2012 Cost of Cyber Crime Study:
Germany

Sponsored by HP Enterprise Security
Independently conducted by Ponemon Institute LLC
Publication Date: October 2012

2012 Cost of Cyber Crime Study: Germany
Benchmark Study of German Organizations
Ponemon Institute October 2012

Part 1. Executive Summary

We are pleased to present the *2012 Cost of Cyber Crime Study: Germany*. Sponsored by HP Enterprise Security, this is the first year the study was conducted in Germany to better understand the economic impact a cyber attack can have on an organization. The benchmark study is based on a representative sample of 43 organizations in various industry sectors.

The first *Cost of Cyber Crime Study* was conducted in the US in 2010 and is now in its third year. This year the scope of the research was expanded to include organizations in Germany as well as in the United Kingdom, Australia and Japan. Findings from these countries are presented in separate reports.

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. In Germany, theft of information and revenue losses create the highest costs for organizations following a cyber attack.

Key takeaways from this report include:

- Cyber crimes are costly. We found that the average annualized cost of cyber crime for the 43 organizations in our study is 4.8 million Euros (€) per year, with a range of 0.6 million to 18.3 million.

- Cyber attacks have become common occurrences. The companies in our study experienced 48 successful attacks per week or more than 1.1 successful attacks per organization per week.

- The most costly cyber crimes are those caused by malicious insiders, denial of services, and malicious code. 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 would not capture the necessary details required to extrapolate cyber crime costs. Therefore, we decided to pursue field-based research that involved interviewing senior-level personnel and collecting details about actual cyber crime incidents. Approximately nine months of effort was required to recruit companies, build an activity-based cost model, collect source information and analyze results.

This research culminated with the completion of case studies involving 43 organizations. For consistency purposes, our benchmark sample consists of only larger-sized organizations (i.e., more than 1,000 enterprise seats[1]).

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

---

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

property, plant and equipment. In addition to external consequences of the cyber crime, the analysis attempted to capture the total cost spent on detection, investigation, containment, recovery and after-the-fact or "ex-post" response.

Global at a glance

As discussed above, the study has been conducted in the US for three years and this is the first year we included the UK, Germany, Australia and Japan. Some of the most interesting similarities and differences are presented below.

Figure 1 presents the estimated average cost of cyber crime for five country samples after conversion into US dollars. As shown, there is significant variation among companies in the benchmark samples. The US sample reports the highest total average cost at $8.9 million and the UK sample reports the lowest total average cost at $3.3 million.

Figure 1. Total cost of cyber crime in five countries
Costs expressed in US dollars, n = 199 separate companies
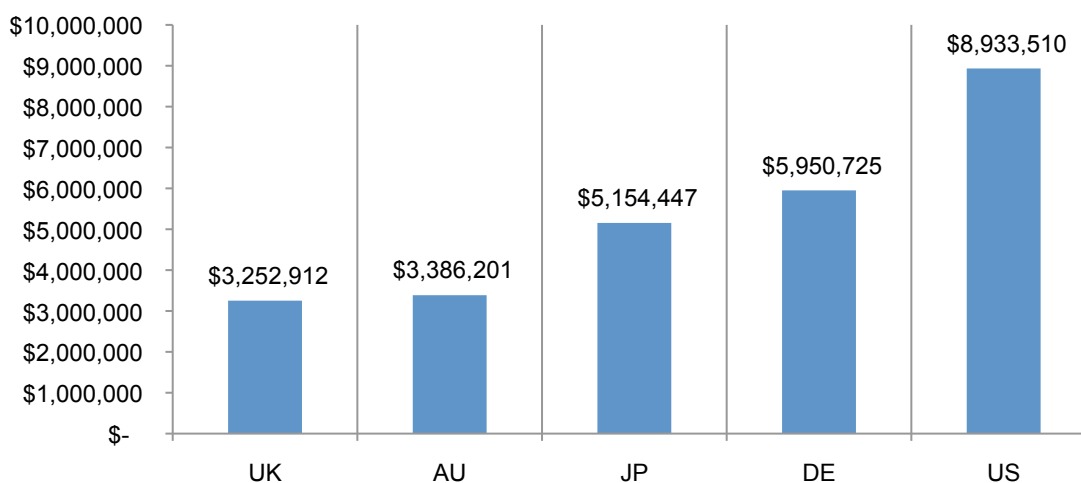
Possible reasons for these differences may be the types and frequencies of attacks experienced as well as the importance that each company places on the theft of information assets versus other consequences of the incident.

We found that US companies were much more likely to experience the most expensive types of cyber attacks, which are malicious insiders, malicious code and web-based incidents. Similarly, UK and Australian were most likely to experience denial of service attacks. In contrast, German companies were least likely to experience malicious code and denial of services. Japanese companies were least likely to experience malicious insiders and web-based attacks.

Another key finding that may explain cost differences among countries concerns the theft of information assets. US and German companies report this as the most significant consequence of a cyber attack. On the other hand, UK and Australia attach more importance to business disruption. As noted in this report, the cost of business disruption can be lower than the theft of information.

With respect to internal activity costs, we also found interesting differences. Specifically, the cost of detecting a cyber attack appears to be the most expensive for German companies. The cost of recovery from a cyber incident appears to be more expensive for companies in the UK and Australia. It is interesting to note that Japanese companies cite higher costs to investigate and manage the incident than the other countries.

Summary of German findings

Following are the most salient findings of this year's study. These findings focus on the factors that affect the cost of cyber crime for organizations.

Cyber crimes are costly. We found that the median annualized cost for 43 benchmarked organizations is 4.8 million Euros per year, with a range from 0.6 million to 18.3 million each year per company.

Cyber crime cost varies by organizational size. Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost. However, based on enterprise seats, we determined that smaller-sized organizations incur a significantly higher per capita cost than larger-sized organizations (780 versus 140 Euros).

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

Cyber crimes are intrusive and common occurrences. The companies participating in our study experienced 48 successful attacks per week – or more than 1.1 successful attacks per organization.

The most costly cyber crimes are those caused by malicious insiders, denial of services and malicious code. These account for more than 58 percent of all cyber crime costs per organization on an annual basis. Mitigation of such attacks requires enabling technologies such as SIEM, intrusion prevention systems, application 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. The average time to resolve a cyber attack was 22 days, with an average cost to participating organizations of 294,829 Euros over this 22-day period. Results show that malicious insider attacks can take more than 42 days on average to contain.

Theft of information assets and revenue losses represent the highest external costs. Information losses account for 40 percent of total external costs.[2] In addition, costs associated with revenue losses and theft of information assets represent 53 percent of external costs.

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

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 1.1 million Euros when compared to companies not deploying security intelligence technologies.

Deployment of enterprise security governance practices moderates the cost of cyber crime. Findings show companies that have adequate resources, appoint a high-level security leader, and employ certified or expert staff experience cyber crime costs that are lower than companies that have not implemented these practices. This so-called "cost savings" for

---

[2]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.

companies deploying good security governance practices is estimated to be on average more than 1.07 million Euros.

A strong security posture moderates the cost of cyber attacks. We utilize a well-known metric called the Security Effectiveness Score (SES) to define an organization's ability to achieve reasonable security objectives.[3]   The higher the SES, the more effective the organization is in achieving its security objectives. The average cost to mitigate a cyber attack for organizations with a high SES is substantially lower than organizations with a low SES score.

---

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

Part 2. Report Findings

Ponemon Institute's *2012 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 ongoing expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

Cyber crimes are costly for participating organizations

The economic impact of a cyber attack is wide ranging and is influenced by a variety of factors discussed in this report. The total annualized cost of cyber crime for the 2012 benchmark sample of 43 organizations ranges from a low of 0.6 million to a high of 18.3 million Euros. Participating companies were asked to report 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, the reported figures were then grossed-up to present an extrapolated annualized cost.[4]

Figure 2 shows the median annualized cost of cyber crime in the study benchmark sample is 3.2 million Euros. The grand mean value is 4.8 million Euros.

Figure 2. The Cost of Cyber Crime

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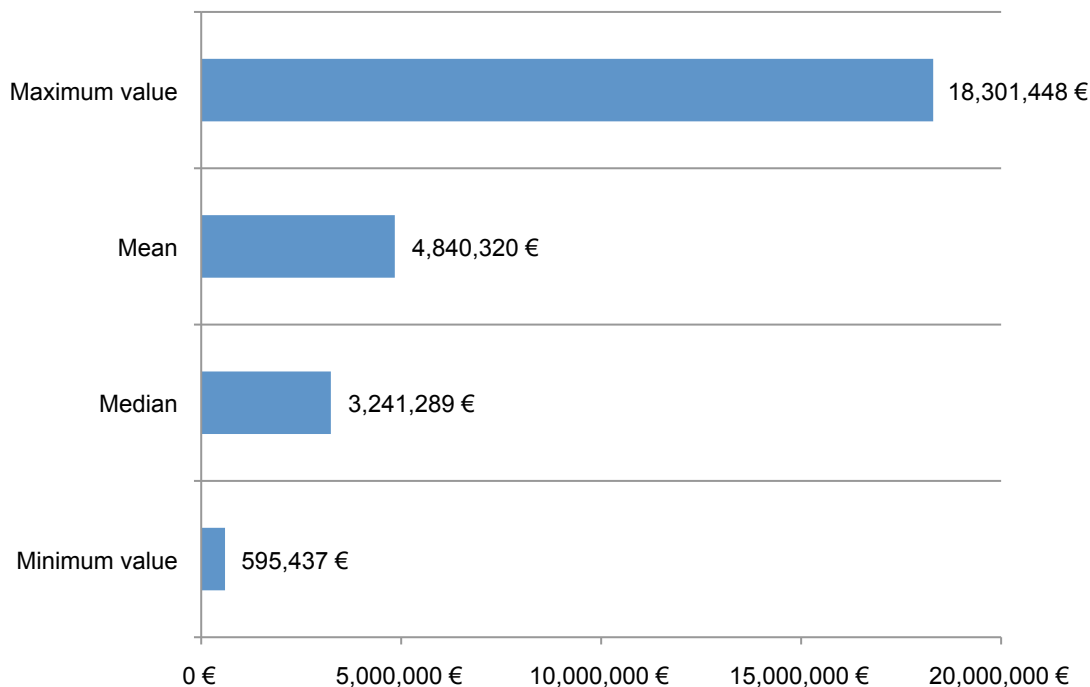
[4]Following is the gross-up statistic: Annualized revenue = [cost estimate]/[4/52 weeks].

