



2013 Cost of Cyber Crime Study: Germany

Sponsored by HP Enterprise Security

Independently conducted by Ponemon Institute^{LLC}

Publication Date: October 2013

2013 Cost of Cyber Crime Study: Germany

Benchmark Study of German Companies
Ponemon Institute October 2013

Part 1. Executive Summary

We are pleased to present the *2013 Cost of Cyber Crime Study: Germany*, which is the second annual study of German companies. Sponsored by HP Enterprise Security, this year's study is based on a representative sample of 47 organizations in various industry sectors. While our research focused on organizations located in Germany, a majority are multinational corporations.

For the fourth year, Ponemon Institute conducted the cyber crime cost study in the United States. This is the second year for the United Kingdom, Australia and Japan benchmark studies. In addition, we conducted a study of French companies for the first time. The findings from this research are presented in separate reports.

German Study at a Glance

47 German companies
398 interviews with DE company personnel
236 attacks used to measure total cost
€5.67 million is the average annualized cost
16% net increase in cost over the past year
16% average ROI for seven security technologies

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. Consistent with the previous study, the loss or misuse of information assets is the most significant consequence of a cyber attack. Based on these findings, organizations need to be more vigilant in protecting their most sensitive and confidential information.

Key takeaways from this research include:

- Cyber crimes continue to be costly. We found that the average annualized cost of cyber crime for 47 organizations in our study is €5.67 million per year, with a range of €380,216 to €27.7 million. In 2012, the average annualized cost was €4.8 million. This represents an increase in cost of 16 percent or €830,169 from the results of our cyber cost study published last year.¹
- Cyber attacks have become common occurrences. The companies in our study experienced 59 successful attacks per week and 1.3 successful attacks per company per week.² This represents an increase of 21 percent from last year's successful attack experience. Last year's study reported 48 successful attacks on average per week.
- The most costly cyber crimes are those caused by malicious insiders, denial of service and phishing attacks. Mitigation of such attacks requires enabling technologies such as SIEM, intrusion prevention systems, application security testing and enterprise governance, risk management and compliance (GRC) solutions.

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.

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

¹See the *2012 Cost of Cyber Crime Study: Germany*, Ponemon Institute, October 2012.

²In 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 a plethora of attacks that are stopped by the company's firewall defenses.

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 10 months of effort was required to recruit companies, build an activity-based cost model, collect source information and complete the analysis.

This research culminated with the completion of case studies involving 47 organizations. For consistency purposes, our benchmark sample consists of only larger-sized organizations (i.e., more than 500 enterprise seats³). 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, incident response, containment, recovery and after-the-fact or “ex-post” response.

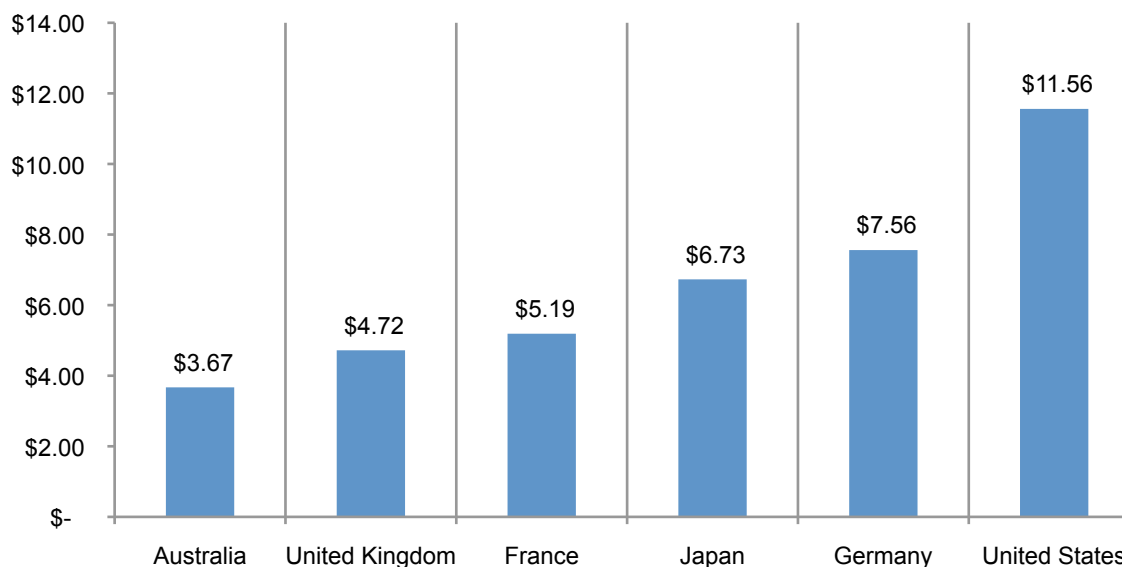
Global at a glance

This year’s annual study was conducted in the United States, United Kingdom, Germany, Australia, Japan and France with a total benchmark sample of 234 organizations. These global results are presented in a separate report entitled, *2013 Cost of Cyber Crime: Global Report*.

Figure 1 presents the estimated average cost of cyber crime for six country samples involving 234 separate companies. 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 \$11.56 million and the Australian sample reports the lowest total average cost at \$3.67 million.

Figure 1. Total cost of cyber crime in six countries

Cost expressed in US dollars \$1,000,000 omitted
n = 234 separate companies



Possible reasons for these differences may be the types and frequencies of attacks experienced as well as the importance that each company places on the theft of information assets versus other consequences of the incident.

³ Enterprise seats refer to the number of direct connections to the network and enterprise systems.

We found that US companies are much more likely to experience the most expensive types of cyber attacks, which are malicious code, denial of service and web-based incidents. Similarly, Australia is most likely to experience denial of service attacks. In contrast, German companies are least likely to experience malicious code and botnets. Japanese companies are least likely to experience stolen devices and malicious code attacks.

Another key finding that may explain cost differences among countries concerns the theft of information assets. US, Japanese and German companies report this as the most significant consequence of a cyber attack. On the other hand, UK, France and Australia cite business disruption as more important.

The analysis of internal activity costs provides interesting differences. The description of this cost is provided in Part 3 of this report. Specifically, the cost of detecting and recovering from a cyber attack appears to be the most expensive for US, French, Japanese and German companies. However, the cost of recovery from a cyber incident is also expensive for companies in the UK Australia. It is interesting to note that Japanese companies attach higher costs to investigate and manage the incident than other countries.

Summary of German findings

Following are the most salient findings for a sample of 47 German-based organizations requiring 398 separate interviews to gather cyber crime cost results. In several places in this report, we compare the present findings to our 2012 study.⁴

Cyber crimes continue to be very costly for organizations. We found that the mean annualized cost for 47 benchmarked organizations is €5.67 million per year, with a range from €380,216 to €27.7 million each year per company. Last year's mean cost per benchmarked organization was €4.84 million. Thus, we observe a €830,169 increase in mean value.

Cyber crime cost varies by organizational size. Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost.⁵ However, based on enterprise seats, we determined that small organizations incur a significantly higher per capita cost than larger organizations (€974 versus €251).

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

The most costly cyber crimes are those caused by malicious services, denial of services, and phishing attacks. These account for 50 percent of all cyber crime costs per organization 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 organizational cost. Please note that resolution does not necessarily mean that the attack has been completely stopped. For example, some attacks remain dormant and undetected (i.e., modern day attacks). The average time to resolve a cyber attack was 22 days, with an average cost to participating organizations of €352,457 during this

⁴Observed differences in median or average value do not reflect a trend since it is calculated from a matched sample of companies each year.

⁵In this study, we define an enterprise seat as one end-user identity/device connected to the company's core networks or enterprise systems.

⁶This year the category malicious insider includes the cost of stolen devices.

22-day period. This represents a 18 percent increase from last year's estimated average cost of €294,829, which was also based upon a 22-day resolution period. Results show that malicious insider attacks can take more than 46 days on average to contain.

Information theft continues to represent the highest external cost, followed by the costs associated with business disruption.⁷ On an annualized basis, information theft accounts for 43 percent of total external costs (up 3 percent from 2012). Costs associated with disruption to business or lost productivity account for 27 percent of external costs (up 2 percent from 2012).

Recovery and detection are the most costly internal activities. On an annualized basis, recovery and detection combined account for 51 percent of the total internal activity cost with productivity loss and direct labor representing the majority of these costs.

Activities relating to IT security in the network layer receive the highest budget allocation. In contrast, the host layer receives the lowest funding level. The percentage allocation to physical layer activities is highest for critical infrastructure companies such as communications, energy and utilities and lowest for retail companies.

Deployment of security intelligence systems makes a difference. The cost of cyber crime is moderated by the use of security intelligence systems (including SIEM). Findings suggest companies using security intelligence technologies were more efficient in detecting and containing cyber attacks. As a result, these companies enjoyed an average cost savings of approximately €1.4 million when compared to companies not deploying security intelligence technologies.

A strong security posture moderates the cost of cyber attacks. We utilize Ponemon Institute's proprietary metric called the Security Effectiveness Score (SES) Index to define an organization's ability to achieve reasonable security objectives.⁸ The higher the SES, the more effective the organization is in achieving its security objectives. The average cost to mitigate a cyber attack for organizations with a high SES is substantially lower than organizations with a low SES score.

Companies deploying encryption technologies experienced a substantially higher ROI at 25 percent than all other technology categories presented. Also significant are the estimated ROI results for companies that extensively deploy security intelligence systems (20 percent) and advanced perimeter controls such as UTM, NGFW, IPS with reputation feeds and more (19 percent).

Deployment of enterprise security governance practices moderates the cost of cyber crime. Findings show companies that certify against leading standards, employ certified or expert staff and appoint a high-level security leader have cyber crime costs that are lower than companies that have not implemented these practices. This so-called "cost savings" for companies deploying good security governance practices is estimated at more than €471,927 on average.

⁷In 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.

