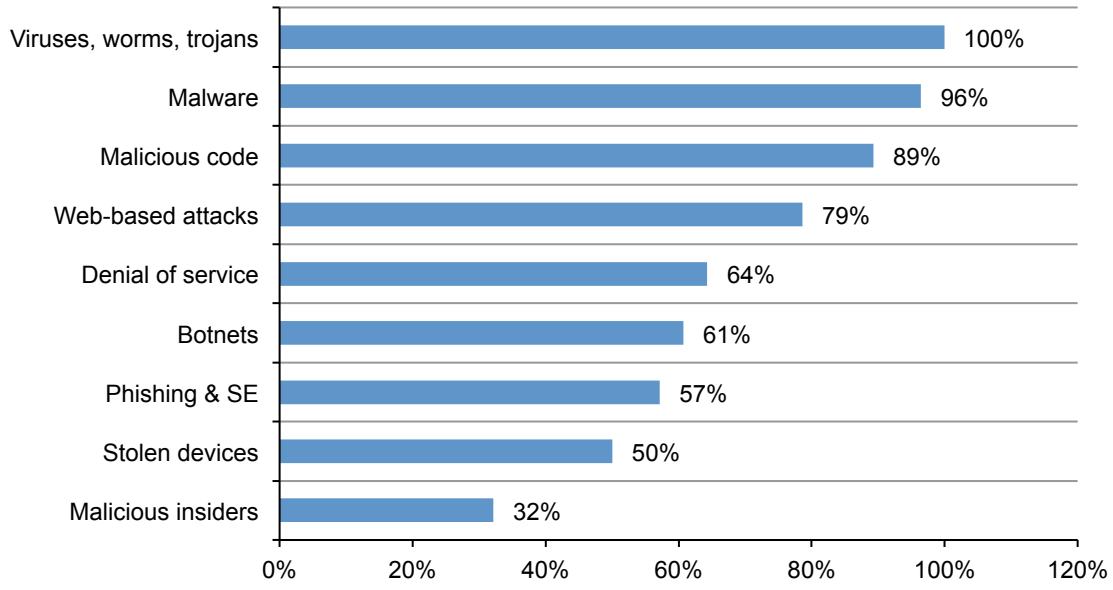
In our studies we look at nine different attack vectors as the source of the cyber crime. This year, the benchmark sample of 28 organisations experienced 50 discernible cyber attacks per week, which translates to 1.8 successful attacks per benchmarked organisation each week.

Last year, the benchmark sample of 30 organisations experienced 47 discernible cyber attacks per week, which translates to 1.6 successful attacks per benchmarked organisation each week. In 2013, the benchmark sample of 33 organisation experienced 45 discernible cyber attacks per week, which translates to 1.4 successful attacks per benchmarked organisation each week. In 2012, the number of successful attacks each week was 40.

Figure 8 summarises in percentages the types of attack methods experienced by participating companies. Virtually all organisations 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 classify malware attacks that successfully infiltrate the organisations' networks or enterprise systems as a malicious code attack.

Eighty-nine percent experienced malicious code and 79 percent had web-based attacks. Only 32 percent of attacks were due to malicious insiders.

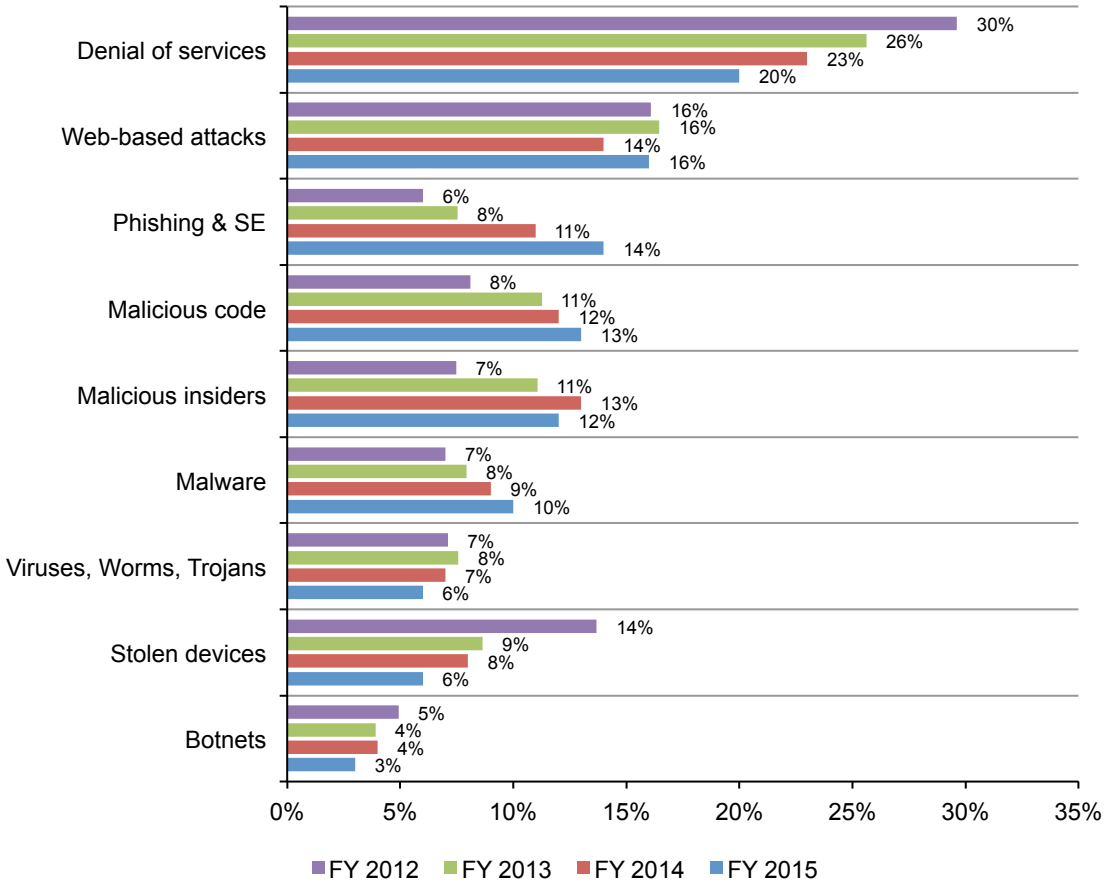
Figure 8. Types of cyber attacks experienced by 28 benchmarked companies



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

In total, the top three attacks account for more than 45 percent of the total annualised cost of cyber crime experienced by 28 companies. While they do not occur as frequently as viruses and malware, denial of service (DoS) attacks are the most costly as a percentage of the average cost of cyber crime. The least costly are stolen devices, viruses, worms and trojans and botnets.