Figure 3 reports the distribution of annualized total cost for 43 companies. As can be seen, 28 of organizations in our sample incurred total costs below the mean value of 4.8 million Euros, thus indicating a skewed distribution. The highest cost estimate of 18.3 million Euros was determined not to be an outlier based on additional analysis. Six other organizations experienced an annualized total cost of cyber crime above 10 million Euros. The lowest total cost was 0.6 million.

Figure 3. Total cost of cyber crime for 43 participating companies
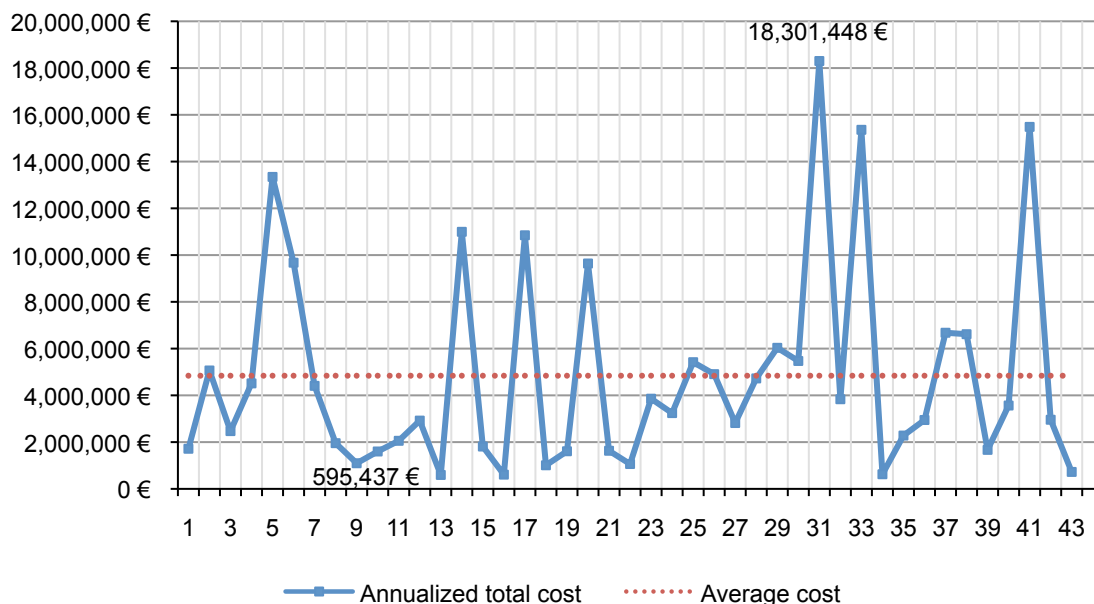
As part of our analysis, we calculated a precision interval for the average cost of 4.8 million. The purpose of this interval is to demonstrate that our cost estimates should be thought of as a range of possible outcomes rather than a single point or number. The range of possible cost estimates widens at increasingly higher levels of confidence, as shown in Figure 4.

**Figure 4. Precision interval for the mean value of annualized total cost**
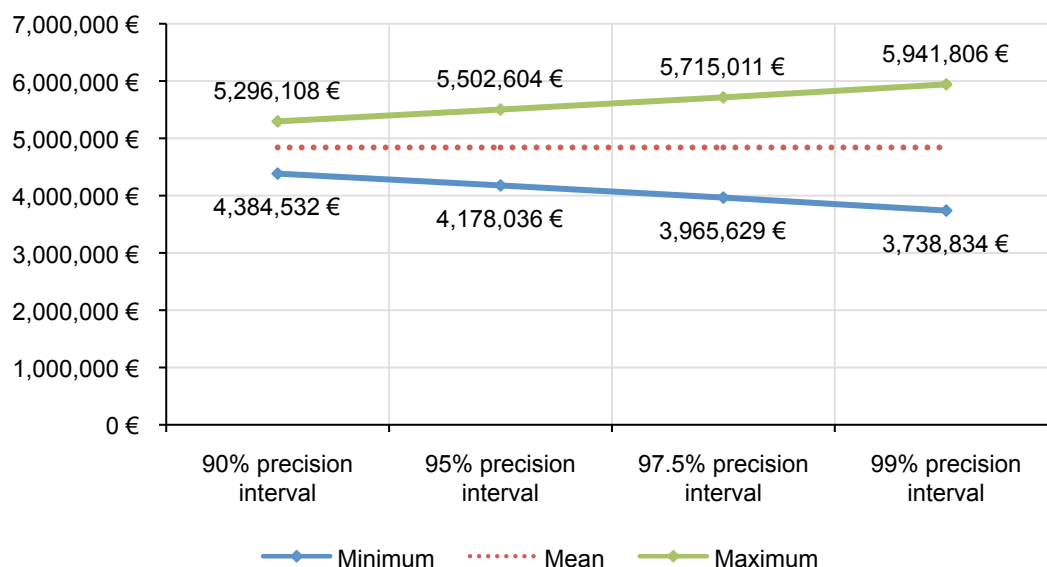
The cost of cyber crime varies by organizational size

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 slopping regression line.

Figure 5. Annualized cost in ascending order by the number of enterprise seats
Regression performed on enterprise seats ranging from 1,044 to 95,419
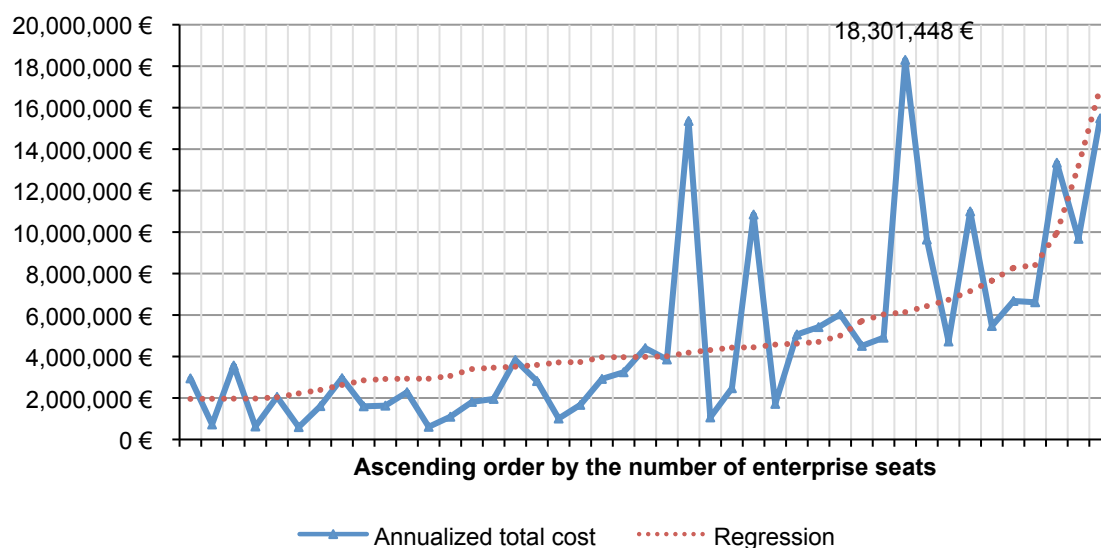
The following tables show that organizational size can influence the cost of cyber crime.

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 2012.

Table 1: Quartile analysis	FY 2012 (n=43)
Quartile 1	2,290,658 €
Quartile 2	3,479,637 €
Quartile 3	4,545,193 €
Quartile 4	8,814,005 €

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). The 2012 average per capita cost for organizations with the fewest seats is more than 3.5 times higher than the average per capita cost for organizations with the most seats.

Table 2. Quartile analysis	2012 cost per seat
Quartile 1 (smallest)	730 €
Quartile 2	328 €
Quartile 3	262 €
Quartile 4 (largest)	200 €

In Figure 6, we compare of smaller and larger-sized organizations split by the sample median of 13,785 seats. This reveals the cost of specific cyber attacks varies by organizational size. Smaller organizations (below the median) experience a higher proportion of cyber crime costs relating to viruses, worms, trojans, phishing, stolen devices, malicious code and web-based attacks. In contrast, larger organizations (above the median) spend a higher proportion of costs when they experience denial of services and malicious insiders.