⁸The 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

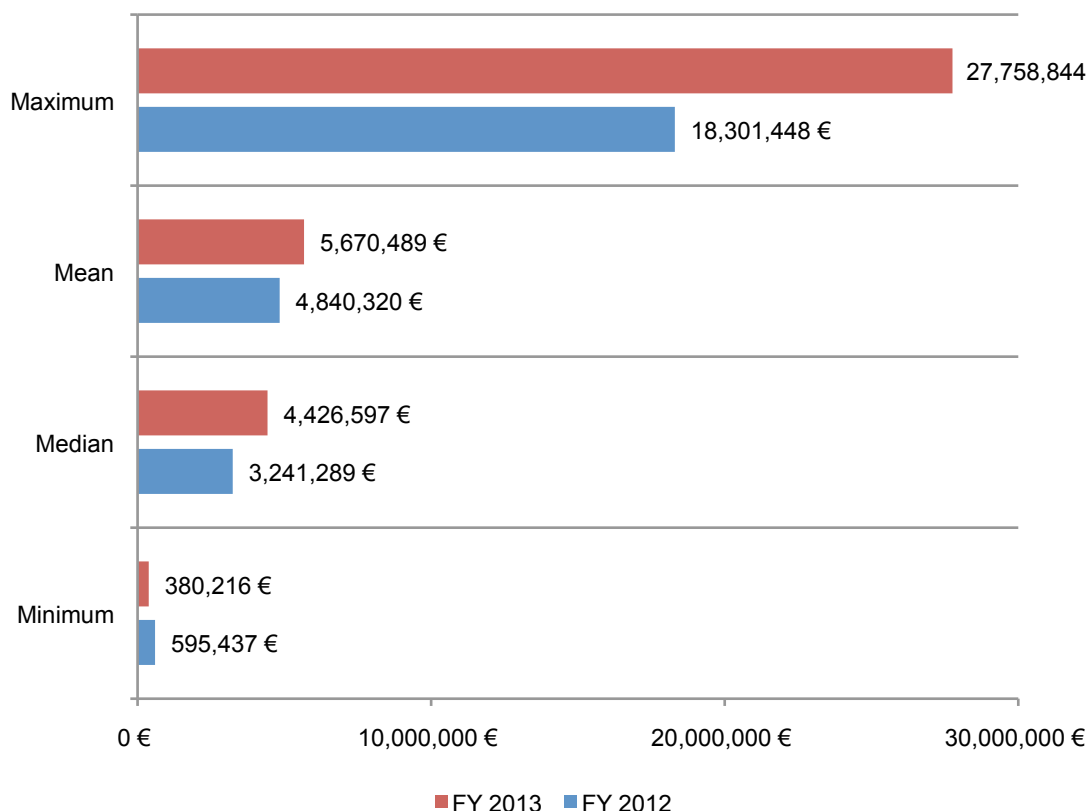
Ponemon Institute's *2013 Cost of Cyber Crime Study: Germany* examines the total costs organizations incur when responding to cyber crime incidents and include the following: detection, recovery, investigation and incident management, ex-post response and cost containment. These costs do not include a plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

Cyber crimes continue to be costly for participating organizations

The economic impact of a cyber attack is wide-ranging and influenced by a variety of factors as discussed in this report. The total annualized cost of cyber crime for the 2013 benchmark sample of 47 organizations ranges from a low of €380,216 to a high of €27.7 million. Participating companies were asked to report what they spent and their in-house cost activities relating to 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 present an extrapolated annualized cost.⁹

Figure 2 shows the median annualized cost of cyber crime in the study benchmark sample is €4.4 million – an increase from last year's median value of €3.2. The mean value is €5.67 million. This is an increase of €830,169 or a 16 percent from last year's mean of €4.84 million.

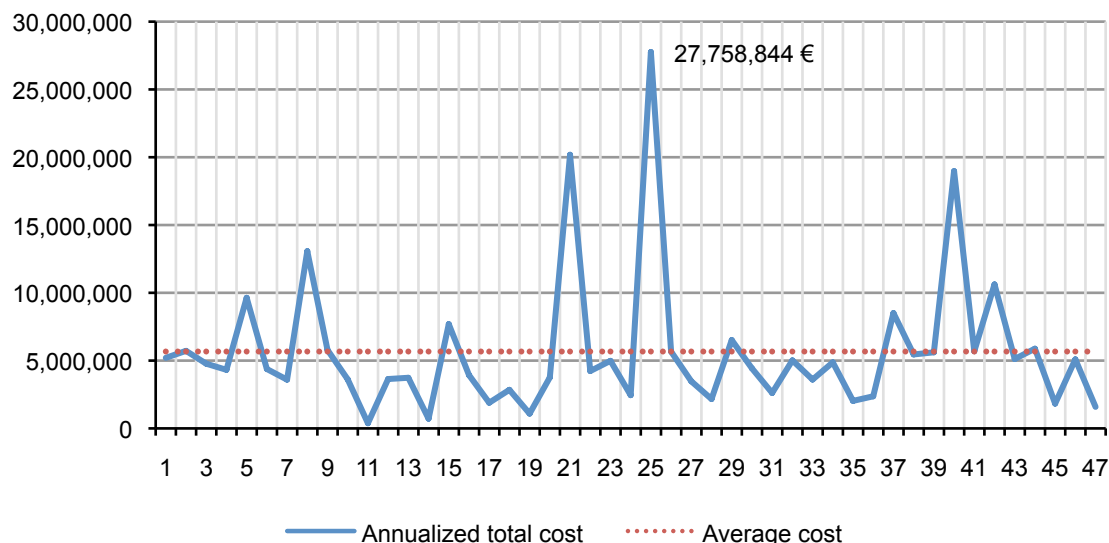
Figure 2. The cost of cyber crime



⁹Following is the gross-up statistic: Annualized revenue = [cost estimate]/[4/52 weeks].

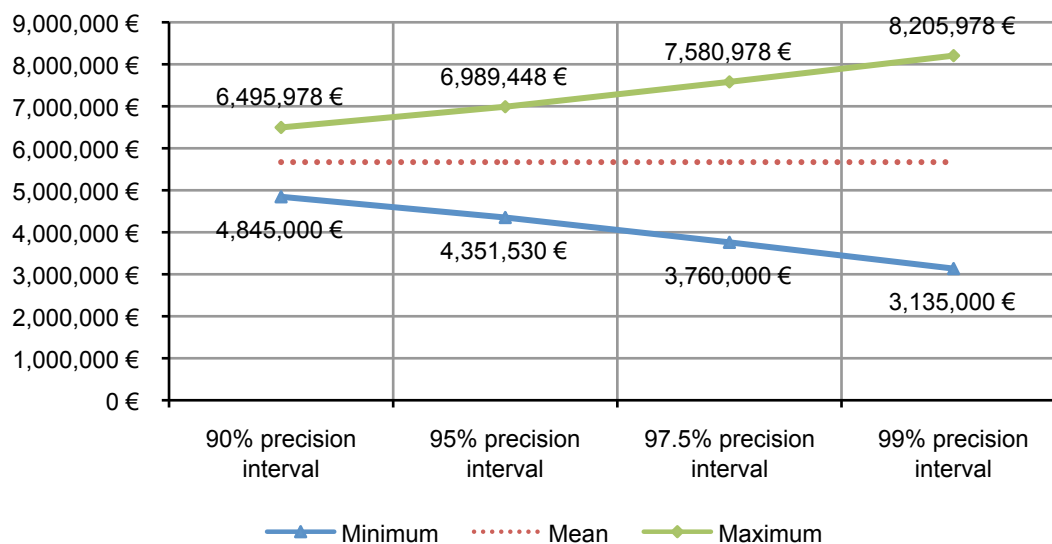
Figure 3 reports the distribution of annualized total cost for 47 companies. As can be seen, 34 companies in our sample incurred total costs below the mean value of €5.67 million, thus indicating a skewed distribution. The highest cost estimate of €27.7 million was determined not to be an outlier based on additional analysis. Thirteen other organizations experienced an annualized total cost of cyber crime above the mean.

Figure 3. Annualized total cost of cyber crime for 47 participating companies



As part of our analysis, we calculated a precision interval for the average cost of €5.67 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.

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

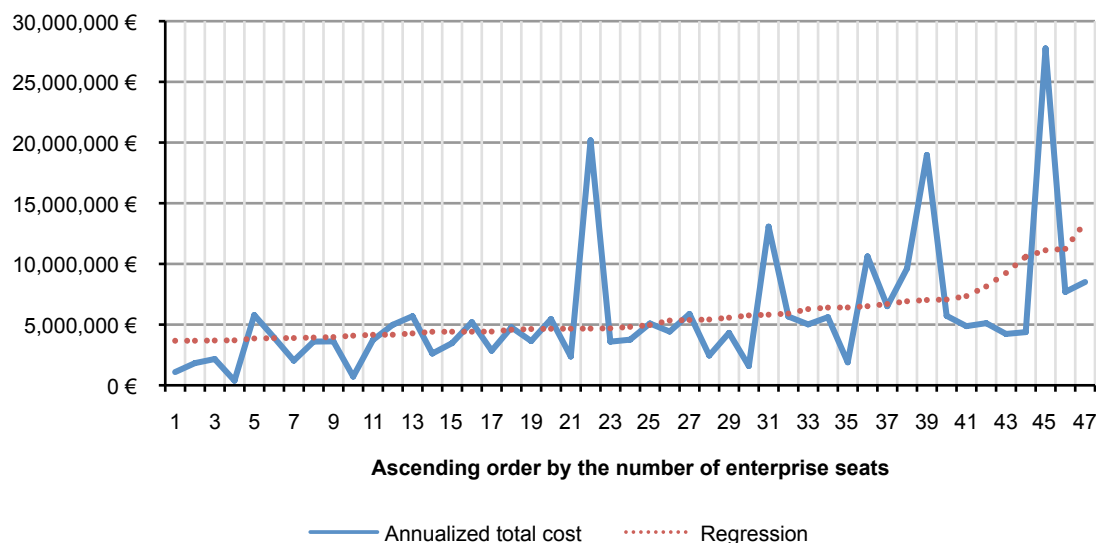


The cost of cyber crime varies by organizational size

As shown in Figure 5, organizational size, as measured by the number of enterprise seats or nodes, is positively correlated to annualized cyber crime cost. This positive correlation is indicated by the upward sloping regression line.

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

Regression performed on enterprise seats ranging from 1,007 to 40,212



The following tables show that organizational size can influence the cost of cyber crime.

Organizations are placed into one of four quartiles based on their total number of enterprise seats (which we use as a size surrogate). We do this to create a more precise understanding of the relationship between organizational size and the cost of cyber crime. Table 1 shows the quartile average cost of cyber crime for two years.

Table 1: Quartile analysis	FY 2012 (n=43)	FY 2013 (n=47)
Quartile 1	2,290,658 €	2,822,186 €
Quartile 2	3,479,637 €	5,300,046 €
Quartile 3	4,545,193 €	5,469,831 €
Quartile 4	8,814,005 €	9,400,748 €

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 the prior year, the 2013 average per capita cost is inversely related to organizational size.

