

Final Document

Sponsored by

Symantec

**2011 Cost of Data Breach Study:
Germany**

Benchmark Research Conducted by

Ponemon Institute LLC

Report: March 2012

2011 Cost of Data Breach Study: Germany

Ponemon Institute, March 2012

Part 1. Executive Summary

Symantec Corporation and the Ponemon Institute are pleased to present *2011 Cost of Data Breach Study: Germany*, our fourth annual benchmark study concerning the cost of data breach incidents for German-based companies. For German organizations the cost of a data breach continues to rise. In 2011 the cost increased from €138 to €146 on a per capita basis.

Ponemon Institute research indicates that data breaches continue to have serious financial consequences on organizations. As in last year's study, we are finding that the September 2009 amendments to the Federal Data Protection Act (*Bundesdatenschutzgesetz* or BDSG) are affecting how German organizations are responding to data breach incidents.

The German data breach notification requirements apply to all companies subject to the German Federal Data Protection Act as well as to companies subject to the German Telecommunications Act (e.g. telecommunications providers and the German Telemedia Act (e.g. website providers)). German DPAs may impose a fine up to €300,000 for failure to provide notification of a data breach or for failing to provide notification correctly, completely, or in a timely manner.

In an effort to reduce administrative burdens and the cost of compliance with data protection laws, including data breach notification, Viviane Reding, European Commissioner for Justice, Fundamental Rights and Citizenship, announced the European Commission's proposal to reform the European Union's data protection framework. Announced in January 2012, the proposed regulation creates a single set of European rules that would be valid everywhere across the EU.¹

Our current analysis of the actual data breach experiences of 26 German companies from 11 different industry sectors takes into account a wide range of business costs, including expense outlays for detection, escalation, notification, and after-the-fact (ex-post) response. We also analyze the economic impact of lost or diminished customer trust and confidence as measured by customer turnover, or churn, rates.

Ponemon Institute conducted its first Cost of a Data Breach study in the United States seven years ago. Since then, we have expanded the study to include Germany, the United Kingdom, France and Australia. This year we are conducting the first *Cost of Data Breach* studies in Italy and India. The initial study established objective methods for quantifying specific activities that result in direct, indirect and opportunity costs from the loss or theft of personal information, thus requiring notification to breach victims as required by law. To maintain consistency from prior years, our methods for quantifying data breach costs has remained relatively constant.

The following are the most interesting findings and implications for organization:

- **The cost of data breach increased.** For the fourth consecutive year, the cost per lost or stolen record has increased. In 2010, the average cost of data breach was €138 and this has increased to €146 in 2011. We define a record as information that identifies an individual and regulations require notification of data breach victims.

The organizational cost has increased slightly from €3.38 in 2010 to €3.40 in this year's study. This very slight increase can be attributed to findings that suggest organizations are more successful in reducing customer churn and the number of records being lost or stolen.

¹ "European Commission Publishes New Framework on Data Protection," IAPP Daily Dashboard, January 25, 2012

- **More customers remain loyal following the data breach.** Fewer customers are abandoning companies that have a data breach. The average abnormal churn decreased from 4.3 percent in 2010 to 3.5 percent this year. However, certain industries, such as industrial and services organizations, are more susceptible to customer churn, which causes their data breach costs to be higher than the average. Taking steps to keep customers loyal and repair any damage to reputation and brand can help reduce the cost of a data breach.
- **Malicious or criminal attacks are the top root cause of a data breach.** Forty-two percent of organizations say that malicious or criminal attacks are the root cause of a data breach and this has increased slightly from 40 percent in 2010. This type of breach is also the most costly. Accordingly, organizations need to focus on processes, policies and technologies that address threats from the malicious insider or hacker. Thirty-eight percent of data breaches involved negligent employees or contractors. Only 19 percent say the breach was due to an IT or business process failure.
- **Lost business costs declined from €1.50 million in 2010 to €1.33 million in 2011.** These costs refer to abnormal turnover of customers (a higher than average loss of customers for the industry or organization), increased customer acquisition activities, reputation losses and diminished goodwill. During the five years we studied this aspect of a data breach, the lowest cost for lost business was €770,000 in 2008.
- **Certain organizational factors reduce the overall cost.** If the organization has a CISO with overall responsibility for enterprise data protection the average cost of a data breach can be reduced as much as €76 per compromised record. A quick response and the use of consultants assisting with the breach response also can save as much as €29 and €16 per record, respectively. When considering the average number of records lost or stolen, all of these factors can provide significant and positive financial benefits. Specific attributes or factors of the data breach also can increase the overall cost. Data breaches caused by third parties or a lost or stolen device increased the cost by €35 and €33, respectively. A first time breach also increases the cost by €34.
- **Detection and escalation costs are higher.** Detection and escalation costs increased very slightly from approximately in €750,000 in 2010 to €890,000 this year. These costs refer to activities that enable a company to detect the breach and whether it occurred in storage or in motion. Controlling these costs suggests that organizations have the appropriate processes and technologies to execute these activities.
- **Notification costs increase slightly.** Notification refers to the steps taken to report the breach of protected information to appropriate personnel within a specified time period. The costs to notify victims of the breach increased in this year's study from approximately €220,000 to €230,000.

Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a nine-month period. Recruiting organizations for the 2011 study began in January 2011 and interviews were completed in December. In each of the 26 participating organisations, we spoke with IT, compliance and information security practitioners who are knowledgeable about their organization's data breach and the costs associated with resolving the breach. For privacy purposes we do not collect any organization-specific information.

How do you calculate the cost of a data breach?

To calculate the average cost of data breach, we collect both the direct and indirect expenses paid by the organisation. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished acquisition rates. For a detailed explanation about Ponemon Institute's benchmark methodology, please see Part 4 of this report.

How does benchmark research differ from survey research? The unit of analysis in the *Cost of Data Breach* study is the organization. In survey research, the unit of analysis is the individual. As discussed previously, we recruited 26 organizations to participate in this study.

Can the average cost of a data breach be used to calculate the financial consequences of a mega breach such as the ones experienced by Sony or Epsilon?

The average cost of data breach in our research does not apply to catastrophic breaches. Primarily because these are not typical of the breaches most organizations experience. In order to be representative of the population of German organizations and draw conclusions from the research that can be useful in understanding costs when protected information is lost or stolen, we do not include data breaches of more than 100,000 compromised records.

Are you tracking the same organizations each year?

Each annual study involves a different sample of companies. In other words, we are not tracking the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach. Since starting this research in 2008, we have studied the data breach experiences of 91 German organizations.

Part 2. Key Findings

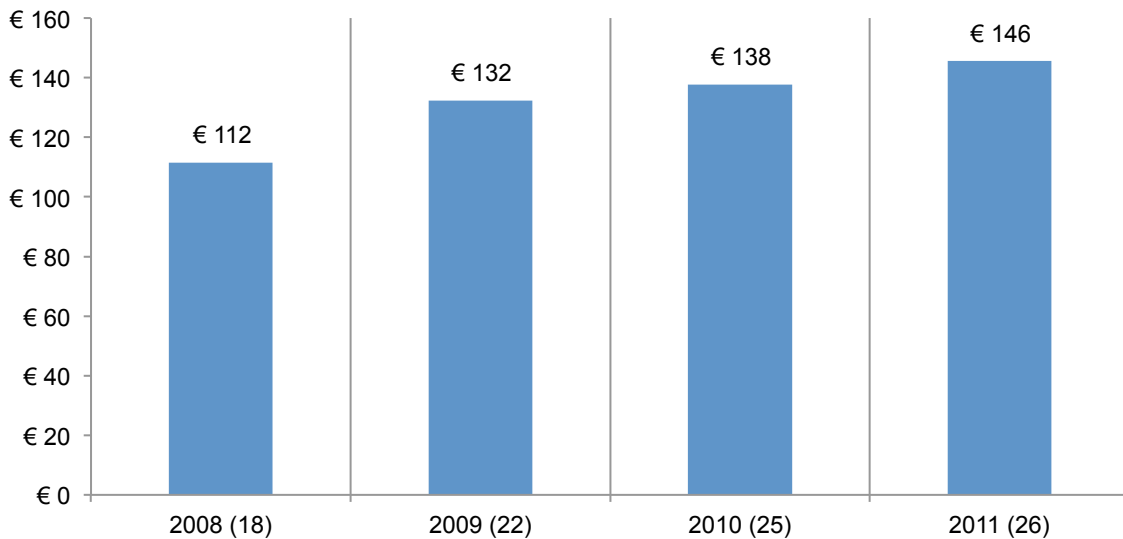
In this section we provide the detailed findings of this research. Topics are presented in the following order:

- Cost of data breach: per record, organizational and industry
- Root causes of a data breach
- Attributes that influence the cost of data breach
- Trends in the frequency of compromised records
- Trends in customer turnover or churn
- Trends in the following costs: detection and escalation, notification, lost business, direct and indirect and post data breach

The cost of data breach increases. Figure 1 reports the average per capita cost of a data breach.² As can be seen, for four consecutive years the average per capita cost has increased. According to this year's benchmark findings, data breaches cost companies an average of €146 per compromised record – of which €75 pertains to indirect costs including abnormal turnover or churn of existing and future customers. Last year's average per capita cost was €138 with an average indirect cost of €72.