Figure 6. The cost of attacks varies according to organizational size
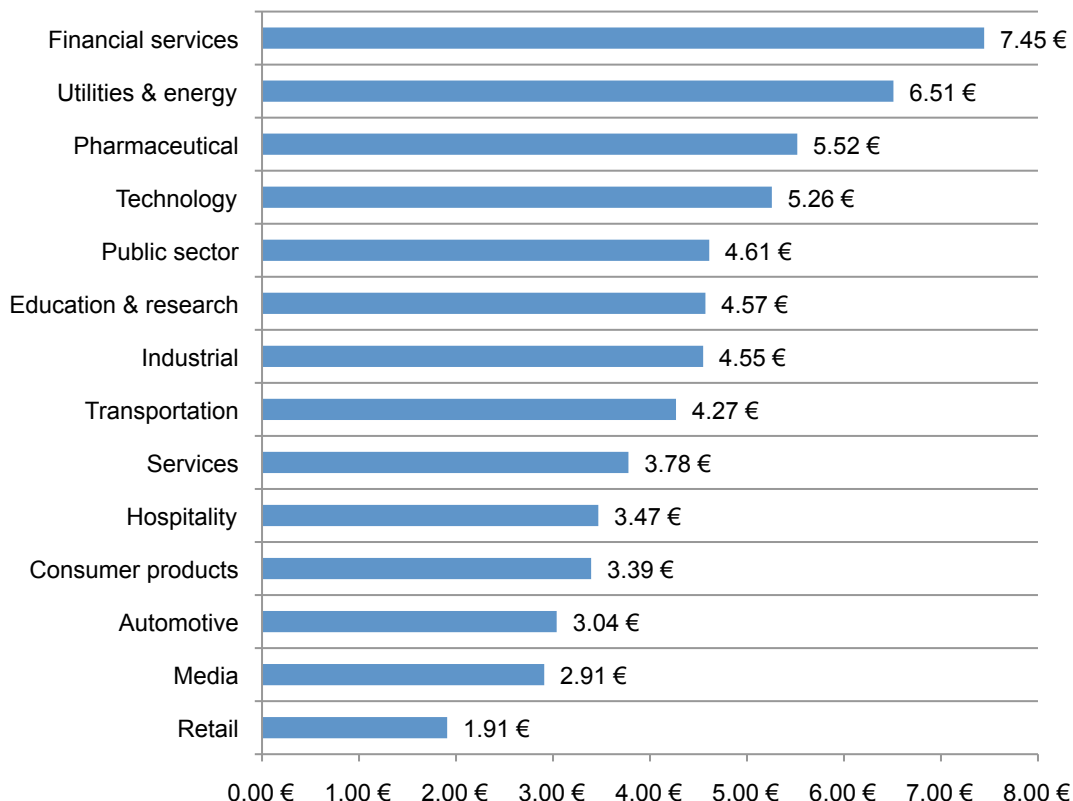Size measured according to the number of enterprise seats within the participating organizations
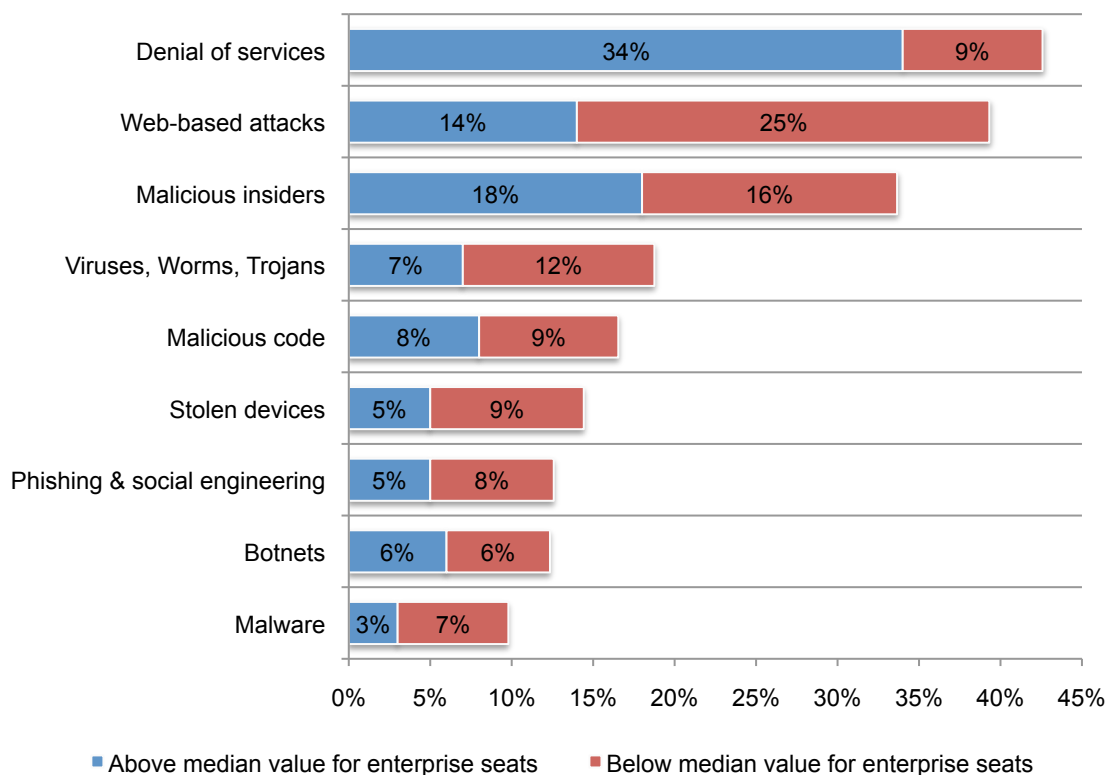
The cost of cyber crime impacts all industries

The average annualized cost of cyber crime appears to vary by industry segment. As seen in Figure 7, financial services, utilities & energy and pharmaceutical companies experience substantially higher costs. Organizations in retail, media and automotive appear to have a lower overall cyber crime cost.[5]

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

| Industry	Cost
Financial services	7.45 €
Utilities & energy	6.51 €
Pharmaceutical	5.52 €
Technology	5.26 €
Public sector	4.61 €
Education & research	4.57 €
Industrial	4.55 €
Transportation	4.27 €
Services	3.78 €
Hospitality	3.47 €
Consumer products	3.39 €
Automotive	3.04 €
Media	2.91 €
Retail	1.91 €

---

[5]This analysis is for illustration purposes only. The sample sizes in all three years are too small to draw definitive conclusions about industry segment differences.

Cyber crimes are intrusive and common occurrences

The benchmark sample of 43 organizations experienced 48 discernible and successful cyber attacks per week, which translates to more than 1.1 successful attacks per benchmarked organization each week. Figure 8 summarizes the types of attack methods experienced by participating companies. Virtually all organizations experienced attacks relating to viruses, worms and/or trojans and malware attacks over the four-week benchmarking period.[6]

Figure 8. Types of cyber attacks experienced by 43 benchmarked companies
The percentage frequency defines a type of attack categories experienced
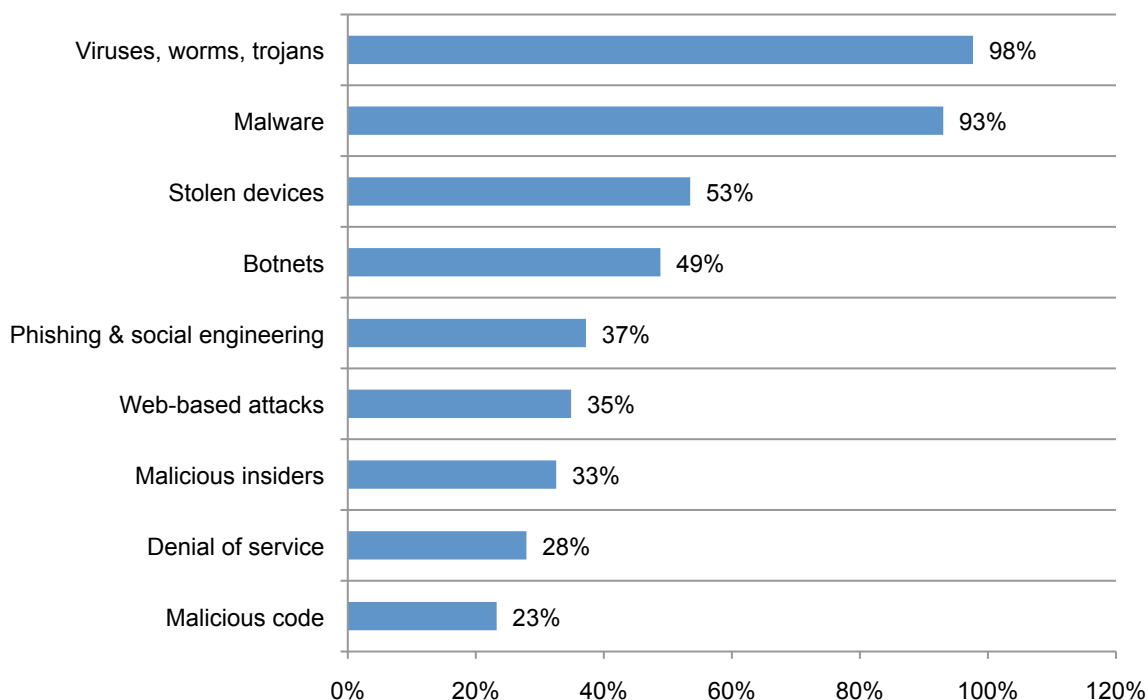
[6]Malware attacks and malicious code attacks are inextricably linked. We classified malware attacks that successfully infiltrated the organizations' networks or enterprise systems as a malicious code attack.

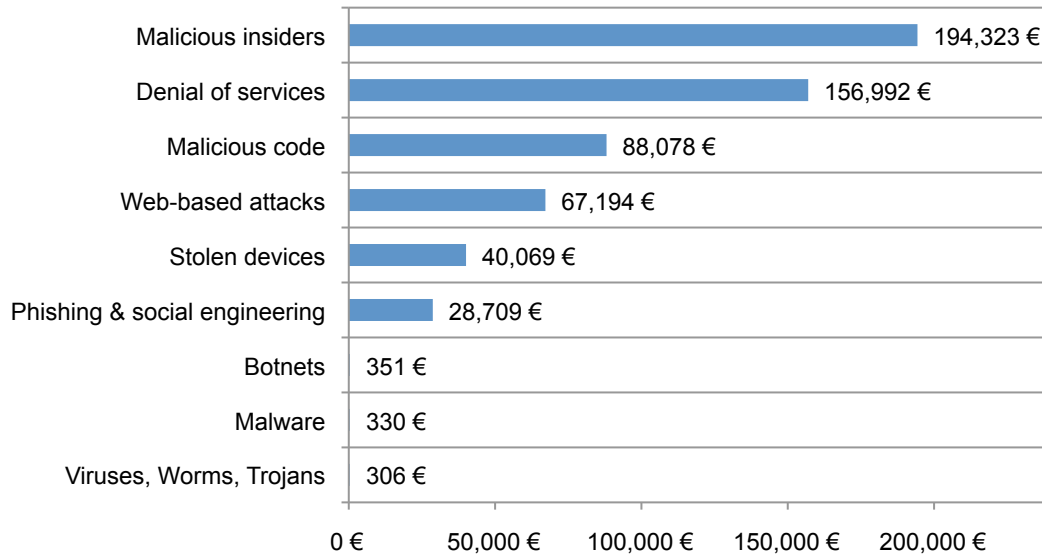**Costs vary considerably by the type of cyber attack**

Figure 9 shows the percentage of annualized cyber crime costs allocated to nine attack types compiled from all benchmarked organizations. Certain attacks represent a higher percentage of the cost of cyber crime. These are: malicious insiders, denial of services and web-based attacks, which represents more than 58 percent of total annualized cost.