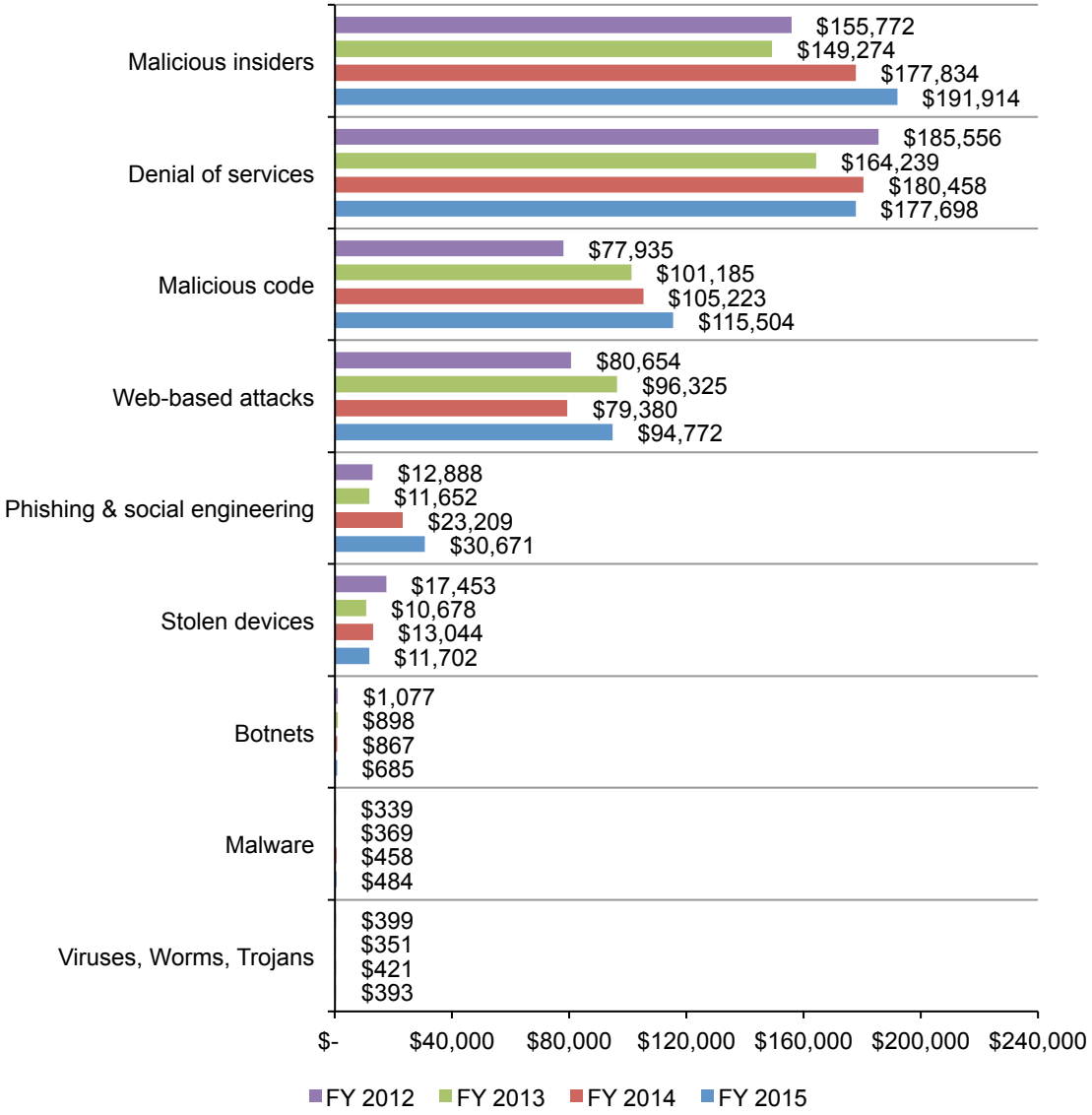
Figure 9. Percentage annualised cyber crime cost by attack type



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 analysed based upon the frequency of incidents. The most expensive attacks are malicious insiders, denial of services and malicious code. As discussed previously, these attacks represent more than 45 percent of the total annualized cost of cyber crime (Figure 9).

Another interesting finding is the significant cost increase for the attack category termed malicious insiders, which rose by $42,640 since 2013. In the context of our study, malicious insiders include employees, temporary employees, contractors and, possibly, business partners. Denial of services attacks decreased slightly in cost and the cost of malicious code increased slightly.

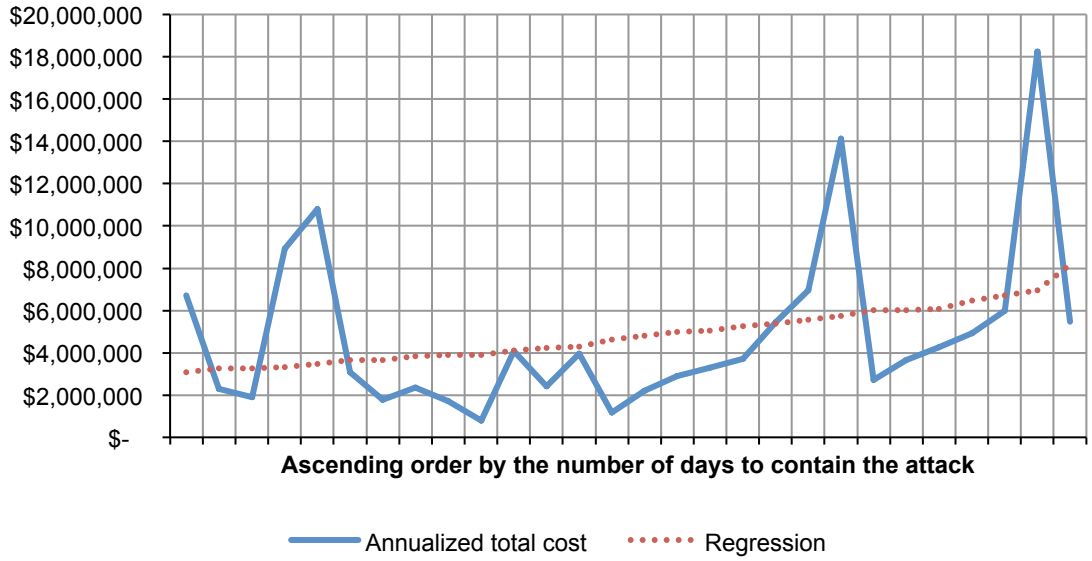
Figure 10. Average annualised cyber crime cost weighted by attack frequency