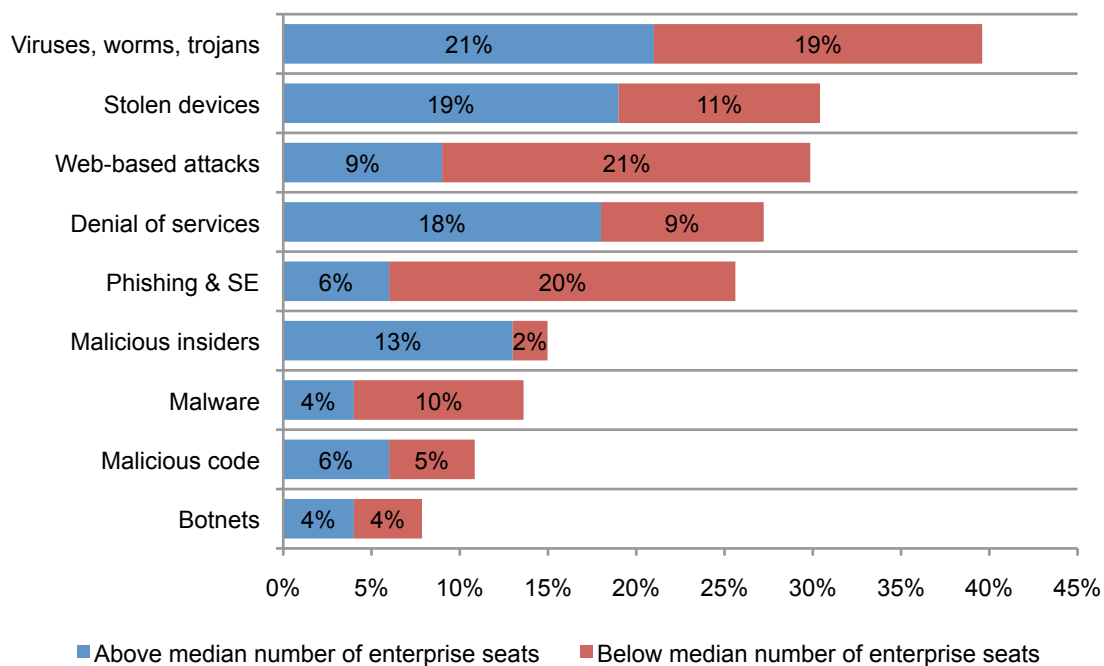
Table 2. Quartile analysis	2012 cost per seat	2013 cost per seat
Quartile 1 (smallest)	1,484 €	974 €
Quartile 2	1,160 €	567 €
Quartile 3	568 €	367 €
Quartile 4 (largest)	420 €	251 €

In Figure 6, we compare smaller and larger-sized organizations split by the sample median of 5,612 seats. This reveals that the cost mix for specific cyber attacks varies by organizational size.

Smaller organizations (below the median) experience a higher proportion of cyber crime costs relating to web-based attacks, phishing, and malware. In contrast, larger organizations (above the median) experience a higher proportion of costs relating to viruses, worms and trojans, stolen devices, denial of services and malicious insiders.¹⁰

Figure 6. The cost mix of attacks by organizational size

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



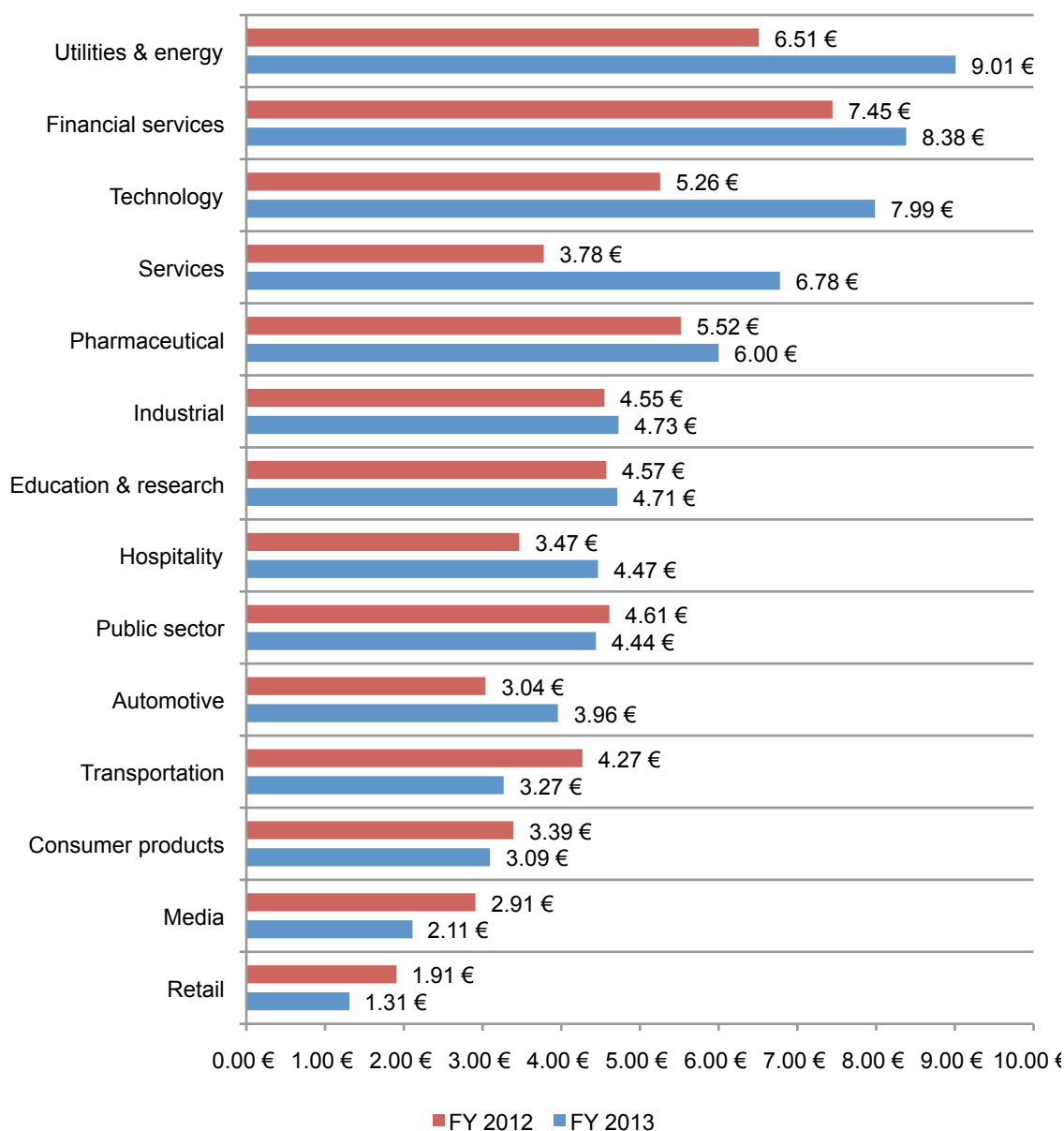
¹⁰In the context of this study, malicious insiders include employees, temporary employees, contractors and, possibly, other business partners.

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 results from the past three years. As seen in Figure 7, utilities and energy, financial services and technology companies experience substantially higher costs in all two annual studies. Organizations in retail, media and consumer products appear to have a lower overall cyber crime cost over two years.¹¹

Figure 7. Average annualized cost by industry sector

1,000,000 € omitted



¹¹This analysis is for illustration purposes only. The sample sizes over two years make it difficult to draw definitive conclusions about industry segment differences.

Cyber crimes are intrusive and common occurrences

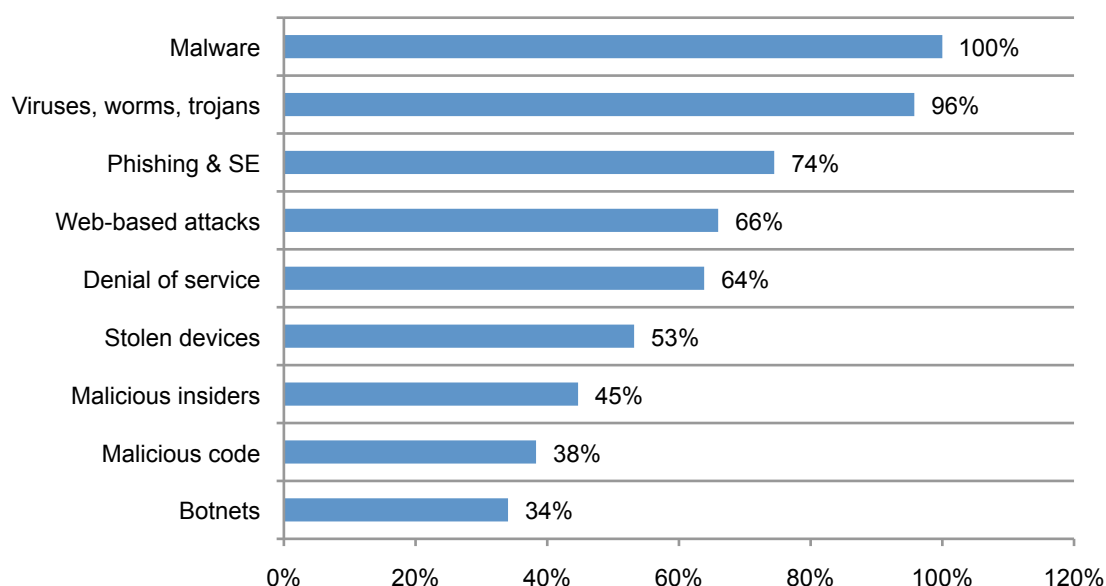
In this year's study, the benchmark sample of 47 organizations experienced 59 discernible cyber attacks per week, which translates to 1.3 successful attacks per benchmarked organization each week. Last year, there were 48 attacks in 43 organizations.

Figure 8 summarizes in percentages the types of attack methods experienced by participating companies. Virtually all organizations had attacks relating to malware.¹² The frequency of these cyber attacks is followed by viruses, worms and/or trojans (96 percent) over the four-week benchmark period.

Seventy-four percent experienced phishing and social engineering attacks. Web-based attacks affected 66 percent of companies. Other high frequency attacks include denial of service and stolen devices (64 percent and 53 percent, respectively).