Figure 9. Percentage annualized cyber crime cost by attack type
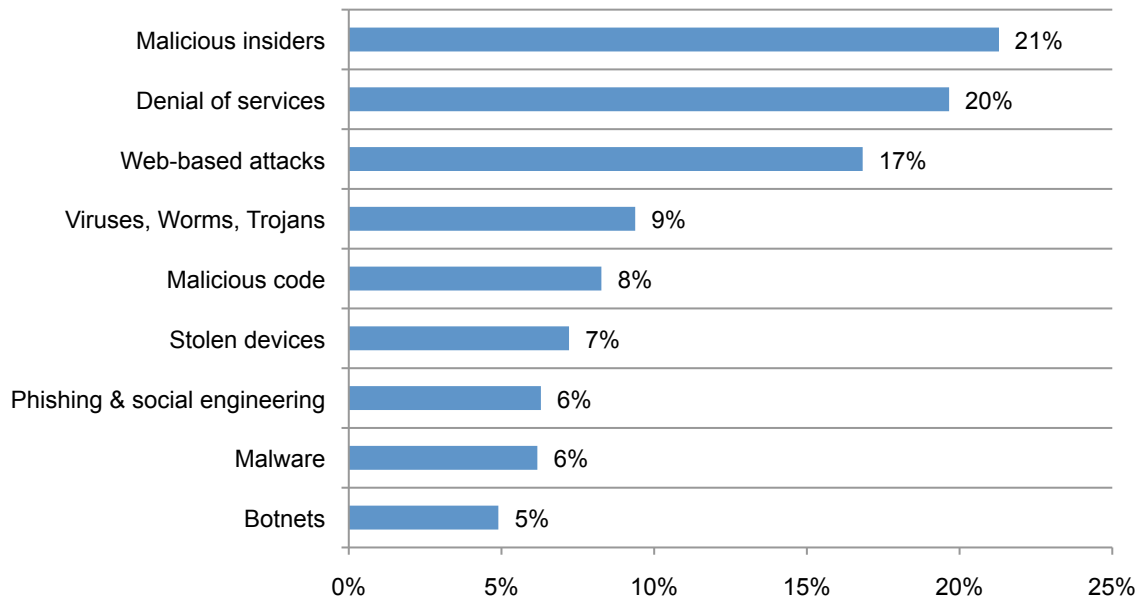
While Figure 9 shows the average percentage of cost according to attack type, Figure 10 reveals the most to least expensive cyber attacks when analyzed on per incident basis. The top two are malicious insiders and denial of services. In the context of our study, malicious insiders include employees, temporary employees, contractors and, possibly, business partners.

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

Attack type	Cost
Malicious insiders	194,323 €
Denial of services	156,992 €
Malicious code	88,078 €
Web-based attacks	67,194 €
Stolen devices	40,069 €
Phishing & social engineering	28,709 €
Botnets	351 €
Malware	330 €
Viruses, Worms, Trojans	306 €

Time to resolve or contain cyber crimes increases the cost

The average number of days to resolve cyber attacks is 22 with a maximum of 53 days. The average cost was 294,829 Euros over the 22-day period. 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
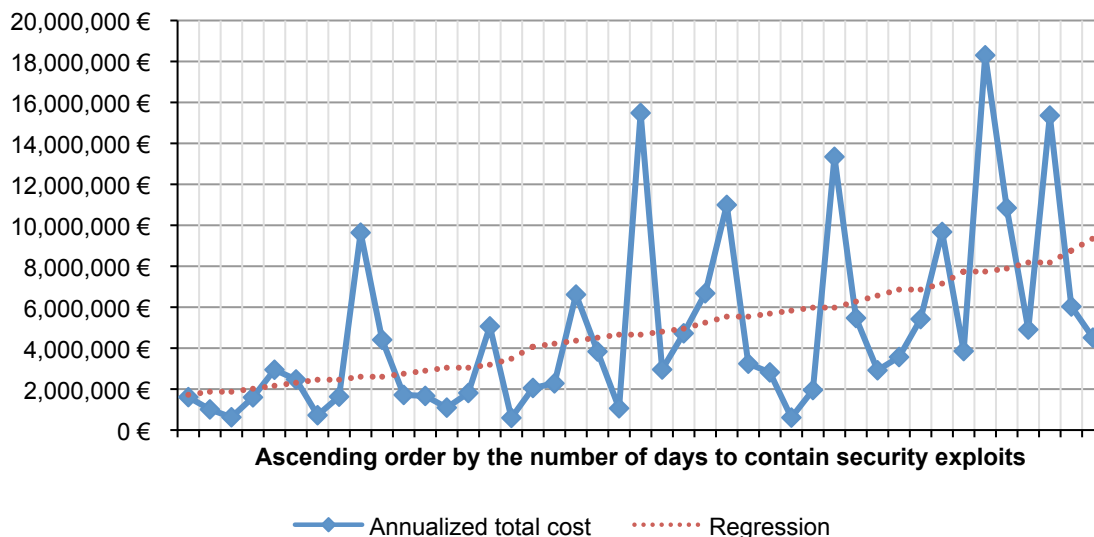Estimated average time is measured for each given organization in days

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, malicious code and web-based attackers (hackers).

Figure 12. Average days to resolve attack
Estimated average time is measured for each attack type in day
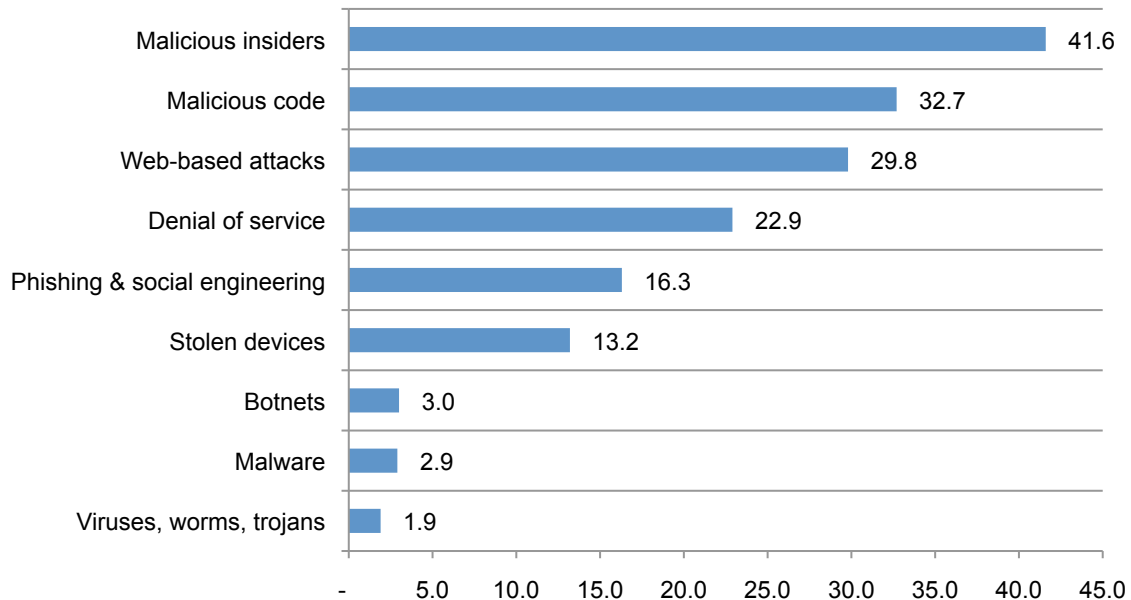
Theft of information assets and revenue losses represents the highest external cost

As shown in Figure 13, at the top end of the external cyber crime cost spectrum is information theft, which accounts for 40 percent of total external costs. In addition, the costs associated with revenue losses and business disruption account for 53 percent of external costs. Equipment damages (5 percent) yield a much lower cost impact.

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
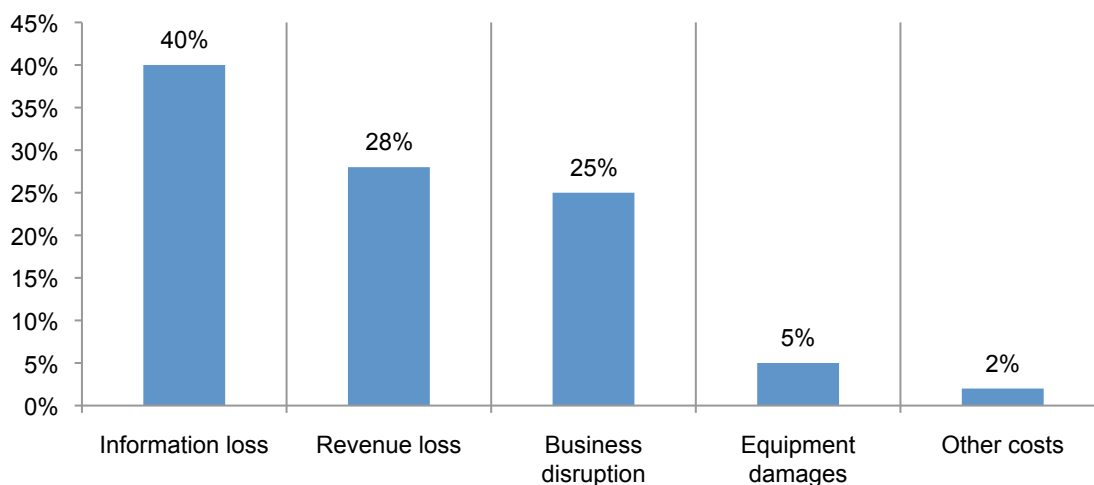
Recovery and detection are the most costly internal activities

Cyber crime detection and recovery activities account for 55 percent of total internal activity cost, as shown in Figure 14. This is followed investigation (19 percent).

Containment and incident management each represent 12 and 9 percent of internal activity cost, respectively. Ex-post response (i.e. after the fact response or remediation) represents the lowest internal activity cost (5 percent). These cost elements highlight a significant cost-reduction opportunity for organizations that are able to automate recovery and detection activities through enabling security technologies.