Time to resolve or contain cyber crimes increases the cost. The mean number of days to resolve cyber attacks is 31 with an average cost of $13,628 per day – or a total cost of $419,542 over the 31-day remediation period. The number of days to resolve an attack ranges from 3 days to 83. 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). Last year's mean number of days to resolve cyber attacks was 23 with an average cost of $11,997 per day – or a total cost of $276,323 over the 23-day remediation period.

Figure 11 shows the annualised 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.

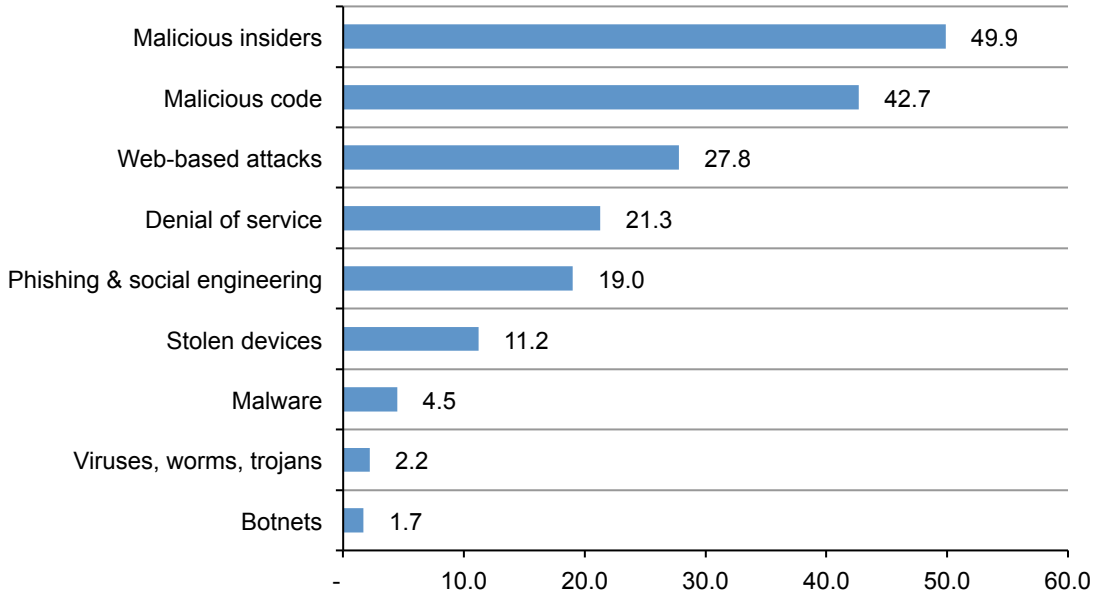
Figure 11. Total annualised cost by the number of days to contain the attack



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

Figure 12 reports the average days to resolve cyber attacks for nine different attack types studied in this report. It is clear from this chart that it takes the most amount of time, on average, to resolve attacks from malicious insiders, malicious code and web-based attacks. Malware, viruses and botnets on average are resolved in just a few days.

Figure 12. Average days to resolve attack by attack type
Estimated average time is measured for each attack type in days

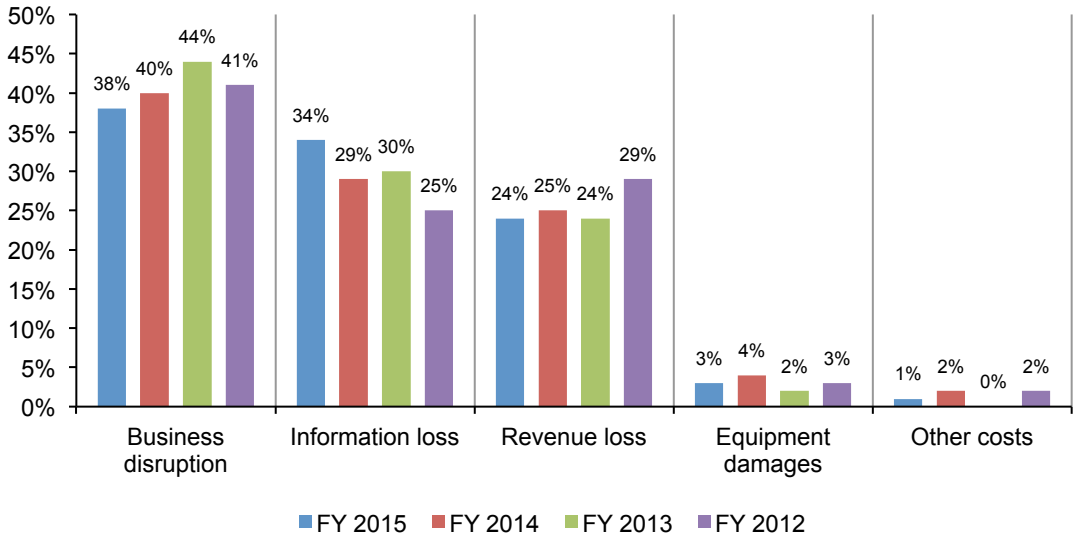


An analysis of the cost components of cyber crime

Business disruption remains the most expensive consequence of a cyber crime. In this research we look at five primary consequences of a cyber attack: the loss of information, disruption of business, loss of revenue, damage to equipment and other. As shown in Figure 13, business disruption represents the highest component (38 percent) of the total cost to an organisation that has a cyber attack. However this cost has been trending downward since 2013.