Figure 8. Types of cyber attacks experienced by 47 benchmarked companies

The percentage frequency defines a type of attack categories experienced

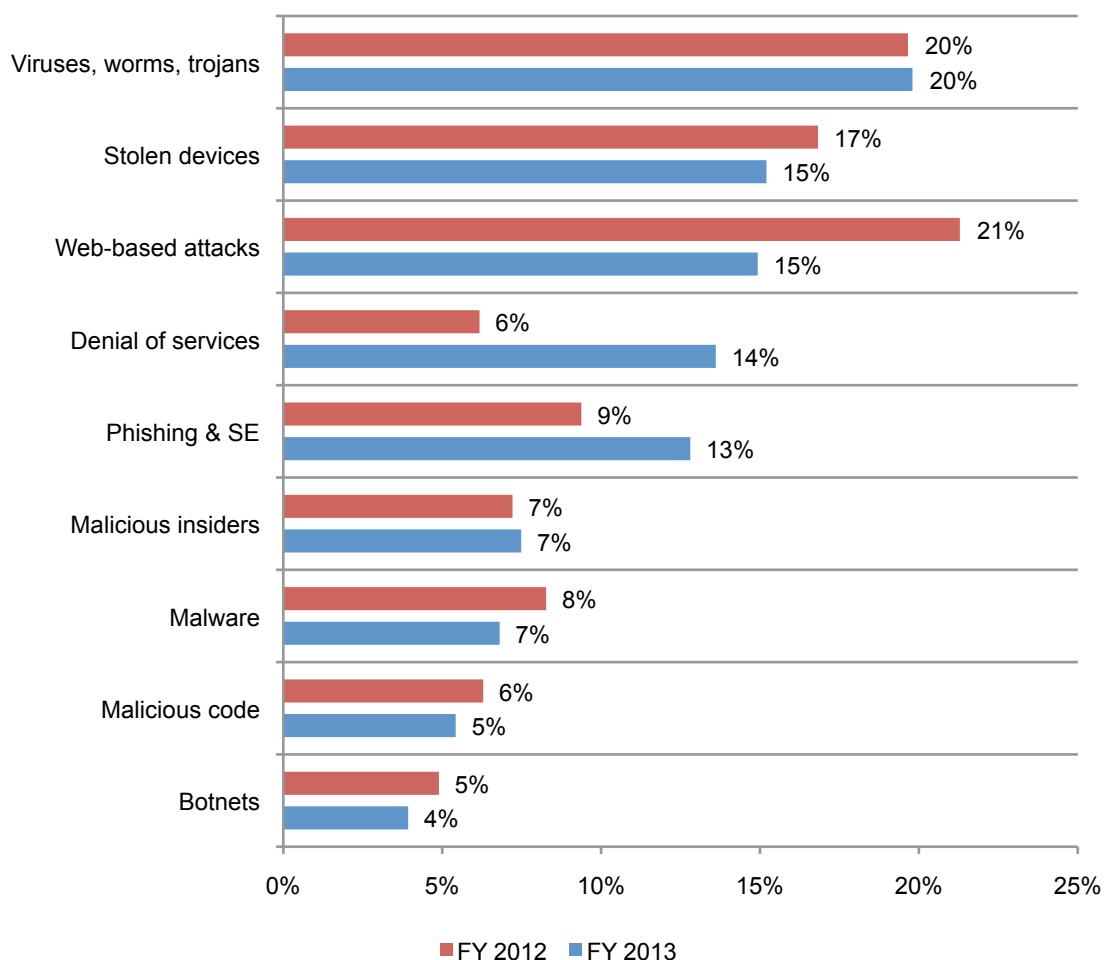


¹²Malware attacks and malicious code attacks are inextricably linked. We classified malware attacks that successfully infiltrated the organizations' networks or enterprise systems as a malicious code attack.

Costs vary considerably by the type of cyber attack

Figure 9 compares our benchmark results over two years, showing the percentage of annualized cost of cyber crime allocated to nine attack types compiled from all benchmarked organizations. In total, the top three attacks account for more than 50 percent of the total annualized cost cyber crime experienced by 47 companies. Viruses, worms and trojans and stolen devices account for the two highest percentage cyber cost types. The least costly are botnets, malicious code and trojans and malware.

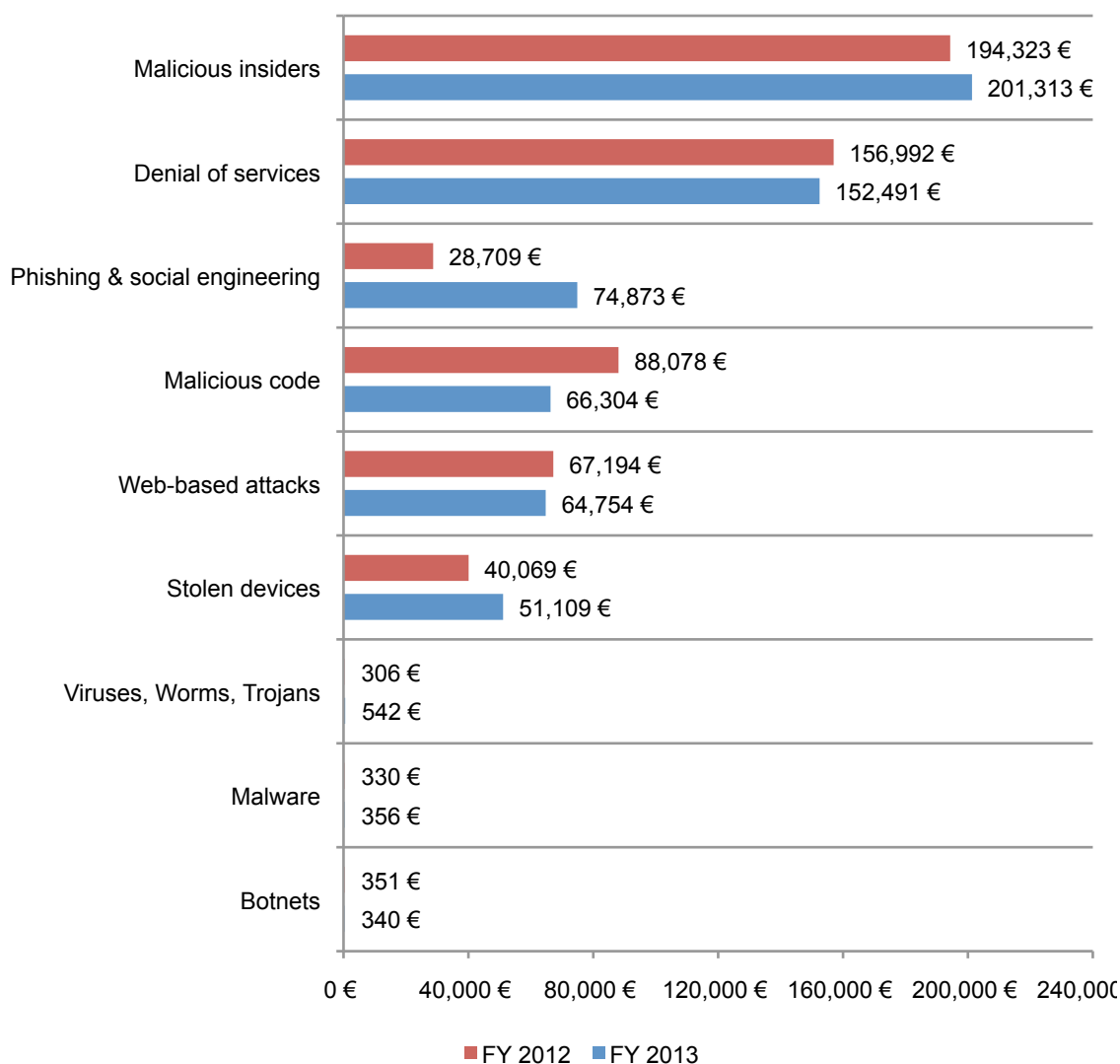
Figure 9. Percentage annualized cyber crime cost by attack type



While Figure 9 shows the average percentage of cost according to attack type, Figure 10 reveals the most to least expensive cyber attacks when analyzed on the frequency of incidents. The most expensive attacks are malicious insiders, denial of services, and phishing attacks.

Another interesting finding is the significant cost increase for the attack category termed phishing and social engineering which rose by more than €46,164. Malicious insiders rose slightly (€6,990). In the context of our study, malicious insiders include employees, temporary employees, contractors and, possibly, business partners.

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



Time to resolve or contain cyber crimes increases the cost

The mean number of days to resolve cyber attacks is 22 with an average cost of €15,928 per day – or a total cost of €352,457 over the 22-day remediation period. This represents a 21 percent increase from last year's cost estimate of €294,829. The time range to resolve attacks is from less than 1 day to over 76 days. Resolution does not necessarily mean that the attack has been completely stopped. For example, some attacks remain dormant and undetected (i.e., modern day attacks).

Figure 11 shows the annualized cost of cyber crime in ascending order by the average number of days to resolve attacks. The regression line shows an upward slope, which suggests cost and time variables are positively related.

Figure 11. Average days to resolve attack in ascending order

Estimated average time is measured for each given organization in days

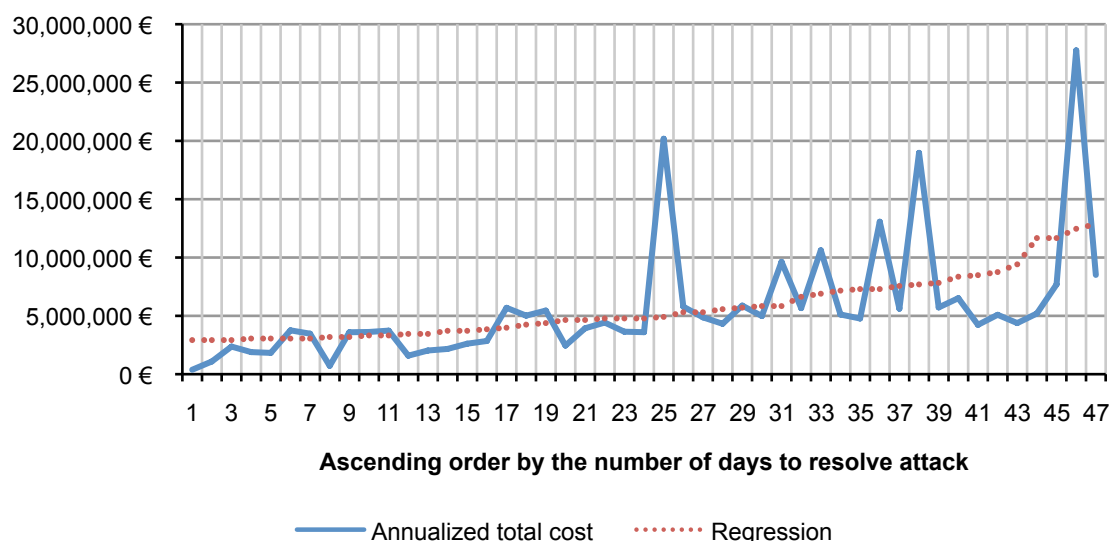
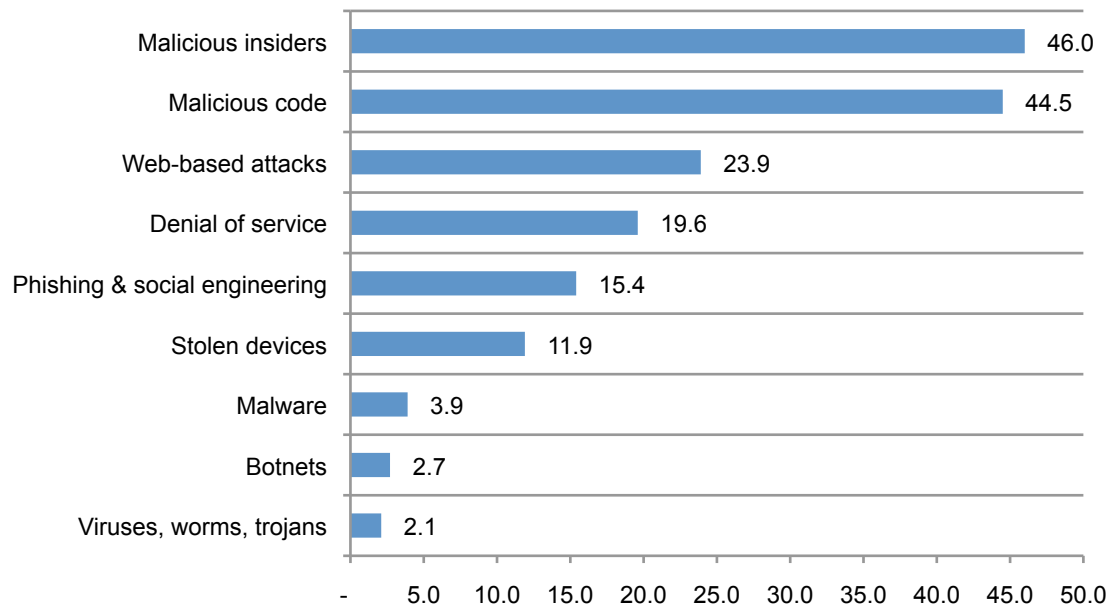