Figure 14. Percentage cost by internal activity center
Investigation includes escalation activities
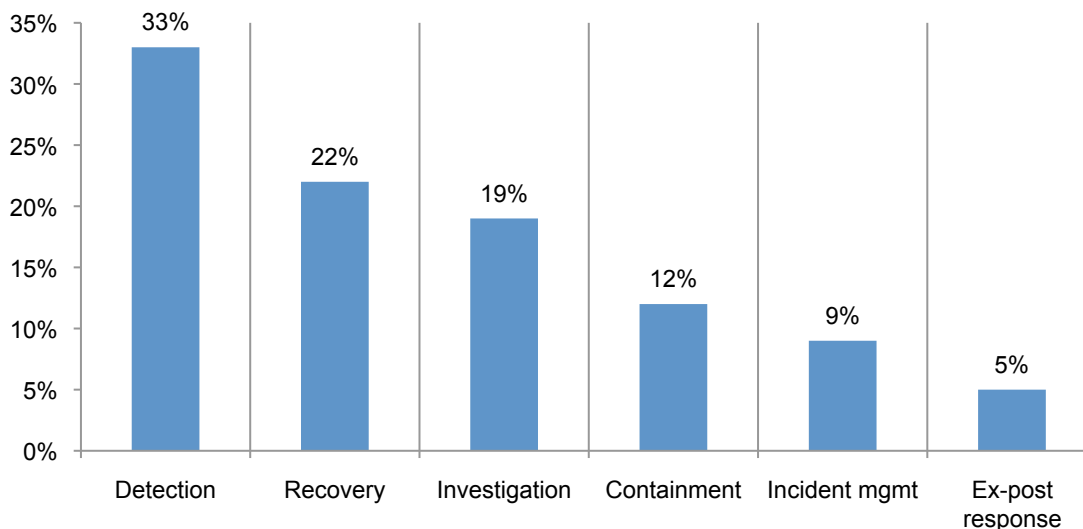
The percentage of annualized costs can be further broken down into six specific expenditure components, which include lost productivity (26 percent), direct labor (23 percent), indirect labor (21 percent) cash outlays (18 percent), overhead (9 percent), as shown in Figure 15.

**Figure 15. Percentage activity cost by six specific cost components**
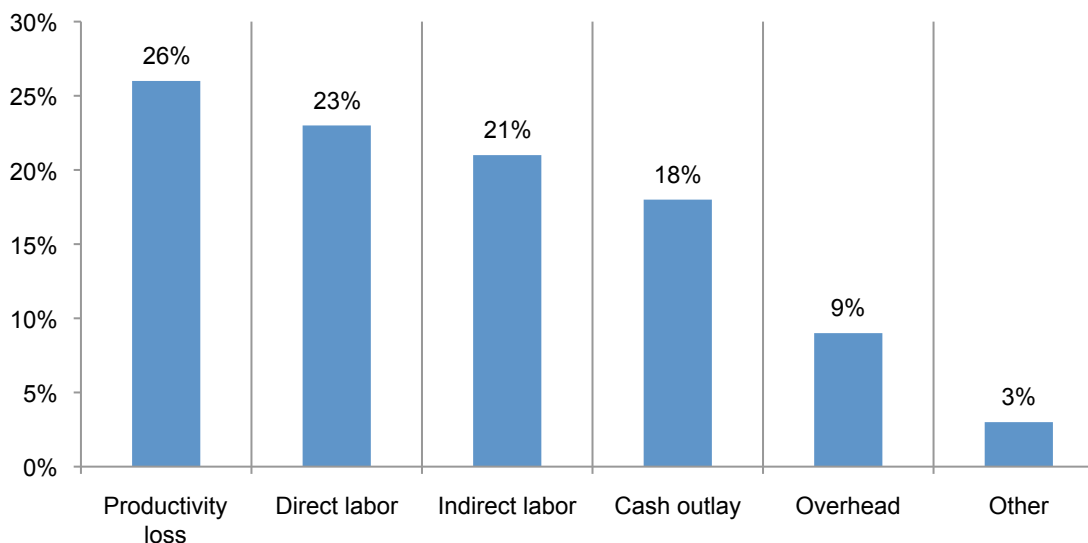
The organization's security posture influences the cost of cyber crime

We measure the security posture of participating organizations as part of the benchmarking process. Figure 16 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 a downward 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 low of -1.00 to a high of +1.58, with a mean value at +0.31.

Figure 16. Annualized cost in ascending order by SES value
Regression performed on SES ranging from -1.00 to +1.58
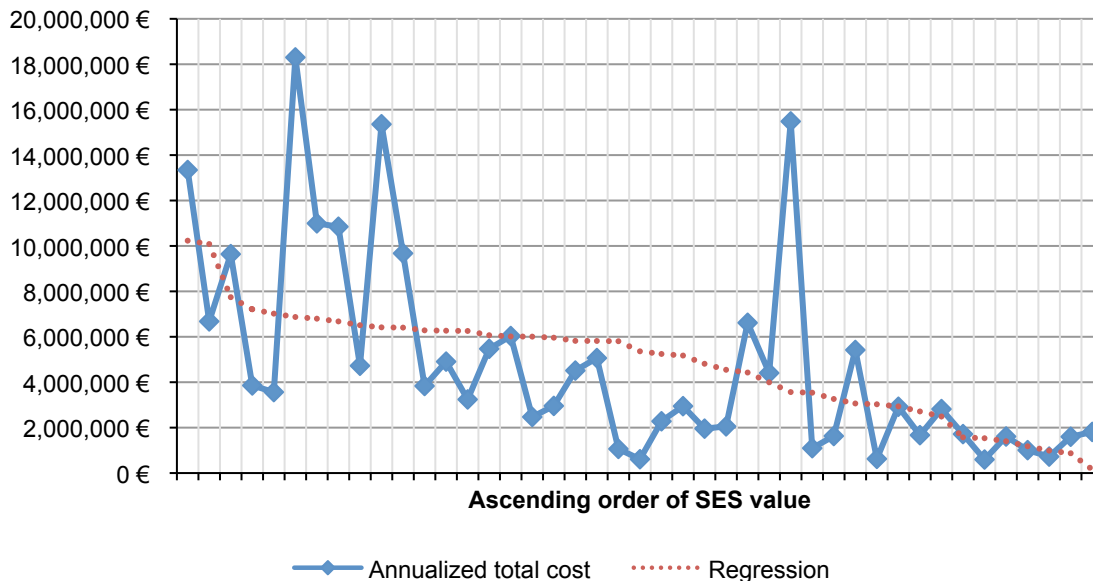
A comparison of organizations grouped into four quartiles based on SES reveals cost differences. Table 3 shows the average cost for companies in quartile 1 is 1.55 million, while the average cost for quartile 4 is substantially higher at 9.73 million Euros. This analysis suggests that the company's security posture has a favorable affect on the total annualized cost of cyber crime.

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

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

Figure 17 reports the annualized cost of cyber crime allocated to the five cost activity centers explained previously. The figure compares companies deploying and not deploying security intelligence systems. As can be seen, companies using security intelligence systems experience a lower cost in three of five activity centers. The largest cost difference pertains to detection (1.91 million vs. 1.36 million), followed by containment (.74 million vs. .45 million) and recovery (1.11 million vs. 1.04 million).

Figure 17. Activity cost comparison and the use of security intelligence activities
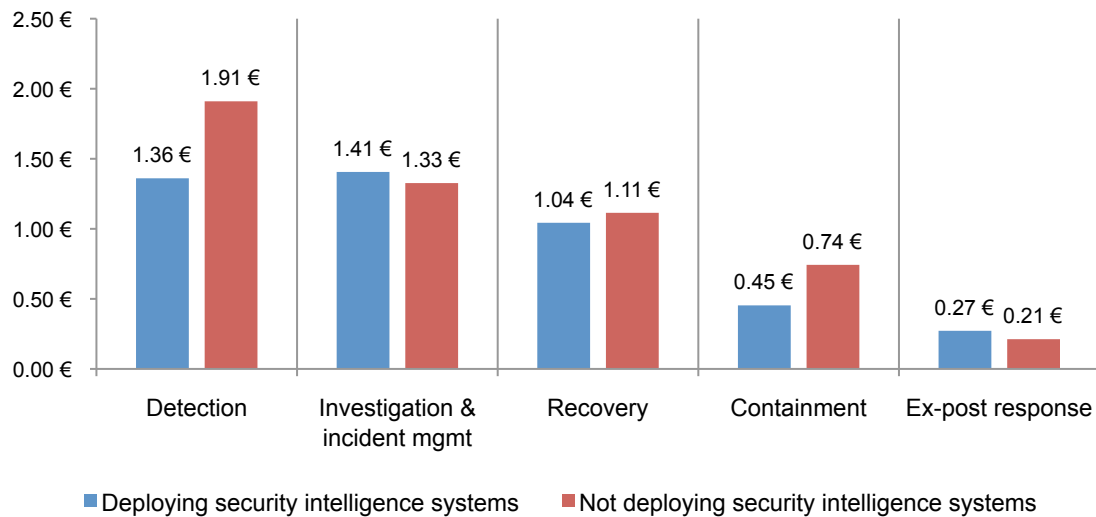1,000,000 € omitted

Figure 18 shows seven enabling security technology categories experienced by a subset of benchmarked companies. Each bar represents the percentage of companies fully deploying the stated technology. The top technology categories include: extensive deployment of encryption technologies (44 percent), security intelligence systems (40 percent) and extensive use of advanced perimeter controls and firewall technologies and data loss prevention tools and (both 28 percent).