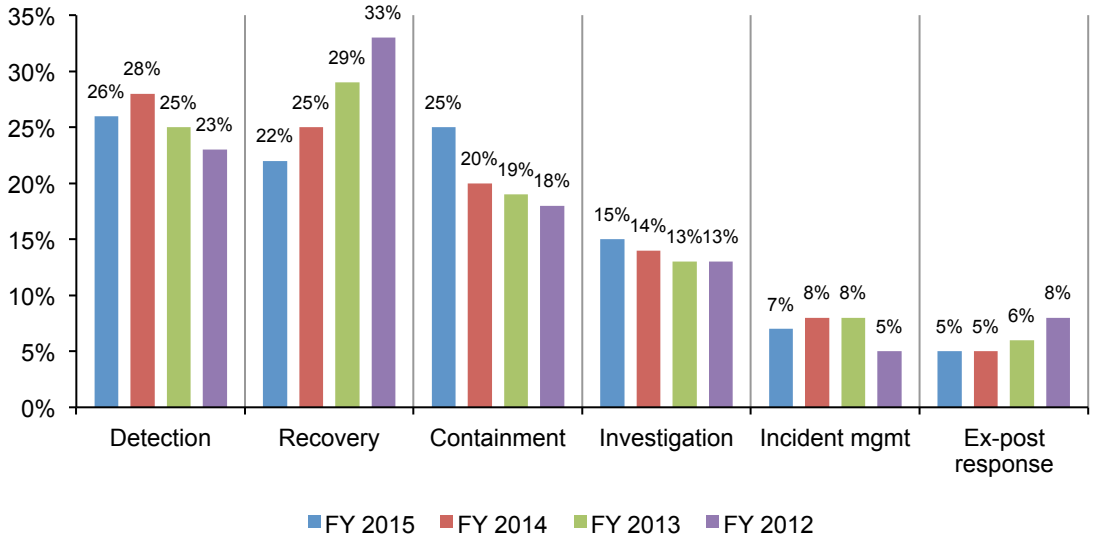
Information loss increased significantly since last year and revenue loss decreased slightly. These two consequences of a cyber incident represent 58 percent of the total cost for external consequences. The cost of equipment damages has been fairly consistent over the past 4 years.

Figure 13. Percentage cost for external consequences



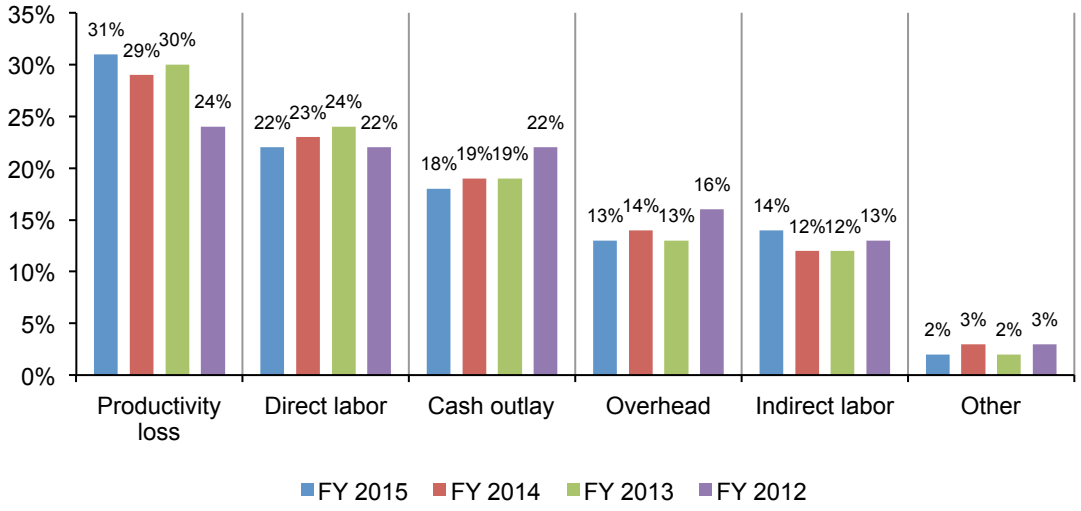
Companies spend the most on detection and recovery. Cyber crime detection and recovery activities have decreased and now account for 48 percent of total internal activity cost, as shown in Figure 14. This indicates better management and the use of security technologies to facilitate the recovery process. Containment and investigation costs have increased (25 percent and 15 percent, respectively) and indicate a cost-reduction opportunity for organisations that are able to use technologies to improve the ability to resolve the security incident.

Figure 14. Percentage cost by internal activity centre



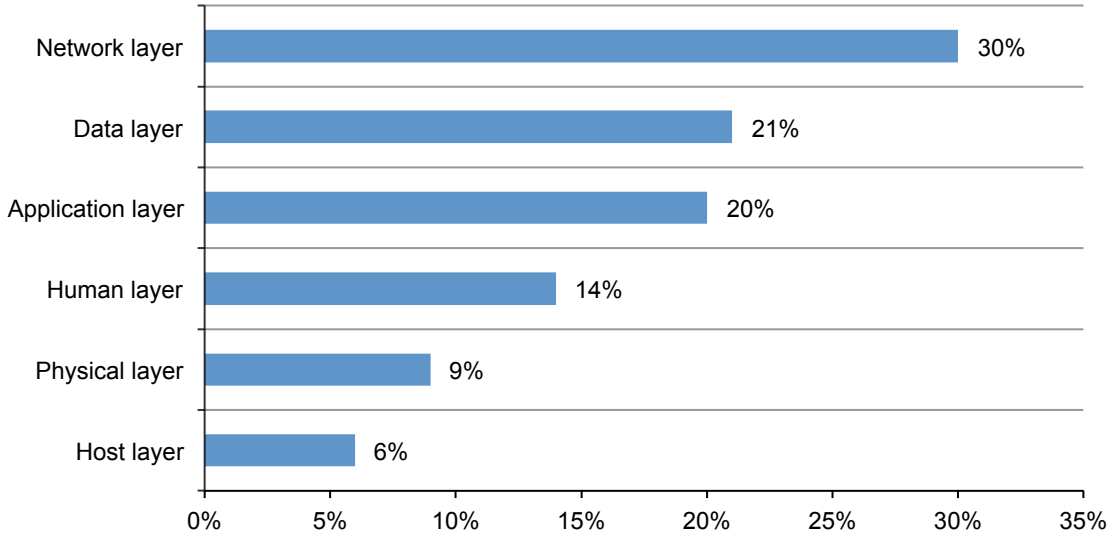
The percentage of annualised costs can be further broken down into specific expenditure components: productivity loss (31 percent), direct labour (22 percent), cash outlay (18 percent), overhead (13 percent) and indirect labour (14 percent). Costs not included in these components are represented in ”other”. As shown in Figure 15, these expenditures have remained stable since last year’s study.