Figure 1: The average per capita cost of data breach over four years

Bracketed number defines the benchmark sample size

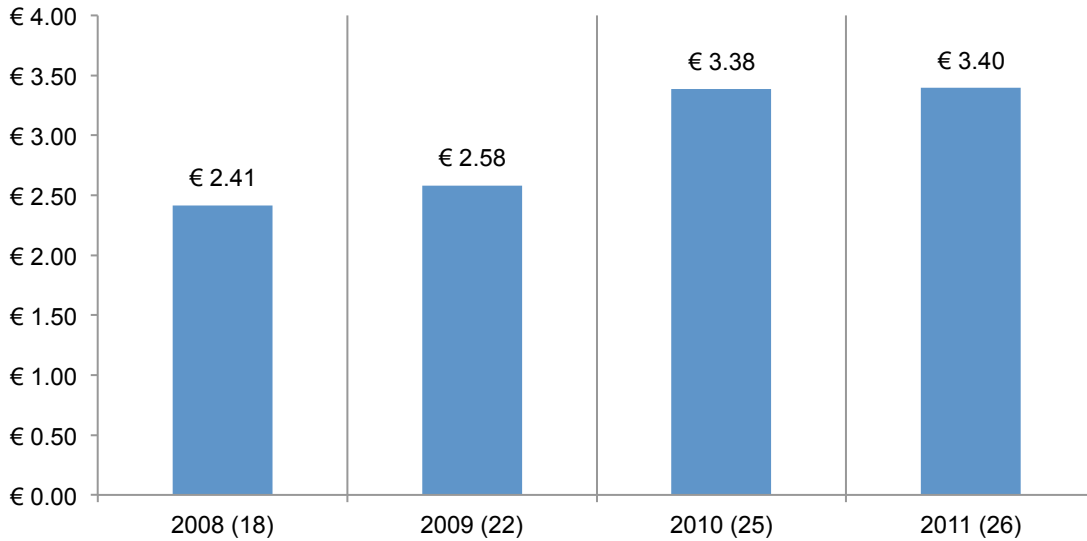


²Per capita cost is defined as the total cost of data breach divided by the size of the data breach in terms of the number of compromised records.

The total average cost of data breach over four years is shown in Figure 2. The total cost of data breach increased very slightly from €3.38 million to €3.40 million – or, a .03% percent increase between 2010 and 2011 results.

Figure 2. The average total organizational cost of data breach over four years

€000,000 omitted



Metrics reveal improvements in customer churn. Figure 3 reports four key metrics that show mixed results. Despite increasing per capita cost, the average total cost of a data breach increased by only a nominal amount (.3 percent). The 18 percent decrease in abnormal churn rate suggests organizations have improved their response to data breach and they are more successful in retaining the loyalty of consumers and customers. The average data breach size has declined by 5 percent, suggesting fewer records are being lost or stolen.