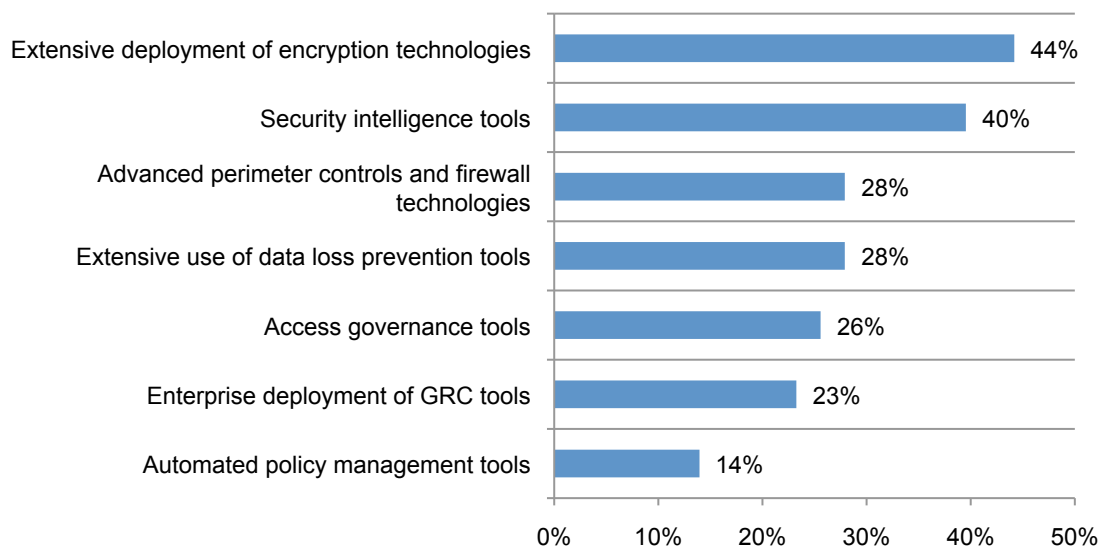**Figure 18. Seven enabling security technologies deployed**

Figure 19 shows the amount of money saved when deploying seven enabling security technologies. For example, companies using access governance tools, on average, experience a cost savings of 0.95 million and companies deploying advanced perimeter controls and firewall technologies have on average a cost savings of 0.85 million Euros. Please note that these cost savings are not additive.

Figure 19. Cost savings when deploying seven enabling security technologies
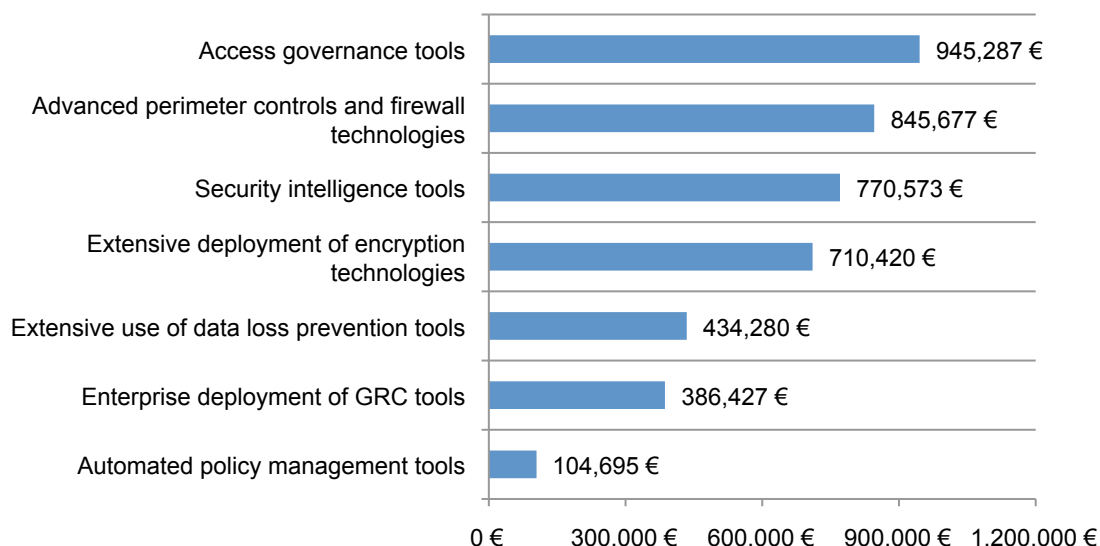
Figure 20 shows seven enterprise governance activities experienced by a subset of benchmarked companies. Each bar represents the percentage of companies fully executing each stated governance activity. The top three governance activities include: certification against industry-leading standards (64 percent), adequacy of budgeted resources (61 percent) and appointment of a high-level security leader (52 percent).

Figure 20. Seven enterprise security governance activities deployed
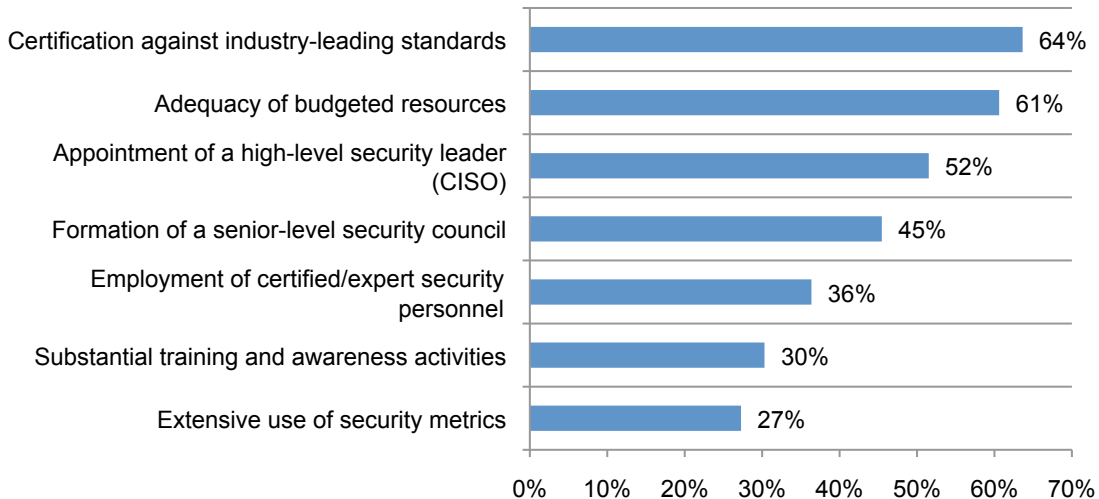
Figure 21 shows the incremental cost savings experienced by companies deploying each one of seven enterprise governance activities. As shown, companies with certification against industry-leading standards save on average 0.89 million Euros. On average, companies employing certified/expert security personnel high-level security leader experience cost savings of 0.55 million Euros. Similar to above, these estimated cost savings are not additive.

Figure 21. Cost savings when deploying seven enterprise governance activities
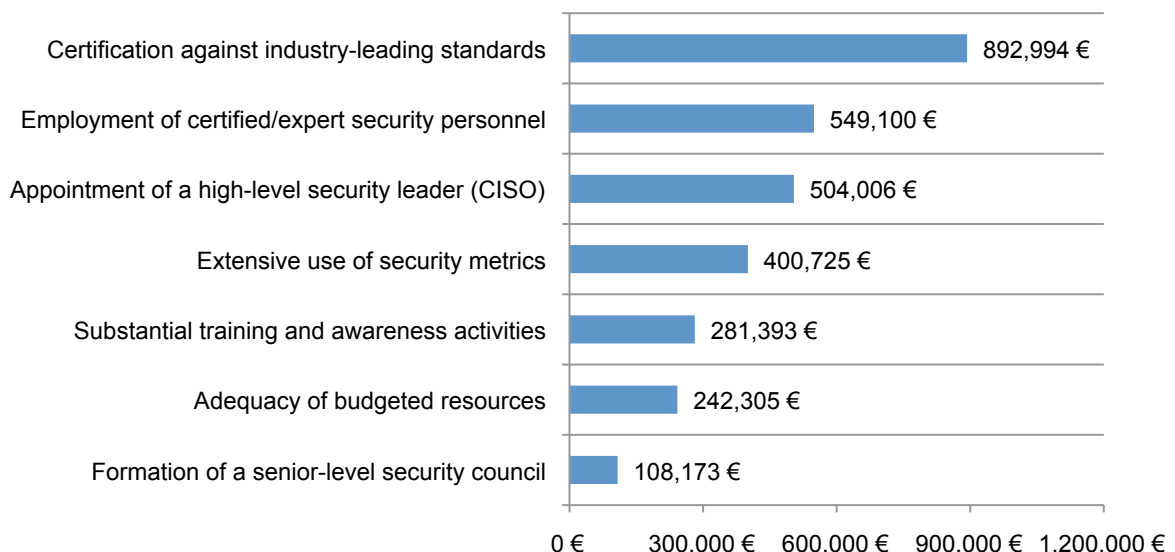
Part 4. Global Findings

Table 4 provides a summary of the total annualized cost of cyber crime for five countries (totaling 199 separate companies). As revealed, there is a significant variation among country samples in terms of total cost. The UK sample reports the lowest and the US sample reports the highest total cost of cyber crime (about a 2.75 X difference).

Table 4: Country analysis	Sample size	Local currency	US$
United States (US)	56	$8,933,510	$8,933,510
United Kingdom (UK)	38	£2,083,165	$3,252,912
Australia (AU)	33	$3,216,891	$3,386,201
Germany (DE)	43	4,840,320 €	$5,950,725
Japan (JP)	29	¥402,820,000	$5,154,447

Figure 22 examines in percentages five external costs or "consequences" of cyber crime for five countries. It clearly shows variation among countries, especially in two categories – that is, business disruption and information loss.

Information loss appears to be a more significant external cost for the US (at 44 percent) and German (40 percent) companies than for the UK (23 percent) and Australia (25 percent). In contrast, business disruption appears to be a more significant external cost for Australian (41 percent) and UK (38 percent) companies than for German (25 percent) and US (30 percent) companies. Finally, Japanese companies rate both business disruption and information loss equally at 36 percent.