Figure 15. Percentage activity cost by specific cost components



The largest portion of the security budget is allocated to the network layer. Figure 16 summarises six layers in a typical multi-layered IT security infrastructure for all benchmarked companies. Each bar reflects the percentage dedicated to spending for the presented layer. The network layer receives the highest allocation at 30 percent of total dedicated IT security funding. At only 6 percent, the host layer receives the lowest funding level.

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



Organisations deploying security intelligence technologies realise a lower annualised cost of cyber crime. Figure 17 shows the average amount of money saved when companies use SEIM in the six activities conducted to resolve the cyber attack. In total, 15 companies (53 percent) deploy security intelligence tools such as SIEM, IPS with reputation feeds, network intelligence systems, big data analytics and others. The largest cost differences in millions pertain to recovery ($.96 vs. $1.43) and incident management ($.33 vs. $.69).

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

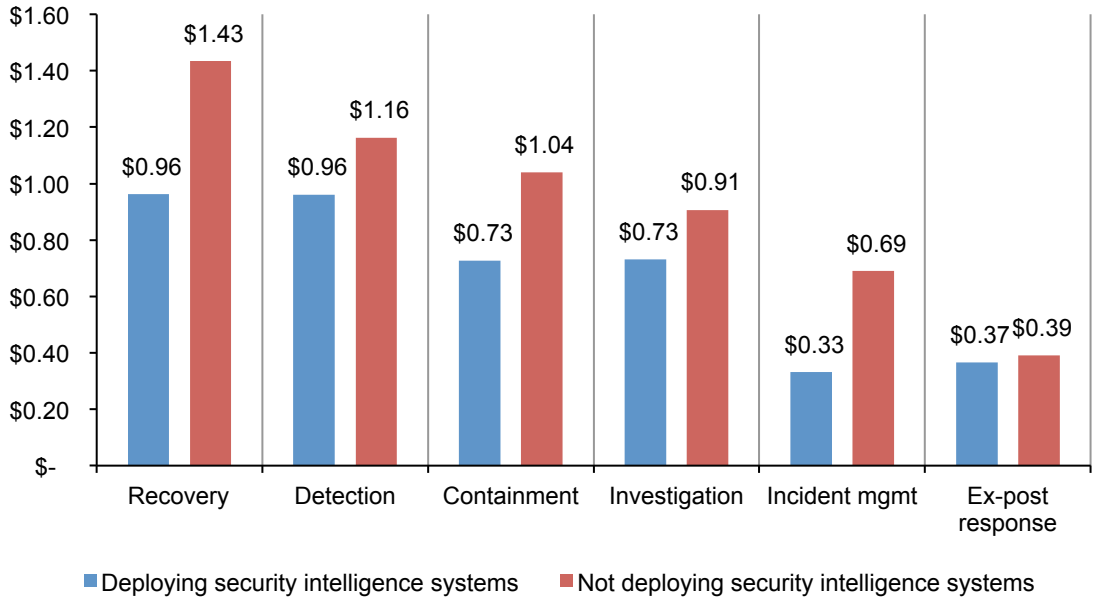


Figure 19 shows seven enabling security technology categories experienced by a subset of benchmarked companies. Each bar represents the percentage of companies fully deploying each given security technology. The top three technology categories include: access governance tools (64 percent), enterprise encryption technologies (57 percent) and security intelligence systems (50 percent).

Figure 18. Seven enabling security technologies deployed

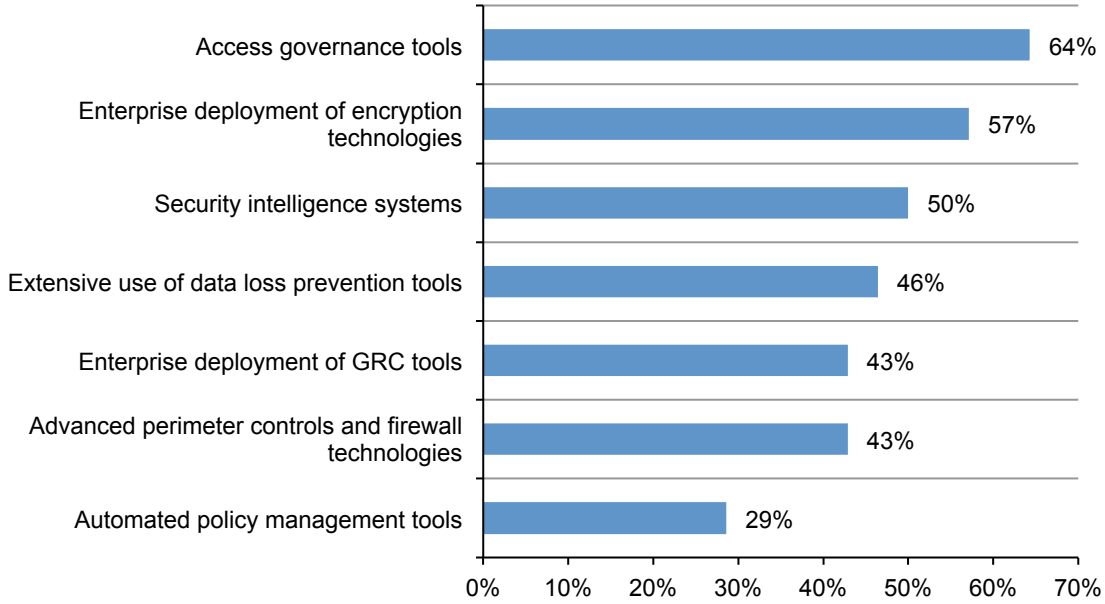
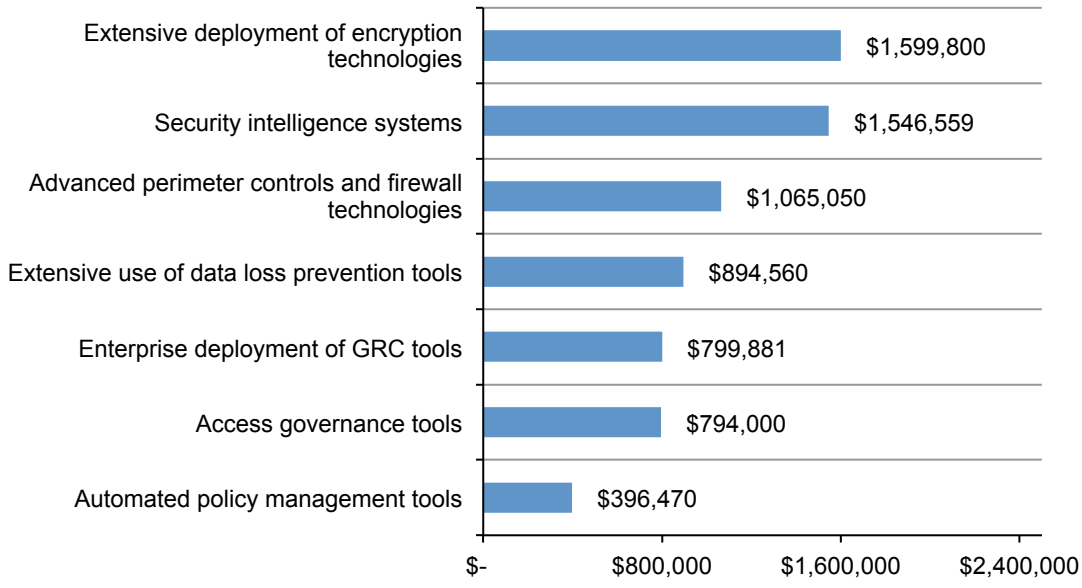