Figure 3: Key metrics in understanding organizational cost of a data breach

Net change defined as the difference between the 2011 and 2010 results

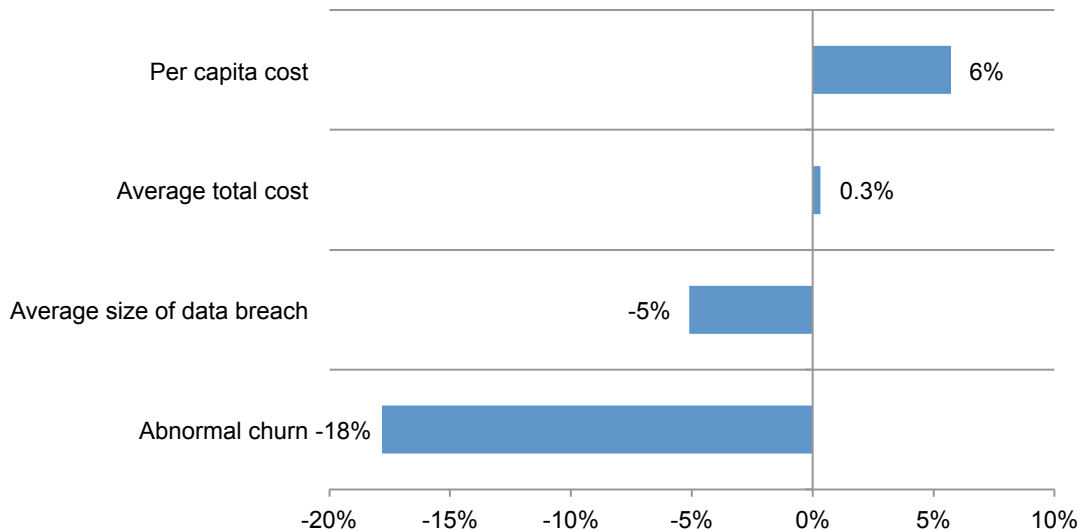
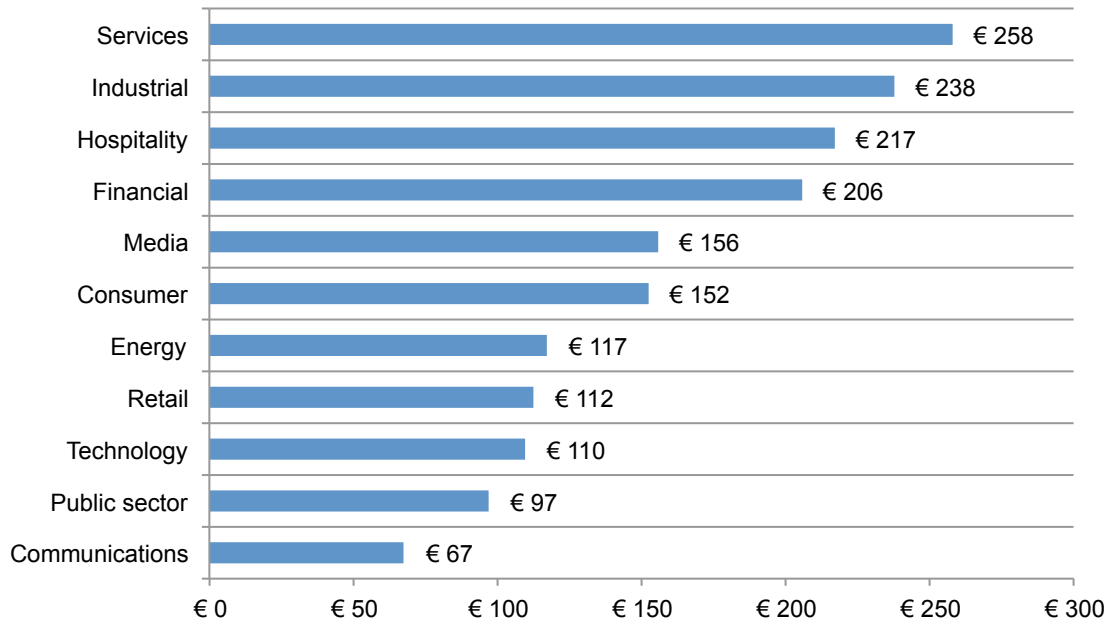


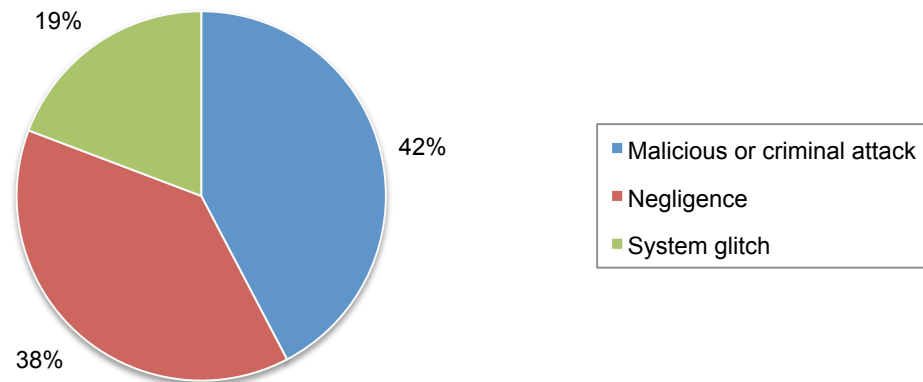
Figure 4 reports the per capita costs for the 2011 study by industry classification. While small sample size prevents us from generalizing industry cost differences, the pattern of 2011 industry results is consistent with prior years. Accordingly, financial service companies tend to have a per capita cost above the mean (€206) and retail companies have a per capita cost below the mean (€112).