Figure 22. Five external costs of cyber crime by country
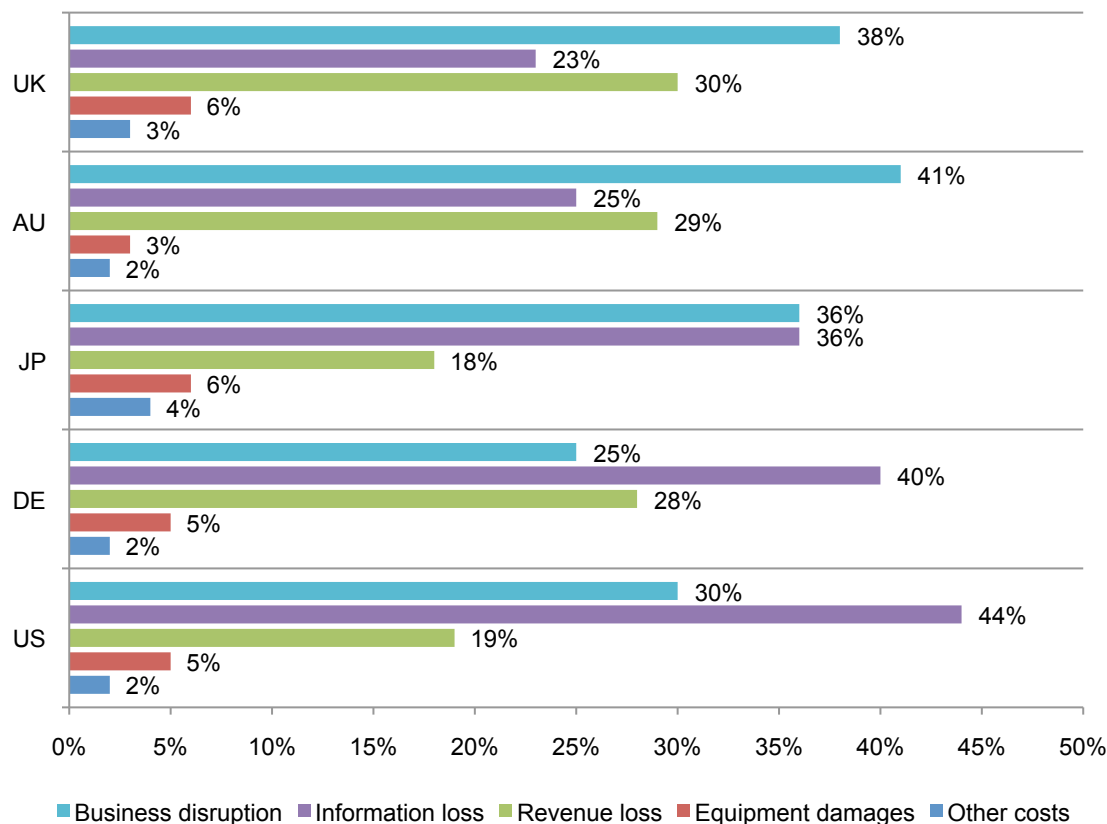
Figure 23 examines five internal or activity cost categories in percentage terms for five countries. It also shows variation among countries, especially in the detection and recovery cost categories. Recovery cost appears to be most significant for UK (35 percent) and Australian (33 percent) companies. Detection cost, appears to be most significant for German companies (33 percent). Finally, Japanese companies rate investigation (20 percent) and incident management (18 percent) at a higher percentage than other countries.

Figure 23. Five internal costs of cyber crime by country

Figure 24 presents the consolidated number of cyber incidents examined within all five countries (including 199 separate co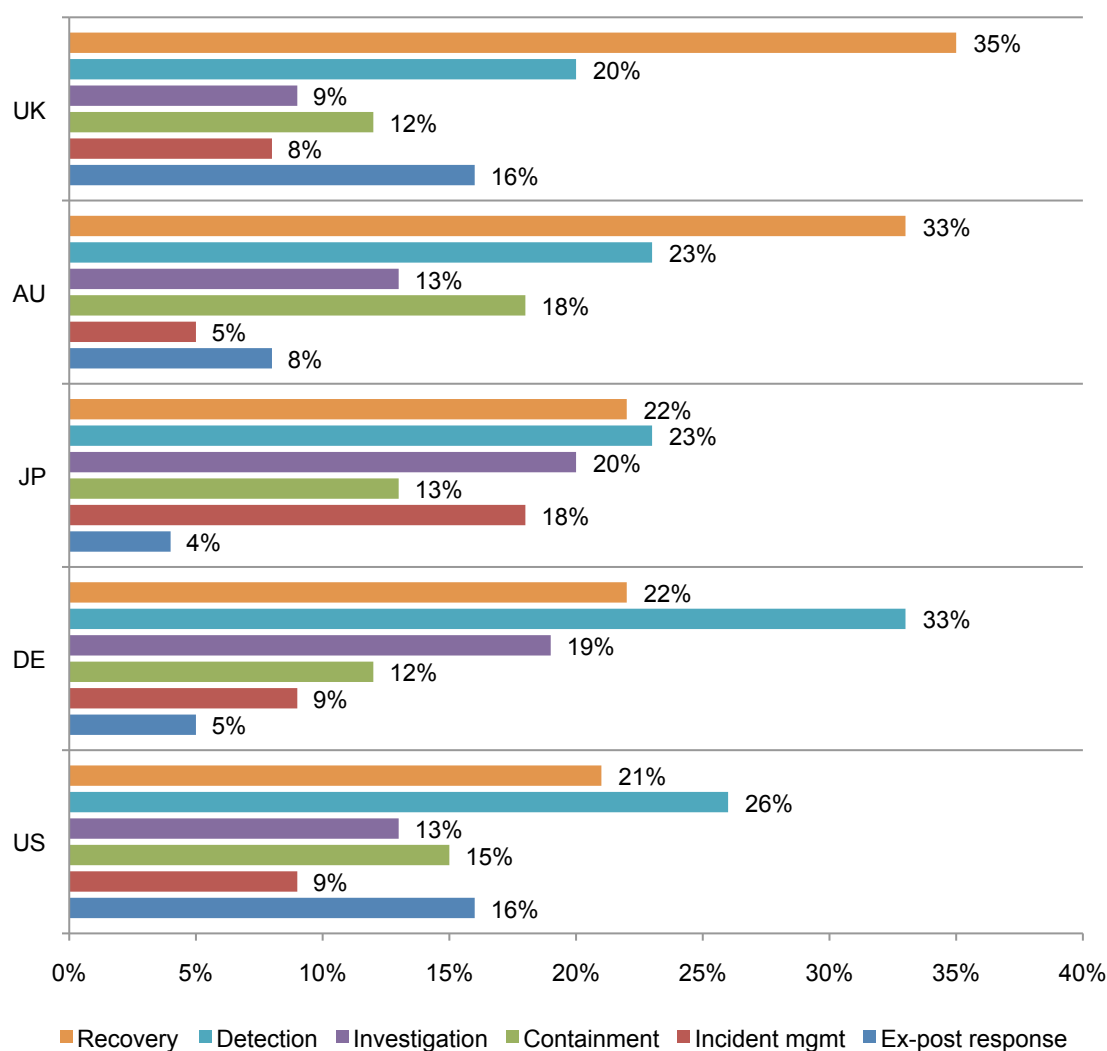mpanies). Our results show virus and malware are the most frequent attack vectors for participating organizations. While at a much lower incident frequency level, our research shows malicious insiders, malicious code, denial of services and web-based incidents are the most costly types of attacks experienced by companies in all countries.

Figure 24. Consolidated number of cyber incidents examined in five country samples
n = 199 separate companies
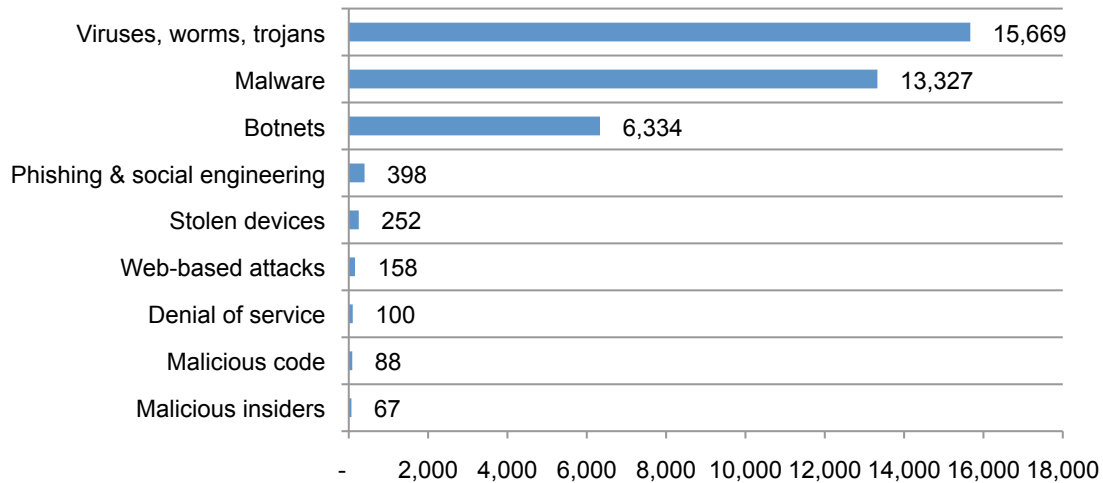
Figure 25 reports the attack frequency adjusted by sample size for the four most expensive types of cyber incidents. As can be seen, companies in the US sample were more likely to experience malicious insiders, malicious code and web-based incidents than other countries. UK and Australian companies appear to be more likely to experience denial of services. Japanese companies appear to be least likely to experience malicious insiders and web-based attacks. German companies are least likely to experience malicious code and denial services.