Figure 12 reports the average days to resolve cyber attacks for nine different attack types studied in this report. It is clear from this chart that it takes the most amount of time, on average, to resolve attacks from malicious insiders and malicious code.

Figure 12. Average days to resolve attack

Estimated average time is measured for each attack type in days



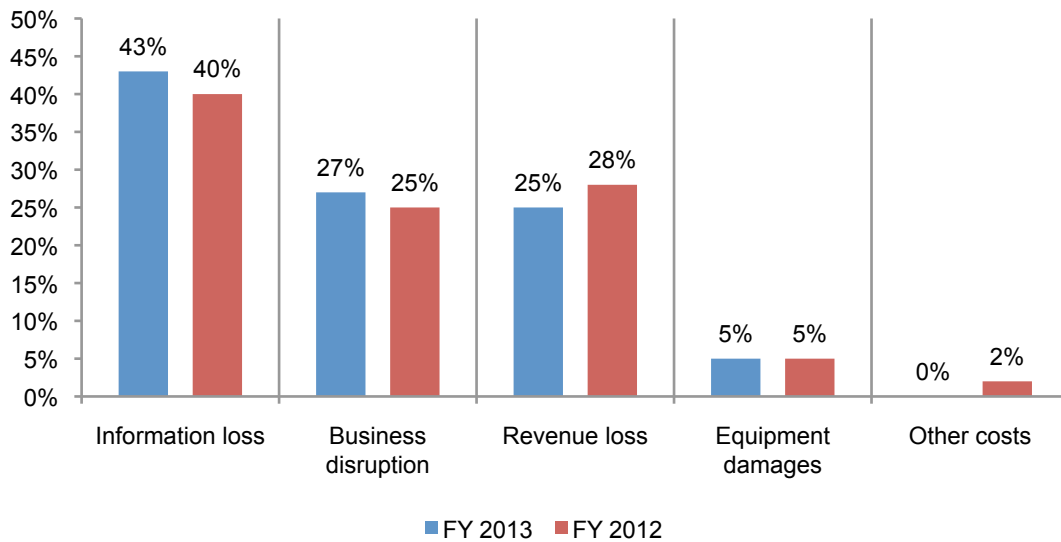
Information theft remains the highest external cost

As shown in Figure 13, at the top end of the external cyber crime cost spectrum is information loss. On an annualized basis, information loss accounts for 43 percent of total external costs, which is a slight increase of three percent from our FY 2012 study.

In contrast, business disruption or loss of productivity accounts for 27 percent of total external costs, an increase of 2 percent from FY 2012. Revenue losses (25 percent) follow and equipment damages (5 percent) yield a much lower cost impact. Costs associated with revenue loss have declined.

Figure 13. Percentage cost for external consequences

Other cost includes direct and indirect costs that could not be allocated to a main external cost category

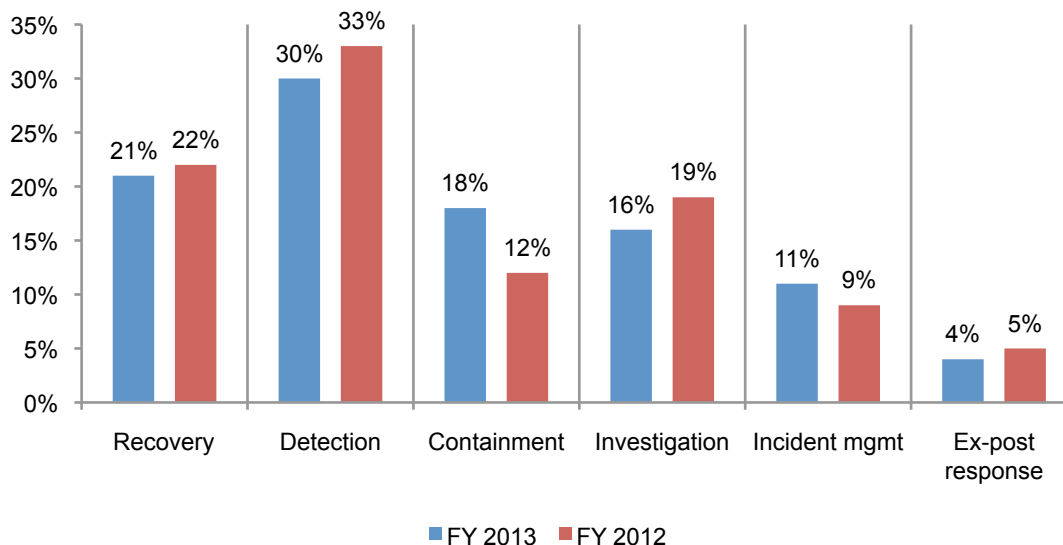


Detection and recovery are the most costly internal activities

Cyber crime recovery and detection activities account for 51 percent of total internal activity cost (a slight decrease from 55 percent in FY 2012), as shown in Figure 14. This is followed by containment and investigation costs (18 percent and 16 percent, respectively). Incident response ex-post response costs are lower at 11 and 4 percent, respectively. These results highlight a significant cost-reduction opportunity for organizations that are able to systematically manage recovery and to deploy enabling security technologies to help facilitate the detection process.

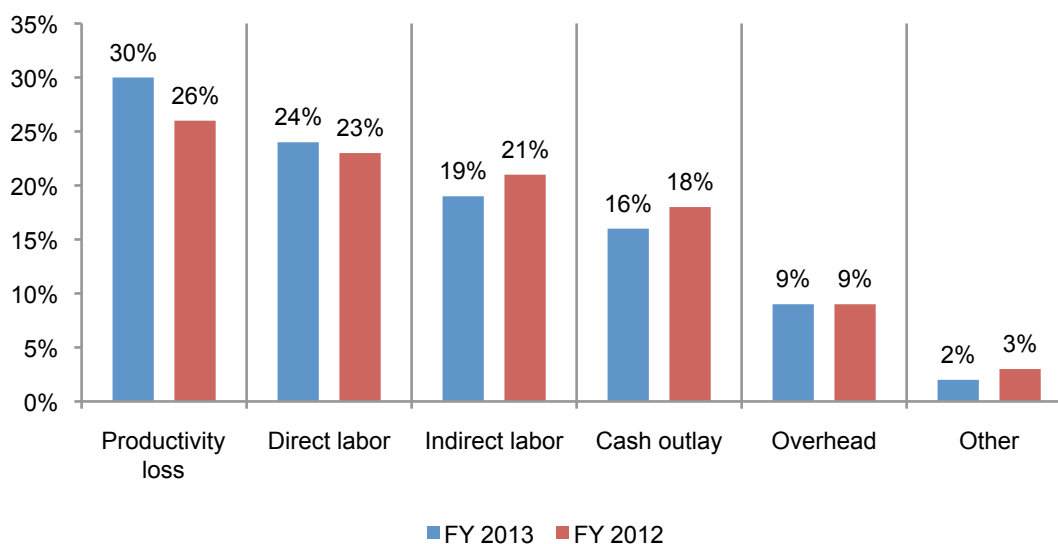
Figure 14. Percentage cost by internal activity center

Investigation includes escalation activities



The percentage of annualized costs can be further broken down into five specific expenditure components, which include: productivity losses (30 percent), direct labor (24 percent), indirect labor (19 percent), cash outlays (16 percent) and overhead (9 percent). As shown in Figure 15, the distribution of indirect labor and cash outlays decreased slightly. In contrast, productivity losses and direct labor increased slightly.

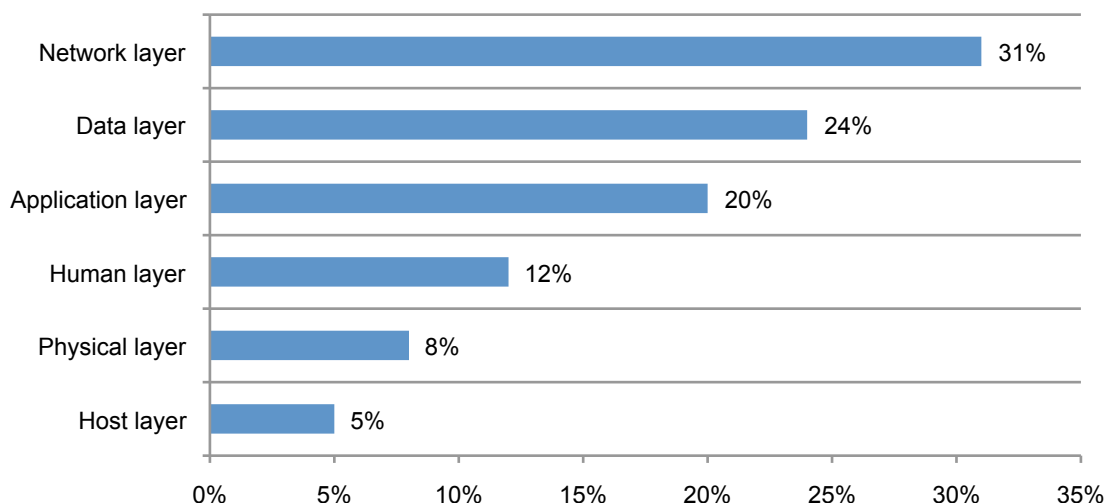
Figure 15. Percentage activity cost by six specific cost components



Cyber security budget allocation

Figure 16 summarizes six layers in a typical multi-layered IT security infrastructure for all benchmarked companies. Each bar reflects the percentage dedicated spending according to the presented layer. The network layer receives the highest allocation at 31 percent of total dedicated IT security funding. At only five percent, the host layer receives the lowest funding level. The percentage allocation to physical layer activities is highest for critical infrastructure companies such as communications, energy and utilities and lowest for retail, hospitality and consumer product companies.