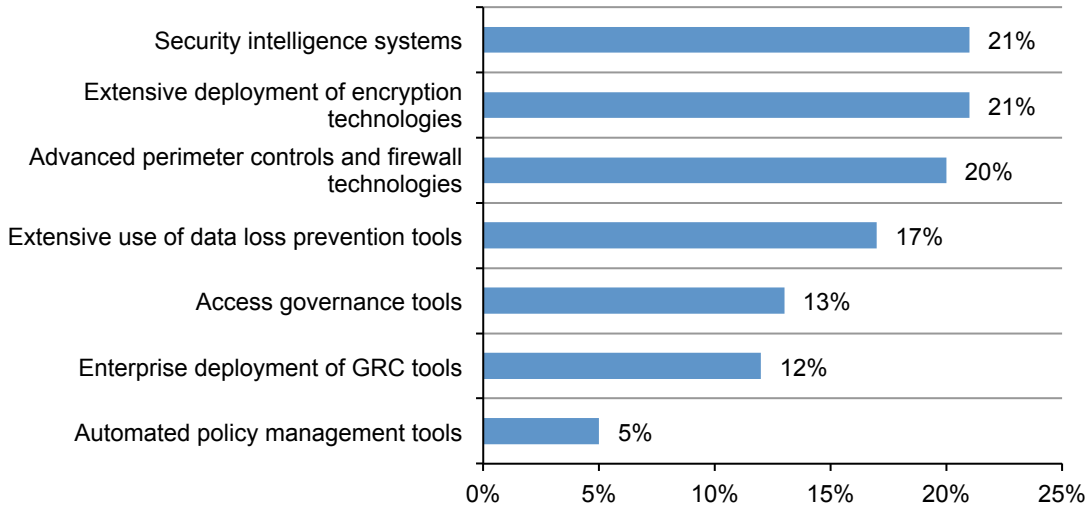
Figure 19 shows the money companies can save by deploying each one of seven enabling security technologies. For example, companies with encryption technologies experience cost savings of $1.6 million on average and those deploying security intelligence systems, on average, experience a substantial cost savings of $1.5 million. 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 technologies



Security intelligence systems have the biggest return on investment. Figure 20 summarises the estimated return on investment (ROI) realised by companies for each one of the seven categories of enabling security technologies indicated above.[10] At 21 percent, companies deploying security intelligence systems and extensive deployment of encryption technologies, on average, experienced a higher ROI than all other technology categories presented. The estimated average ROI for all seven categories of enabling security technologies is 16 percent.

Figure 20. Estimated ROI for seven categories of enabling security technologies



[10]The return on investment calculated for each security technology category is defined as: (1) gains from the investment divided by (2) cost of investment (minus any residual value). We estimate a three-year life for all technology categories presented. Hence, investments are simply amortised 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: employment of certified/expert security personnel (68 percent), appointment of a high-level security leader (64 percent) and formation of a senior-level security council (57 percent).