Figure 4. Per capita cost by industry classification of benchmarked companies



Malicious or criminal attacks are most often the cause of a data breach. Figure 5 provides a summary of the main root causes of a data breach for all 26 organizations. Forty-two percent experienced a malicious or criminal attack.³ Thirty-eight percent of incidents involved a negligent employee or contractor, and 19 percent involved system glitches, including a combination of both IT and business process failures.

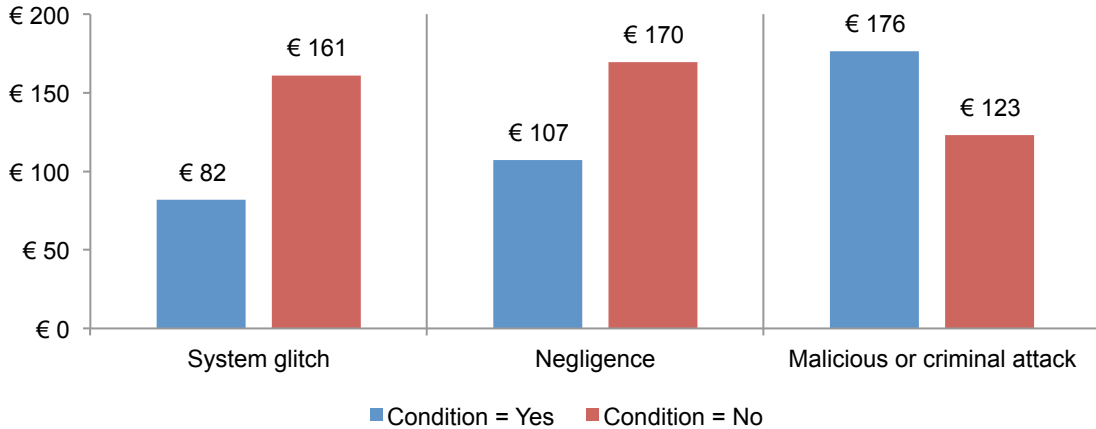
Figure 5. Distribution of the benchmark sample by root cause of the data breach



³Malicious and criminal attacks increased slightly from 40 percent in our 2010 study.

Malicious attacks are most costly. Hackers or criminal insiders (employees, contractors and other third parties) typically cause the data breach as determined by the post data breach investigation. Figure 6 reports per capita cost of data breach for three conditions or root causes of the breach incident. Again, the pattern of results in 2011 is consistent with prior years' research, wherein the most costly breaches typically involve malicious acts against the company rather than negligence or system glitches. Accordingly, companies that experience malicious or criminal attacks have the highest per capita cost (€176), and companies experiencing system glitches have the lowest per capita cost (€82). Negligence results in a per capita cost of €107, which is substantially below the overall mean of €146.

Figure 6. Per capita cost for three root causes of the data breach

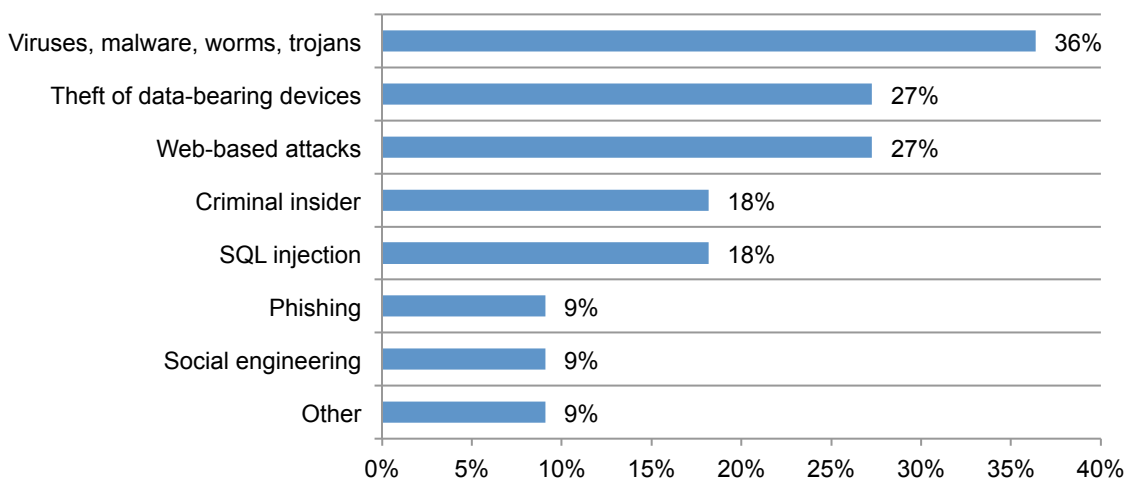


Criminal attacks are mainly electronic agents. In this year's report, we analyzed the findings from the 11 organizations that report their data breach was caused by a malicious insider or hacker as previously described. Figure 7 summarizes the types of criminal attacks experienced. Please note that a given company might have experienced two or more of these attacks.