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



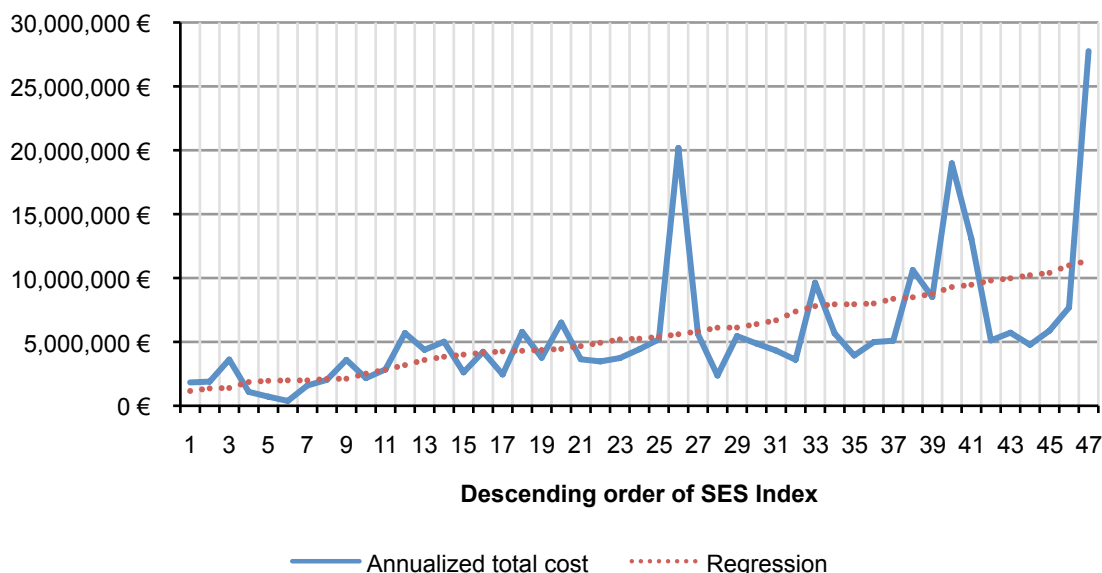
The organization's security posture influences the cost of cyber crime

We measure the security posture of participating organizations as part of the benchmarking process. Figure 17 reports the annualized cost and regression of companies in descending order of their security effectiveness as measured by the SES (see footnote 3).

The figure shows an upward sloping regression, suggesting that companies with a stronger security posture experience a lower overall cost. The SES range of possible scores is +2 (most favorable) to -2 (least favorable). Compiled results for the present benchmark sample vary from a high of +1.84 to a low of -1.25 with an SES mean value at 0.481.

Figure 17. Annualized cost in descending order by SES

Regression performed on SES ranging from -1.25 to +1.84.



A comparison of organizations grouped into four quartiles based on SES reveals cost differences. According to Table 3 the average cost for companies in SES quartile 1 is €2.29 million, while the average cost for SES quartile 4 is substantially higher at €10.29 million. This analysis supports the above regression equation, which shows a company's security posture has a net favorable affect on cyber crime costs.

Table 3. Quartile analysis 1,000,000 omitted	2012 total cost	2013 total cost
Quartile 1 (highest SES)	1.55 €	2.29 €
Quartile 2	4.05 €	4.17 €
Quartile 3	4.48 €	6.32 €
Quartile 4 (lowest SES)	9.73 €	10.29 €

Organizations deploying security intelligence technologies realize a lower annualized cost of cyber crime.

Figure 18 reports the annualized cost of cyber crime allocated to the six cost activity centers explained previously. The Figure below compares companies deploying and not deploying security intelligence systems. In total, 25 companies (53 percent) deploy security intelligence tools such as SIEM, IPS with reputation feeds, network intelligence systems, big data analytics and others.

With one exception (containment costs), companies using security intelligence systems experience lower activity costs than companies that do not use these technologies. The largest cost differences in millions pertain to investigation (€1.16 vs. €0.65), recovery (€1.41 vs. €1.00) and incident management (€0.77 vs. €0.50) activities, respectively.

Figure 18. Activity cost comparison and the use of security intelligence technologies

1,000,000 € omitted

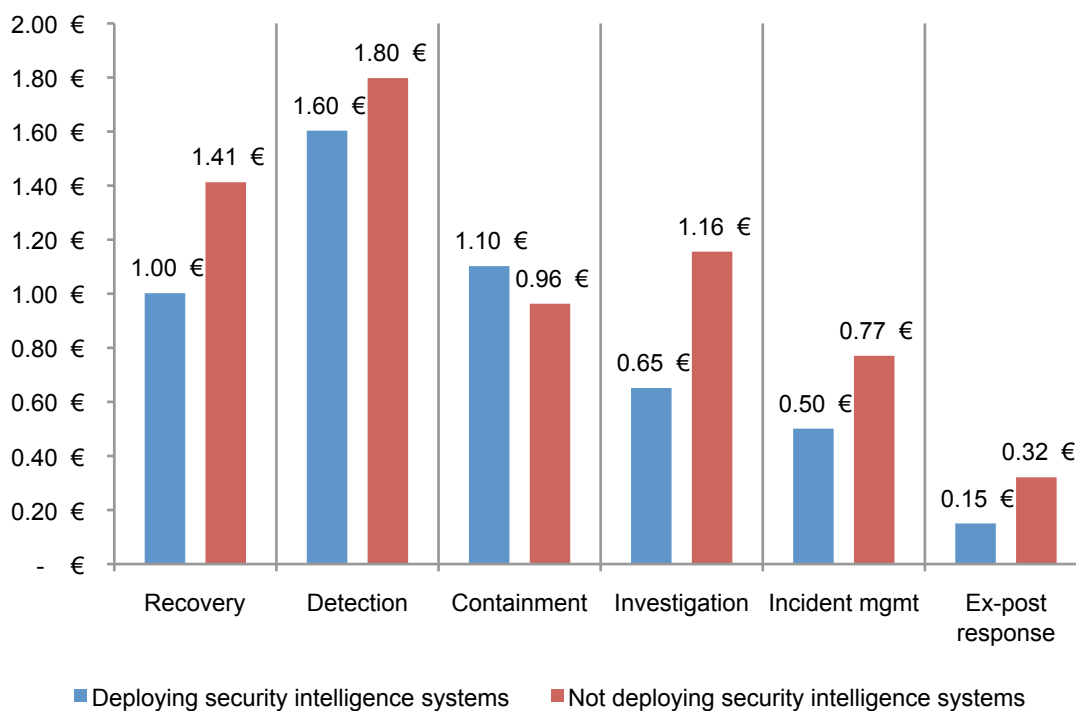


Figure 19 shows seven enabling security technology categories experienced by a subset of benchmarked companies. Each bar represents the percentage of companies fully deploying each given security technology. The top three technology categories include: enterprise encryption technologies (60 percent), security intelligence systems (53 percent) and extensive use of data loss prevention tools (51 percent).

Figure 19. Seven enabling security technologies deployed

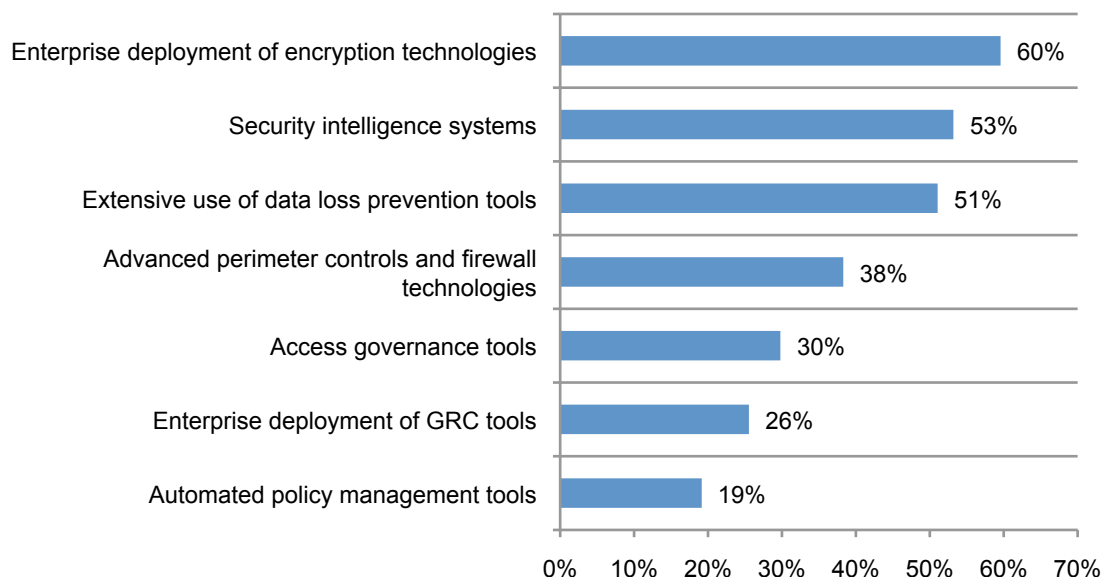


Figure 20 shows the amount of money companies save by deploying each one of seven enabling security technologies. For example, companies deploying security intelligence systems, on average, experience a substantial cost savings of €1.4 million. Similarly, companies deploying encryption tools experience cost savings of €1.25 million on average. Please note that these extrapolated cost savings are not additive.