Figure 21. Seven enterprise security governance activities deployed

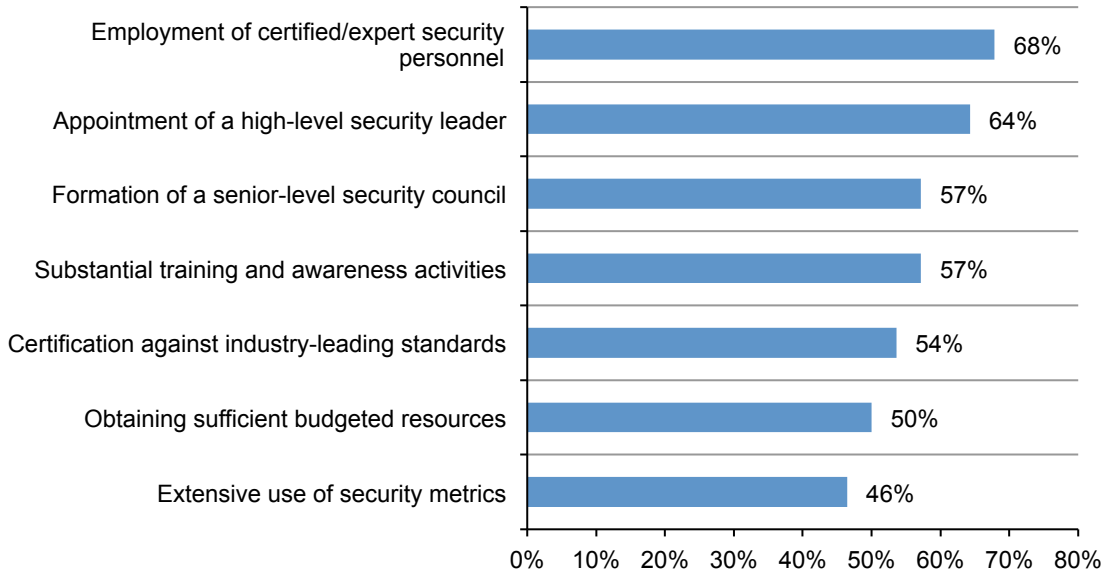
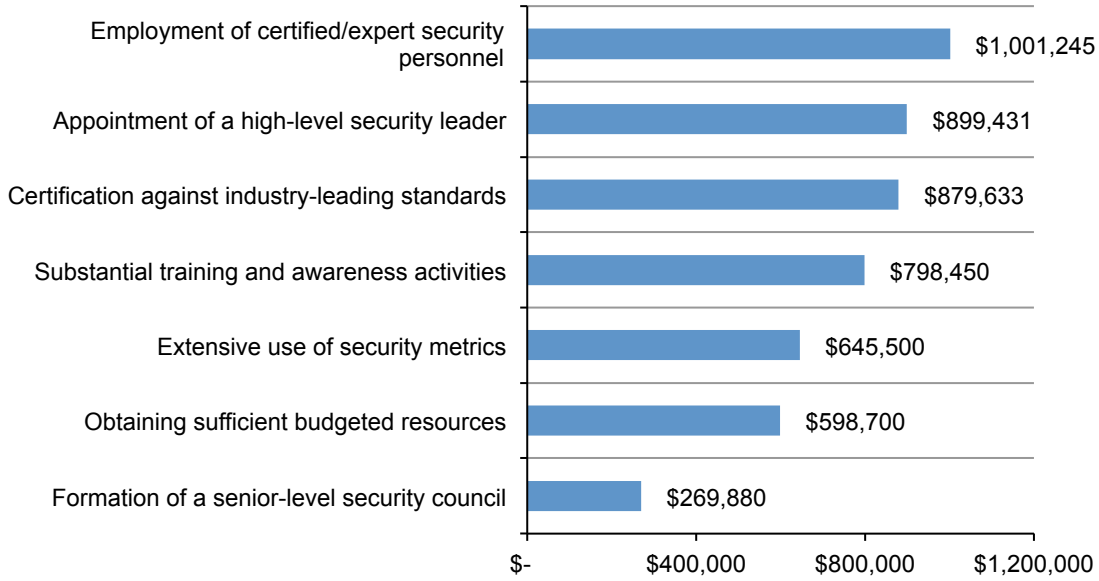


Figure 22 shows the incremental cost savings for each one of seven enterprise governance activities. As shown, companies with expert security personnel save an average of $1 million. Similar to security technology categories, cost savings resulting from improved governance activities are independent of each other and cannot be added together.

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



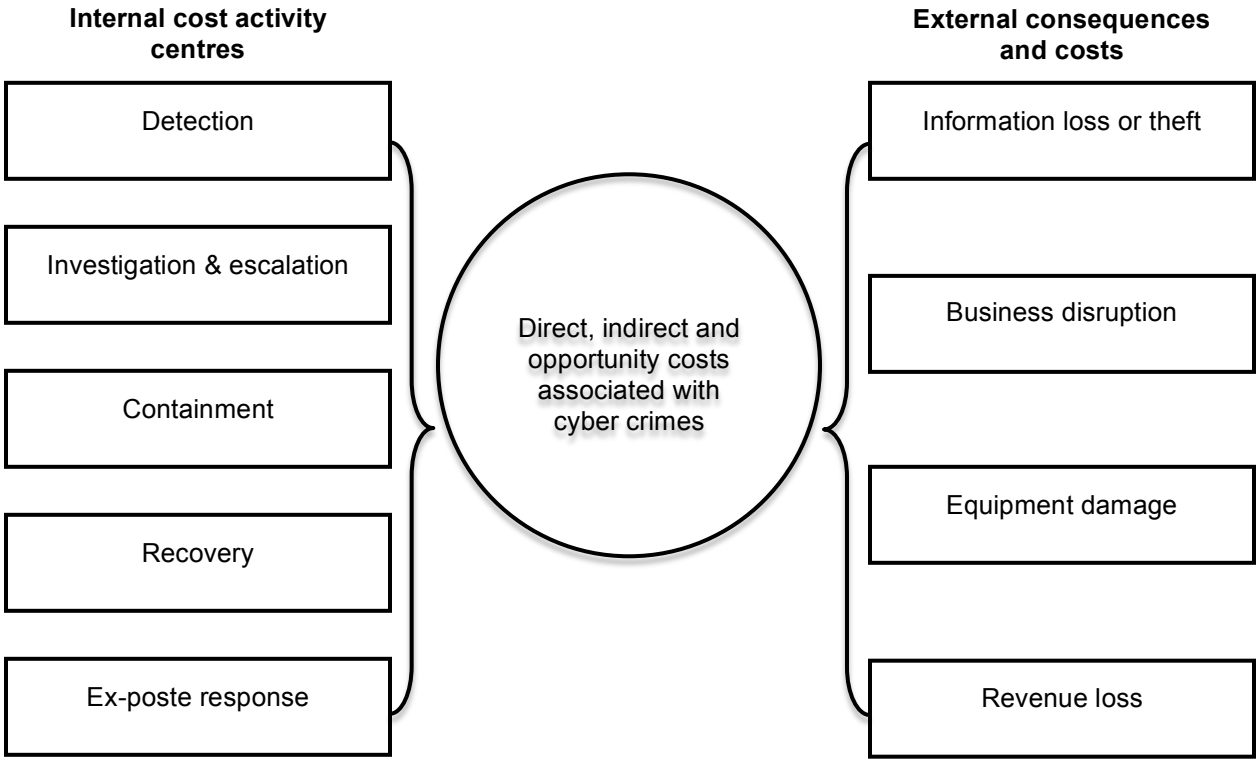
Part 3. Framework

The purpose of this research is to provide guidance on what a successful cyber attack can cost an organisation. 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 organisation 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 centres.
- 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 analyse the internal cost centres 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 centres 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 organisational 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 devices; malicious code (including SQL injection); and denial of services.[11]

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 centres in our framework include:[12]

- Detection: Activities that enable an organisation 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 organise 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 organisation's systems and core business processes. These include the restoration of damaged information assets and other IT (data centre) assets.
- Ex-post response: Activities to help the organisation minimise 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, organisations often experience external consequences or costs associated with the aftermath of successful attacks – which are defined as attacks that infiltrate the organisation'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.