Thirty-six percent of the subsample experienced electronic agents such as viruses, malware, worms and trojans. Other major conditions include the theft of data-bearing devices and web-based attacks (both at 27 percent).

Figure 7. Analysis of malicious or criminal attacks experienced by 11 companies

More than one attack type may exist for each company



Six positive and negative attributes can influence the cost of a data breach. Over the years of conducting this research, we have identified six attributes that can influence the cost of a data breach. The percent of organizations that have these attributes is shown in Figure 8.

- **The organization notified data breach victims quickly.** Forty-six percent say their organizations responded and provided notice about the data breach within 30 days of discovery.
- **CISO (or equivalent title) has overall responsibility for enterprise data protection.** Thirty-eight percent of participating organizations have centralized the management of data protection with the appointment of a C-level security professional.
- **The organization had its first data breach.** Thirty-eight percent say the incident was their first data breach involving 1,000+ records.
- **Consultants are engaged to help remediate the data breach.** As can be seen, 35 percent say their organizations engaged a consultant to assist in the data breach response or remediation.
- **The data breach involved lost or stolen devices.** Thirty-one percent say the incident involved one or more lost or stolen data-bearing devices – which included laptops, smartphones, tablets and servers.
- **Data was lost or stolen due to a third-party flub.** Thirty-one percent say their data breach involved one or more third parties – including outsourcers, cloud providers and business partners.

Figure 8. Defining attributes for the benchmark sample

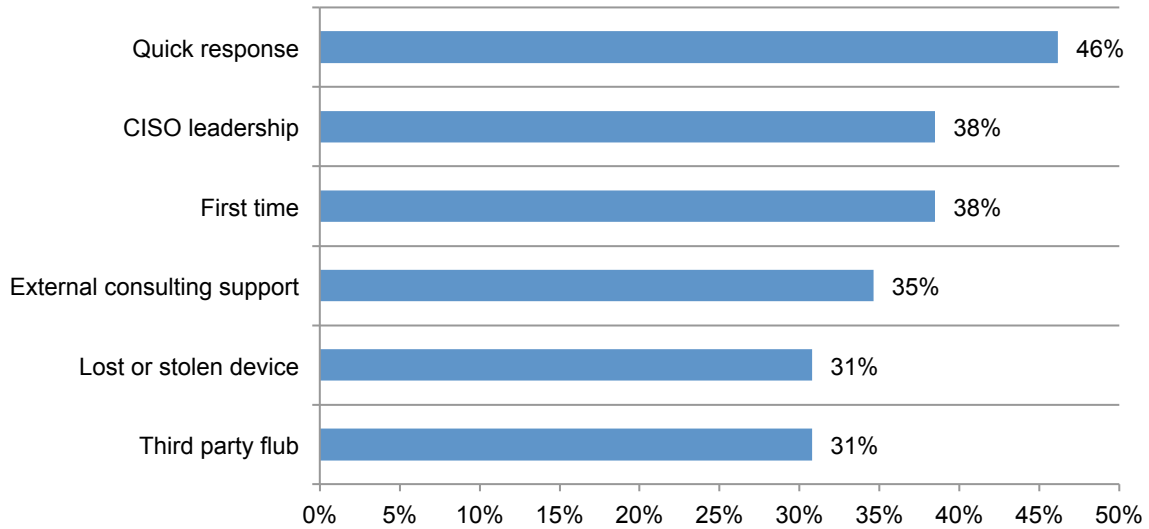


Figure 9 summarizes the per capita costs for six normatively important conditions or attributes about the benchmark sample. As previously mentioned, these attributes were selected based on learned experiences from previous cost benchmark studies.

Per capita costs are above the mean for third party mistakes, those experiencing lost or stolen devices and those experiencing a major data breach involving 1,000+ records for the first time. Per capita costs are below the mean for organizations that have the following: a CISO in-charge of data protection efforts, quick response to the breach event and external consultants to assist in data breach investigation, containment and/or remediation.