Figure 20. Cost savings when deploying seven enabling security technologies

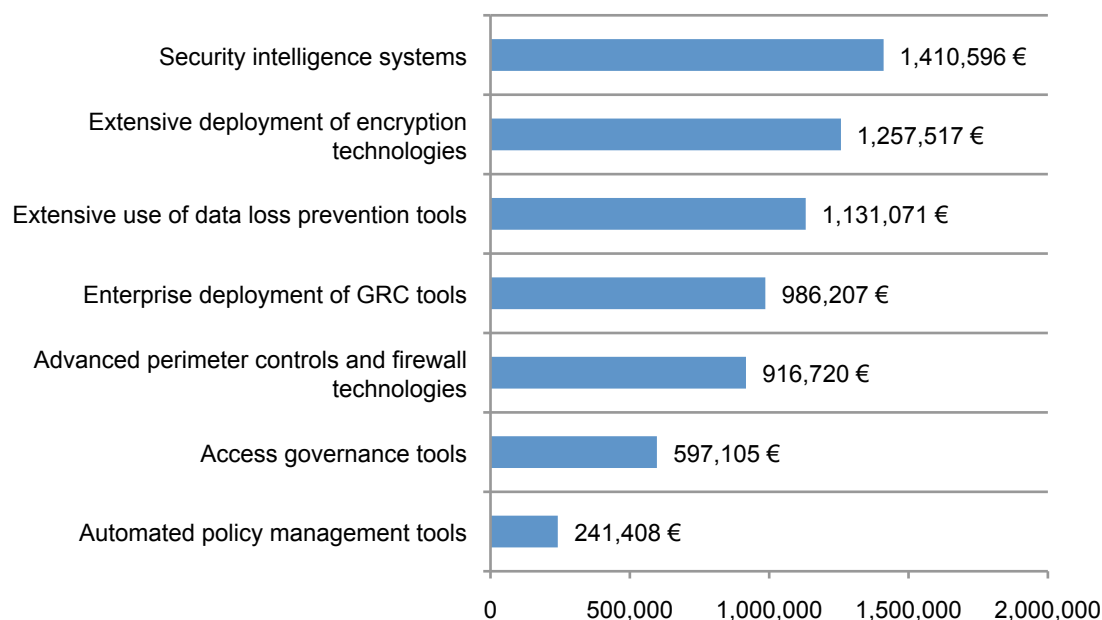
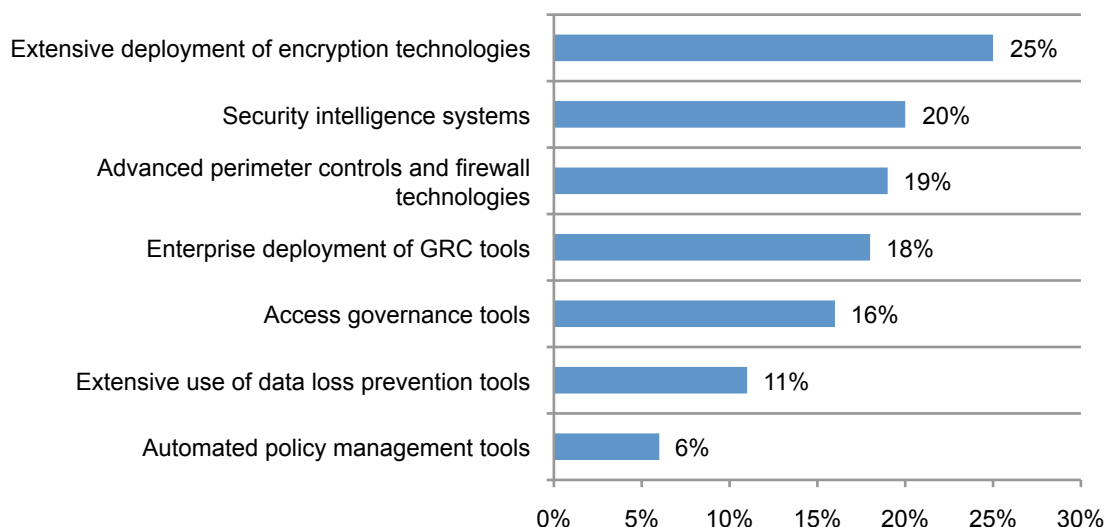


Figure 21 summarizes the estimated return on investment (ROI) realized by companies for each one of the seven categories of enabling security technologies indicated above.¹³ At 25 percent, companies deploying encryption, on average, experienced a substantially higher ROI than all other technology categories presented.

Also significant are the estimated ROI results for companies that extensively deploy security intelligence systems (20 percent) and advanced perimeter controls such as UTM, NGFW, IPS with reputation feeds and more (19 percent). The estimated average ROI for all seven categories of enabling security technologies is 16 percent.

Figure 21. Estimated ROI for seven categories of enabling security technologies



¹³The return on investment calculated for each security technology category is defined as: (1) gains from the investment divided by (2) cost of investment (minus any residual value). We estimate a three-year life for all technology categories presented. Hence, investments are simply amortized over three years. The gains are the net present value of cost savings expected over the investment life. From this amount, we subtract conservative estimates for operations and maintenance cost each year. The net present value used the prime plus 2 percent discount rate per year. We also assume no (zero) residual value.

Figure 22 shows seven enterprise governance activities experienced by a subset of benchmarked companies. Each bar represents the percentage of companies fully executing each stated governance activity. The top three governance activities include: certification against industry-leading standards (68 percent), obtaining sufficient budget (60 percent) and appointment of a high-level security leader (57 percent).

Figure 22. Seven enterprise security governance activities deployed

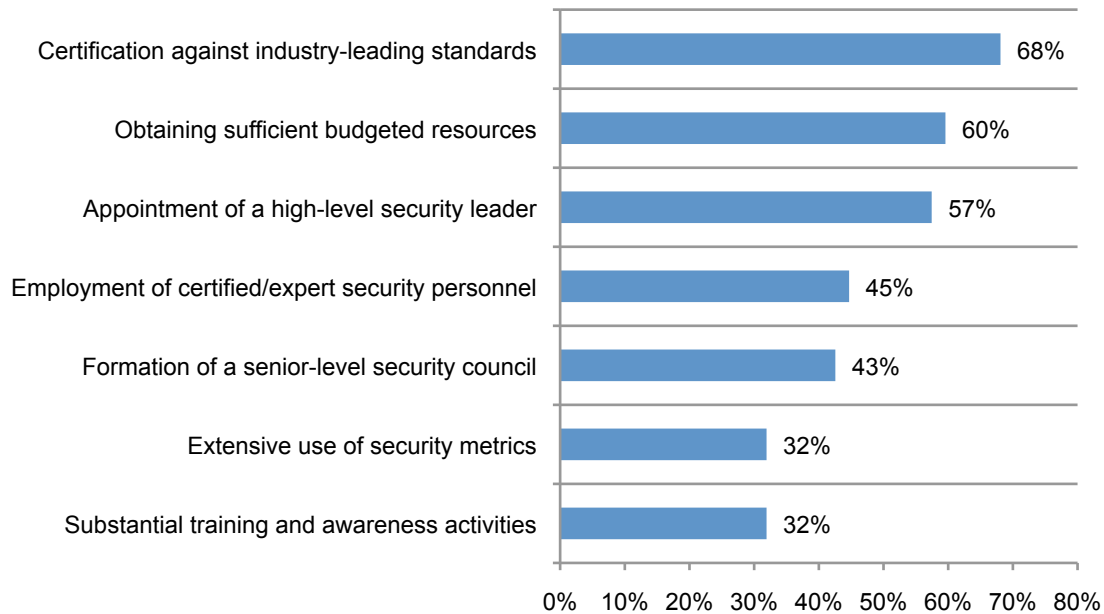
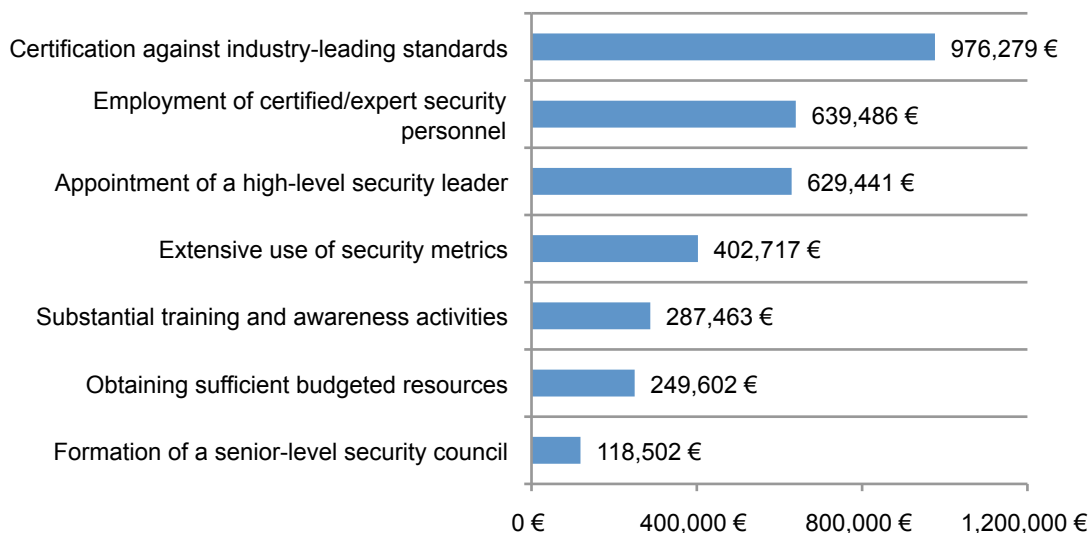


Figure 23 shows the incremental cost savings experienced by companies deploying each one of seven enterprise governance activities. As shown, companies certifying against industry-leading standards save an average of €976,279. Employment of certified/expert personnel saves an average of €639,486. Similar to the above analysis of security technology categories, cost savings resulting from improved governance activities are not additive.