[11] 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.

[12] Internal costs are extrapolated using labour (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 organisation 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 organisation.

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 organisation. Table 3 reports the frequency of individuals by their approximate functional discipline that participated in this year's Australian study. As can be seen, this year's study involved an average of 283 interviews for each benchmarked company.

Table 3. Functional areas of interview respondents	**FY2015**	**Pct%**
IT operations	46	16%
IT security	44	16%
Data center management	32	11%
Compliance	28	10%
Network operations	21	7%
Legal	14	5%
Internal or IT audit	12	4%
Accounting & finance	20	7%
IT risk management	13	5%
Enterprise risk management	8	3%
Physical security/facilities mgmt	10	4%
Application development	9	3%
Human resources	8	3%
Quality assurance	6	2%
Industrial control systems	5	2%
Procurement/vendor mgmt	7	2%
Total	283	100%
Interviews per company on average	9.43	

Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant. Within each category, cost estimation was a two-stage process. First, the benchmark instrument required individuals to rate direct cost estimates for each cost category by marking a range variable defined in the following number line format.

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, labour 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 organisation 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.

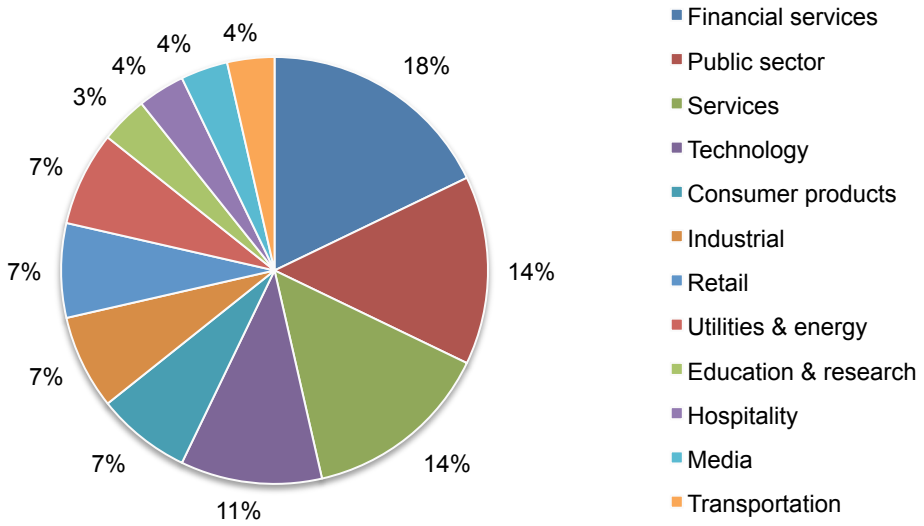
Field research was conducted over several months concluding in August 2015. To maintain consistency for all benchmark companies, information was collected about the organisations' cyber crime experience was limited to four consecutive weeks. This time frame was not necessarily the same time period as other organisations in this study. The extrapolated direct, indirect and opportunity costs of cyber crime were annualised 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 personalised letter and a follow-up phone call to 117 Australian-based organisations for possible participation and[13] 28 organisations permitted Ponemon Institute to perform the benchmark analysis.

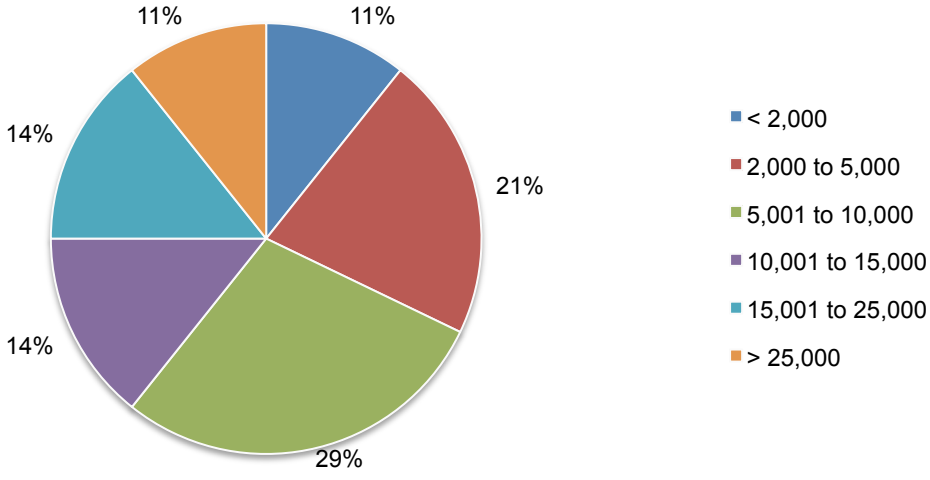
Pie Chart 1 summarises the current (FY 2015) sample of participating companies based on 12 primary industry classifications. As can be seen, financial services (18 percent) represent the largest segment. This includes retail banking, insurance, brokerage and credit card companies. The second largest segments are public sector and services (both at 14 percent).

Pie Chart 1. Industry sectors of participating organisations



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 organisations with a minimum of 890 seats. The largest enterprise has 39,554 seats.

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



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

Part 6. Limitations & Conclusions

This study utilises 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 organisations, all Australian-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 organisations, all believed to have experienced one or more cyber attacks. Twenty-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 organisational 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 organisations.

As a member of the **Council of American Survey Research Organisations (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.