Figure 25. Adjusted frequency of four types of cyber attacks by country
Each bar shows the total frequency of the attack type divided by sample size
*The US sample shows that web-based attacks were observed more than once for some companies
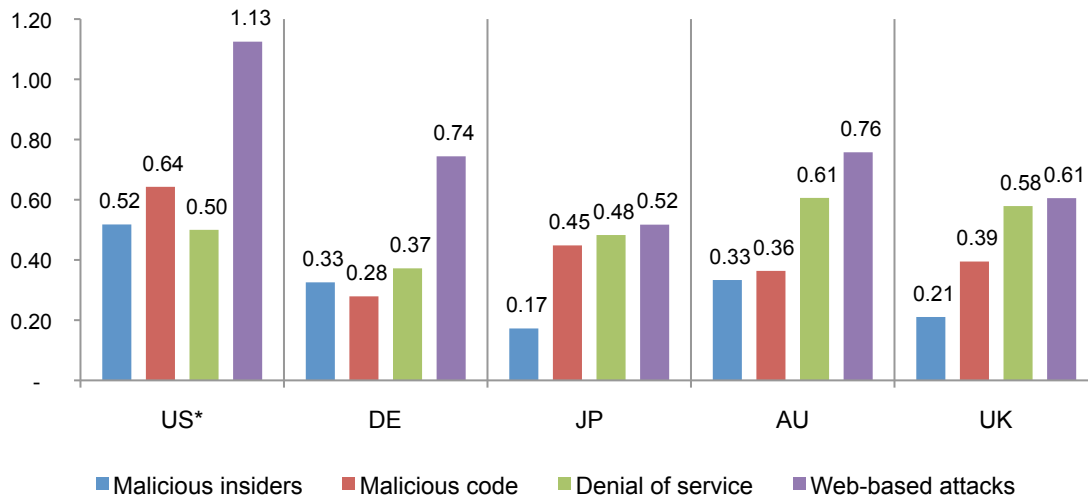
Part 5. Framework

Benchmark results of 43 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.

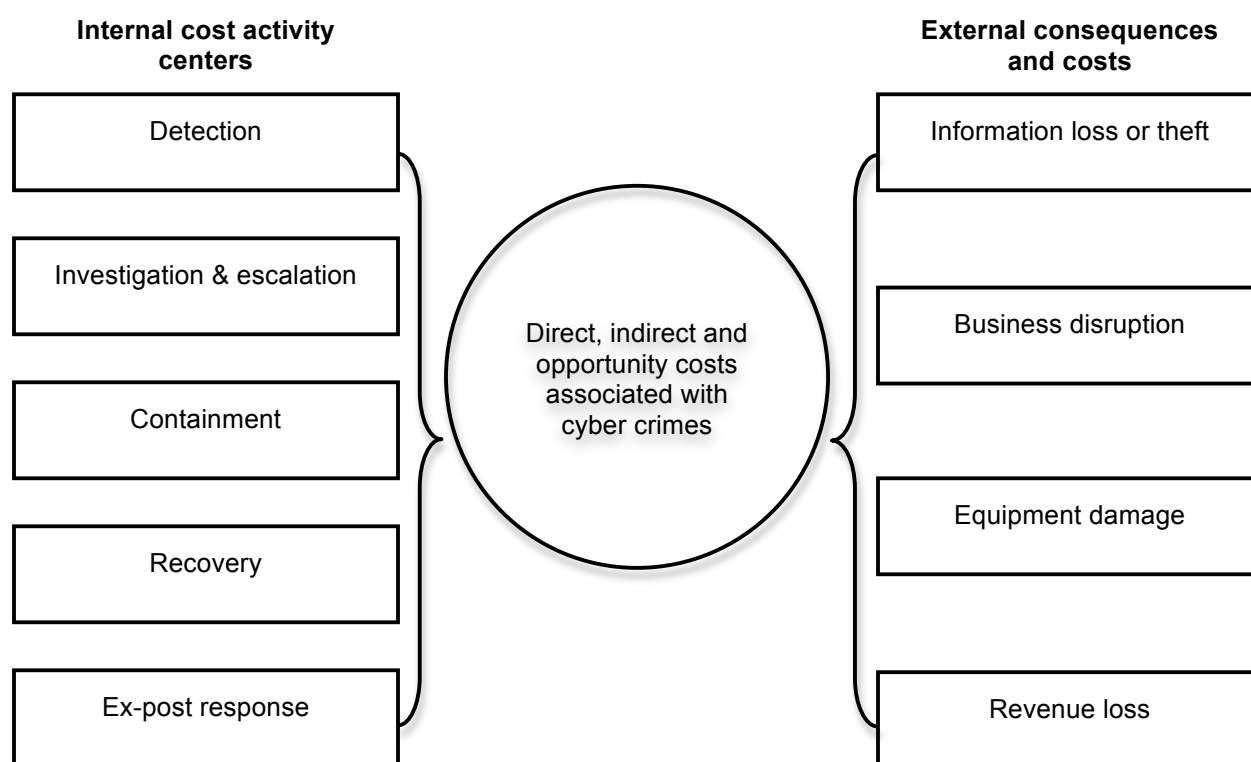The cost framework in Figure 26 presents the two separate cost streams used to measure the total cyber crime cost for each participating organization. These two cost streams pertain to internal security-related activities and the external consequences experienced by organizations after experiencing an 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 26
Cost Framework for Cyber Crime

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

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:[7]

▪ 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.

---

[7] 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 26, 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.[8]

---

[8] 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 6. Benchmark Methods

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

Cost estimation is based on confidential diagnostic interviews with key respondents within each benchmarked organization. Table 5 reports the frequency of individuals by their approximate functional discipline that participated in this year's study. As can be seen, this year's study involved 418 individuals or an average of 9.7 interviews for each benchmarked company.

Table 5: Functional areas of interview respondents	Frequency
IT security	67
Compliance	60
IT operations	55
Data center management	53
Network operations	43
Physical security/facilities mgmt	35
Industrial control systems	29
Human resources	27
Quality assurance	25
Accounting & finance	21
Internal or IT audit	16
Legal	15
Application development	15
Procurement/vendor mgmt	9
Total	418
Interviews per company	9.72

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 | _____|_____ | 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 26 (shown in Part 5) 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 five internal activity centers (see Figure 13). External costs, including the loss of information assets, business disruption, equipment damage and revenue loss, were captured using shadow-costing methods. Total costs were allocated to eight discernible attack vectors.
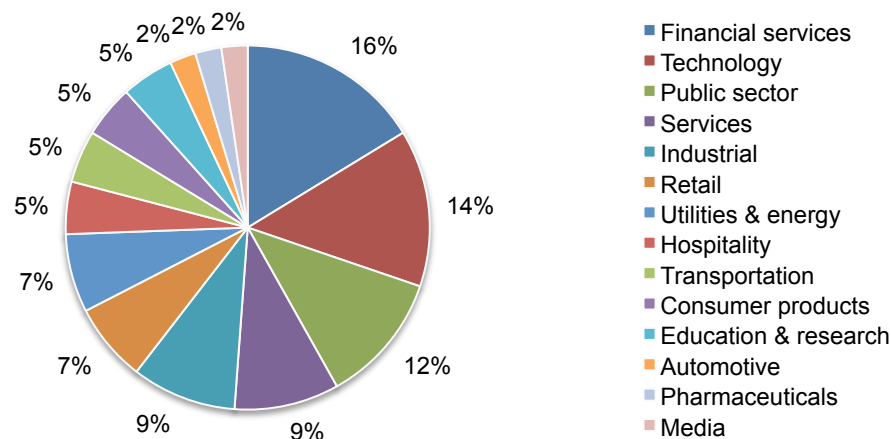
Field research was conducted over a six-month period concluding in August 2012. To maintain consistency across all benchmarked companies, we collected information over four consecutive weeks. The four consecutive weeks for any given organization was not necessarily the same time period as every other organization is this study. The extrapolated direct, indirect and opportunity costs of cyber crime were annualized by dividing the total cost collected over four weeks (ratio = 4/52 weeks).

Part 7. Benchmark Sample

The present study was launched in January 2012. The recruitment started with a personalized letter and a follow-up phone call to 461 German organizations for possible participation in our study.[9] While 65 organizations initially agreed to participate, 43 organizations permitted our researchers to complete the benchmark analysis.

Pie Chart 1 summarizes the current (FY 2012) sample of participating companies based on 14 primary industry classifications. As can be seen, both financial services (16 percent) and technology (14 percent) represent the largest segments. Financial services include retail banking, insurance, brokerage and credit card companies. The technology segment represents organizations in software and IT management.

Pie Chart 1. Industry sectors of participating organizations

Legend:
- Financial services
- Technology
- Public sector
- Services
- Industrial
- Retail
- Utilities & energy
- Hospitality
- Transportation
- Consumer products
- Education & research
- Automotive
- Pharmaceuticals
- Media

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 1,044 seats. The largest enterprise has approximately 95,412 seats.

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

Legend:
- < 2,000
- 2,000 to 5,000
- 5,001 to 10,000
- 10,001 to 15,000
- 15,001 to 25,000
- > 25,000

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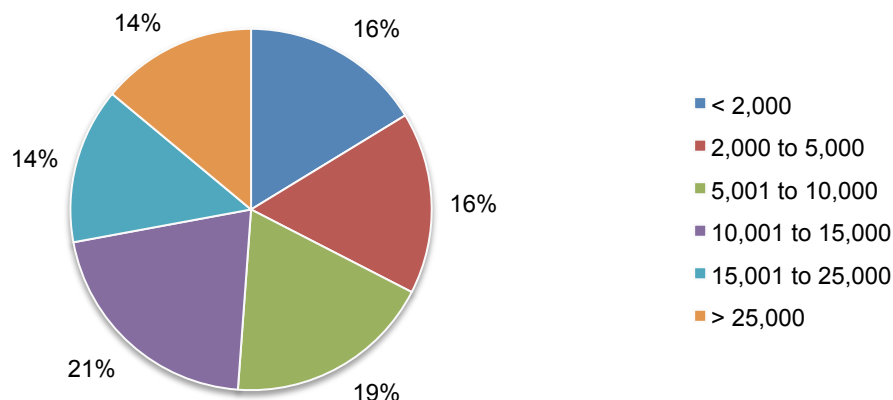
[9]Approximately, half of the organizations contacted for possible participation in this year's study are members of Ponemon Institute's benchmarking community. This community of companies is composed of organizations that have participated in one or more benchmarking studies sometime over the past nine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

Part 8. 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 461 separate organizations, all believed to have experienced one or more cyber attacks. Forty-three 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.

Report Conclusions

The findings of our first German study on the cost of cyber crime provide evidence that companies expend considerable time and resources responding to a plethora of different types of attacks. As in prior years, the most significant costs result from the theft or misuse of information assets. Our findings also suggest that the cost of cyber crime is on the rise.

On a positive note, we found that the cost of any given attack can be substantially reduced by deploying certain security technologies and by advancing good governance practices throughout the company. Finally, despite its stated limitations, this research is encouraging to those who believe in the proposition that good security practices have a positive return on investment.

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.