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

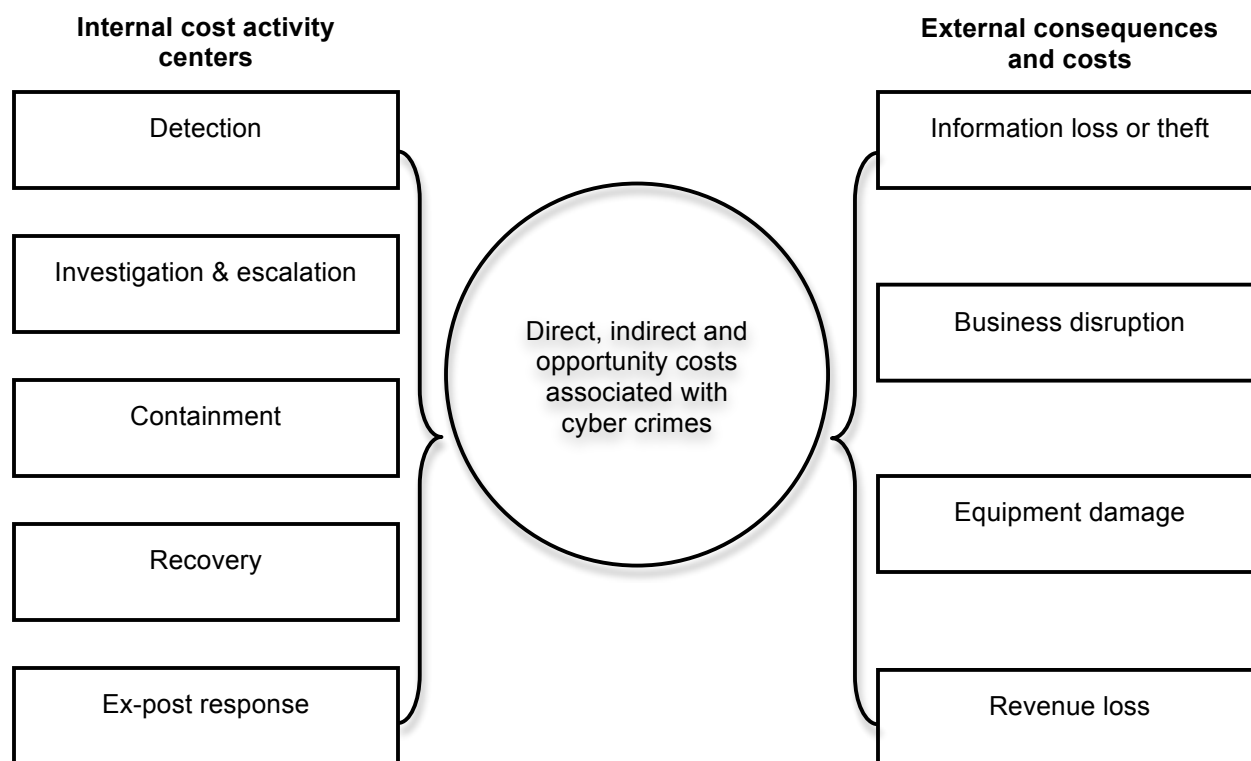


Part 3. Framework

Benchmark results of 47 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 cost framework in Figure 24 presents the two separate cost streams used to measure the 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 24
Cost 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:¹⁴

- **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.

¹⁴ 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.

- Investigation and escalation: Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents. The escalation activity also includes the steps taken to organize an initial management response.
- Containment: Activities that focus on stopping or lessening the severity of cyber attacks or advanced threats. These include shutting down high-risk attack vectors such as insecure applications or endpoints.
- Recovery: Activities associated with repairing and remediating the organization's systems and core business processes. These include the restoration of damaged information assets and other IT (data center) assets.
- Ex-post response: Activities to help the organization minimize potential future attacks. These include 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 specifically mentioned in Figure 24, the nature of attacks that underlie cost in our framework include the following attack types: viruses, worms, trojans; malware; botnets; web-based attacks; phishing and social engineering; malicious insiders (including stolen devices); malicious code (including SQL injection); and denial of services.¹⁵

¹⁵ 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 4. Benchmarking

The cost of cyber crime benchmark instrument is designed to collect descriptive information from IT, information security and other key individuals about the actual costs incurred either directly or indirectly as a result of cyber attacks actually detected. Our cost method does not require subjects to provide actual accounting results, but instead relies on estimation and extrapolation from interview data over a four-week period.

Cost estimation is based on confidential diagnostic interviews with key respondents within each benchmarked organization. Table 4 reports the frequency of individuals by their approximate functional discipline that participated in this year's German study. As can be seen, this year's study involved 398 individuals or an average of 8.47 interviews for each benchmarked company.

Table 4: Functional areas of interview respondents	Frequency	Pct%
IT security	72	18%
IT operations	65	16%
Compliance	46	12%
Data center management	42	11%
Network operations	39	10%
Legal	21	5%
IT risk management	19	5%
Accounting & finance	19	5%
Internal or IT audit	18	5%
Physical security/facilities mgmt	15	4%
Application development	13	3%
Enterprise risk management	10	3%
Human resources	8	2%
Industrial control systems	5	1%
Quality assurance	4	1%
Procurement/vendor mgmt	2	1%
Total	398	100%
Interviews per company	8.47	

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, labor and overhead incurred. Please mark only one point somewhere between the lower and upper limits set above. You can reset the lower and upper limits of the number line at any time during the interview process.

Post your estimate of direct costs here for [presented cost category]

LL	<div style="border-bottom: 1px solid black; height: 20px; position: relative;"> <div style="position: absolute; left: 50%; transform: translateX(-50%); border-left: 1px solid black; border-right: 1px solid black; height: 10px;"></div> </div>	UL
----	---	----

The numerical value obtained from the number line rather than a point estimate for each presented cost category preserved confidentiality and ensured a higher response rate. The

benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

Cost estimates were then compiled for each organization based on the relative magnitude of these costs in comparison to a direct cost within a given category. Finally, we administered general interview questions to obtain additional facts, including estimated revenue losses as a result of the cyber crime.

The size and scope of survey items was limited to known cost categories that cut across different industry sectors. In our experience, a survey focusing on process yields a higher response rate and better quality of results. We also used a paper instrument, rather than an electronic survey, to provide greater assurances of confidentiality.

Figure 24 (shown above) 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, a few companies were rejected because of incomplete, inconsistent or blank responses.

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 six internal activity centers (see Figures 14 & 15). 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.

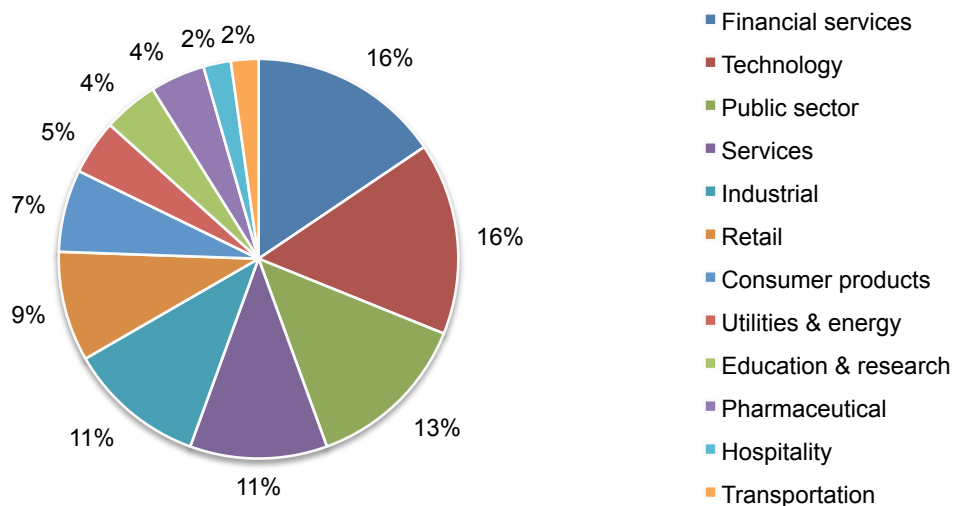
Field research was conducted over several months concluding in August 2013. To maintain consistency for all benchmark companies, information was collected above the organizations' cyber crime experience was limited to four consecutive weeks. The four consecutive weeks for any given organization was not necessarily the same time period as every other organization in this study. The extrapolated direct, indirect and opportunity costs of cyber crime were annualized by dividing the total cost collected over four weeks (ratio = 4/52 weeks).

Part 5. Benchmark Sample

The recruitment of the annual study started with a personalized letter and a follow-up phone call to 246 German organizations for possible participation.¹⁶ While 50 organizations initially agreed to participate, 47 organizations permitted Ponemon Institute to perform the benchmark analysis.

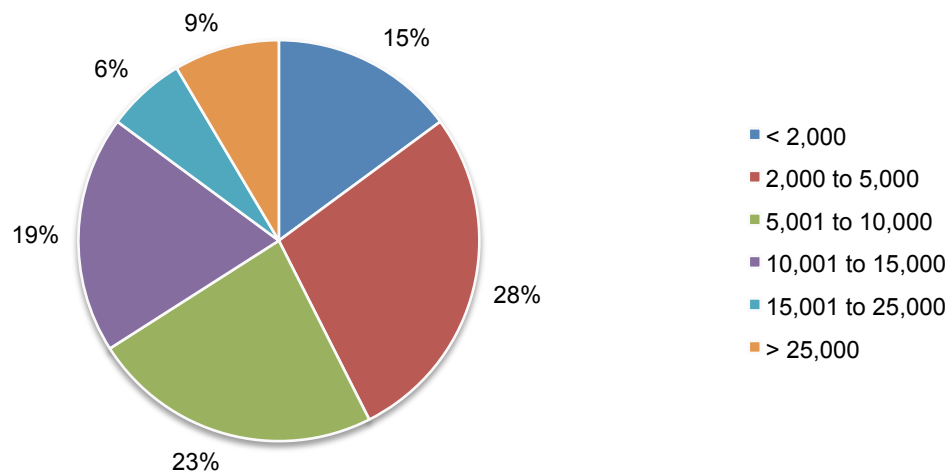
Pie Chart 1 summarizes the current (FY 2013) sample of participating companies based on 12 primary industry classifications. As can be seen, financial services and technology (both 16 percent) represent the largest segment. Financial services include retail banking, insurance, brokerage and credit card companies. The technology segment includes organizations in software and IT management.

Pie Chart 1. Industry sectors of participating organizations



Pie Chart 2 reports the percentage frequency of companies based on the number of enterprise seats connected to networks or systems. Our analysis of cyber crime cost only pertains to organizations with a minimum of over 500 seats. The largest enterprise has 40,260 seats.

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



¹⁶Approximately, half of the organizations contacted for possible participation in this year's study are members of Ponemon Institute's benchmarking community.

Part 6. Limitations & Conclusions

This study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier Ponemon Institute research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

- **Non-statistical results:** The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of organizations, all German-based entities experiencing one or more cyber attacks during a four-week fielding period. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the nature of our sampling plan.
- **Non-response:** The current findings are based on a small representative sample of completed case studies. An initial mailing of benchmark surveys was sent to a targeted group of organizations, all believed to have experienced one or more cyber attacks. Forty-seven companies provided usable benchmark surveys. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the methods used to manage the cyber crime containment and recovery process, as well as the underlying costs involved.
- **Sampling-frame bias:** Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature information security programs.
- **Company-specific information:** The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.
- **Unmeasured factors:** To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.
- **Estimated cost results.** The quality of survey research is based on the integrity of confidential responses received from companies. While certain checks and balances can be incorporated into the survey process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique (termed shadow costing methods) rather than actual cost data could create significant bias in presented results.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49629 USA
1.800.887.3118
research@ponemon.org

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.