Figure 9. Per capita cost for six attributes or conditions

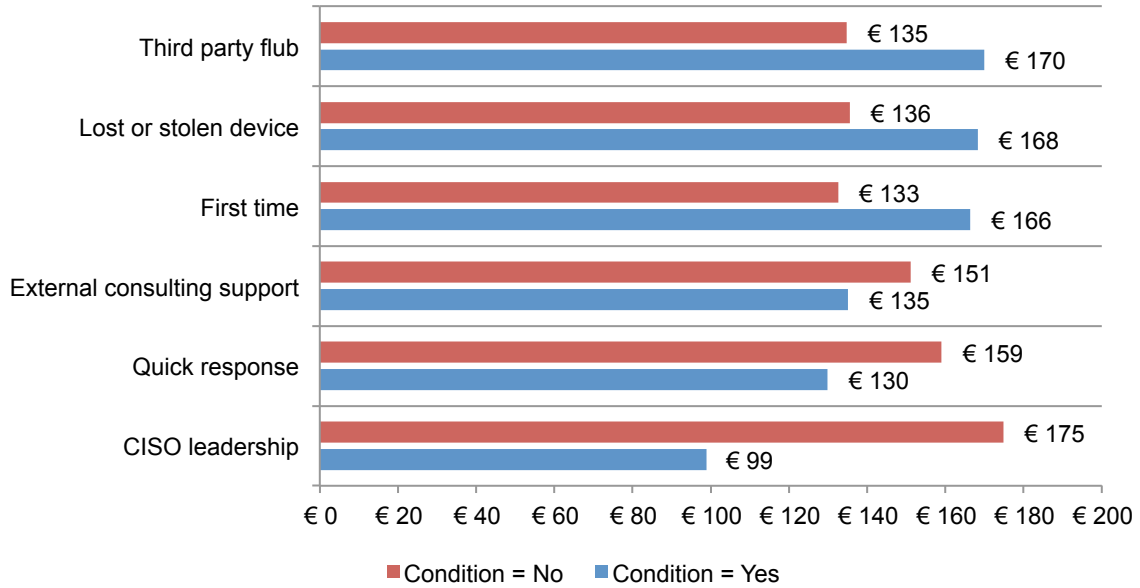


Figure 10 summarizes the per capita cost differences for six important conditions or attributes about the benchmark sample. In this analysis, a negative difference means that the attribute or condition moderates or lessens data breach costs. A positive difference has the opposite effect.

As can be seen, organizations that employ a CISO with enterprise-wide responsibility for data protection experience a €76 cost saving per compromised Organizations that respond quickly to the data breach incident appear to have a lower per capita cost (€29). Finally, organizations engaging an external consultant enjoy a €16 per capita cost saving.

Figure 10. Per capita cost differences for six attributes or conditions

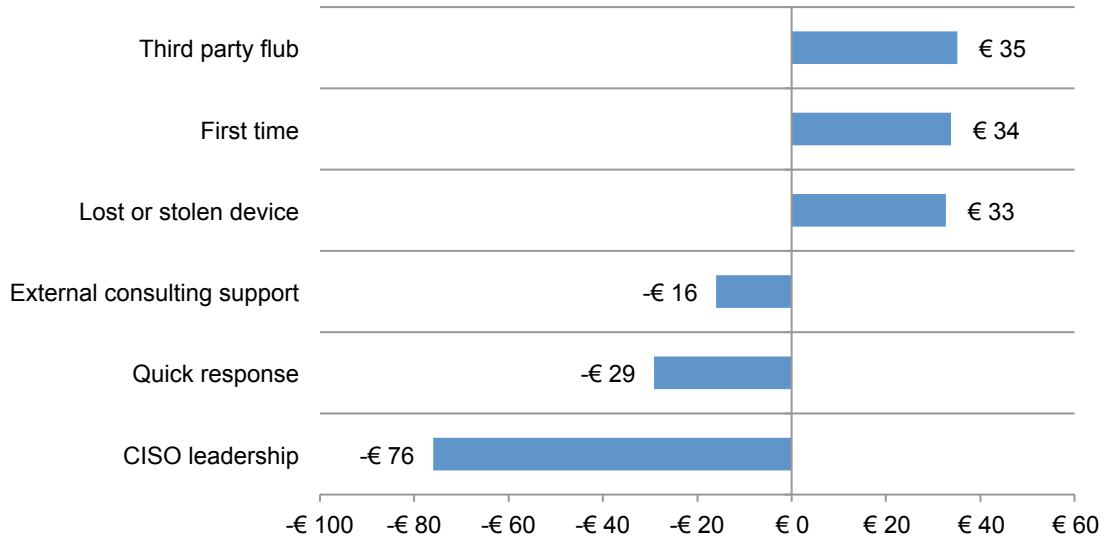
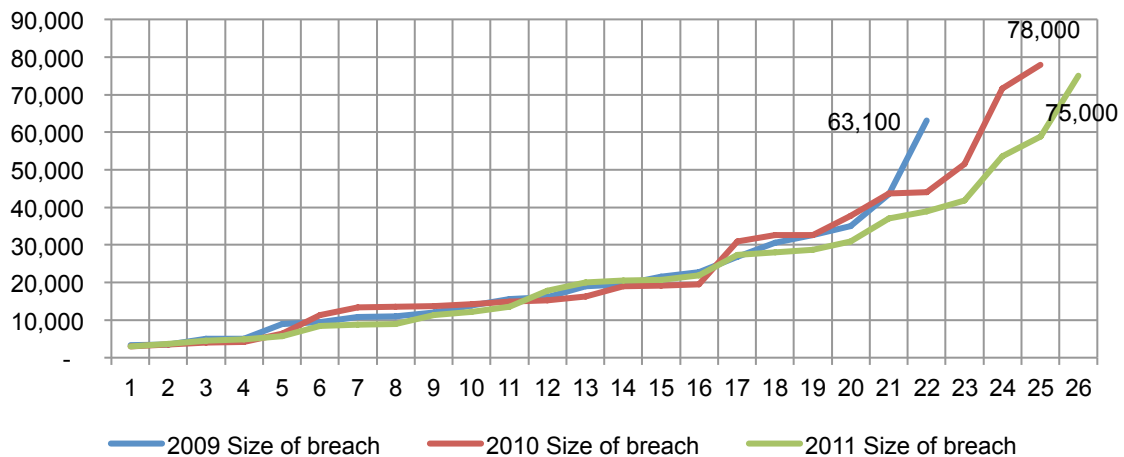


Figure 11 shows, in ascending order, the number of lost or stolen records involved in data breach incidents included in studies conducted over the past three years. According to the figure, the number of compromised records has remained consistent since 2009. The benchmark samples do not contain data breach incidents involving millions of compromised records. In our experience, these so-called “mega breaches” are rare events and including them would skew results. The largest data breach incident in this year’s study involved 75,000 records.

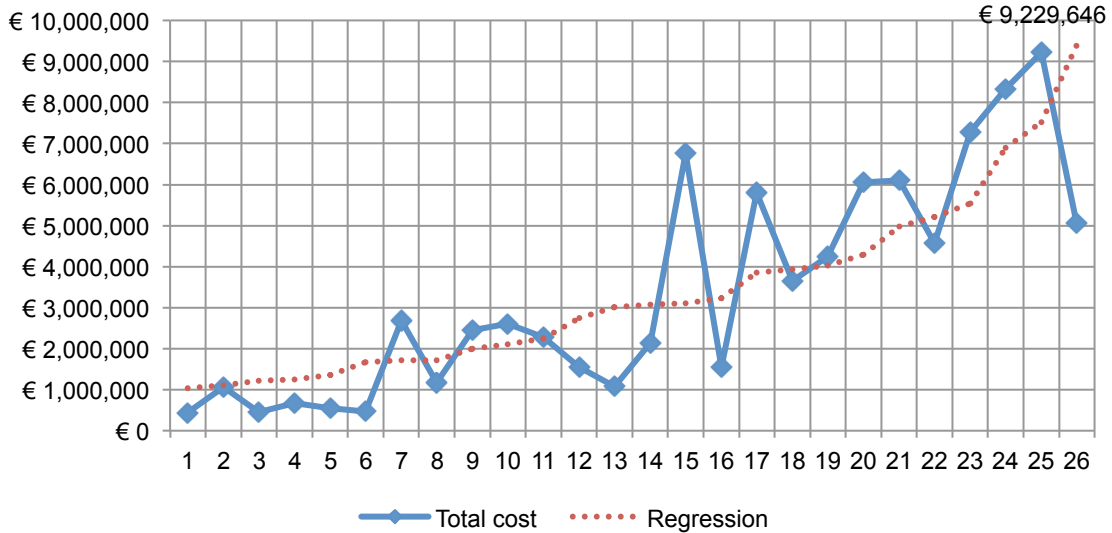
Figure 11. Ascending frequency of compromised records over three years



The more records lost, the higher the cost of the data breach. Figure 12 shows the relationship between the total cost of a data breach and the size of the incident for 26 benchmarked companies in ascending order by the size of the breach incident. The regression line clearly indicates that the size of the data breach incident and total costs are linearly related. In this year's study, the cost ranged from €443,395 to €9,229,646.

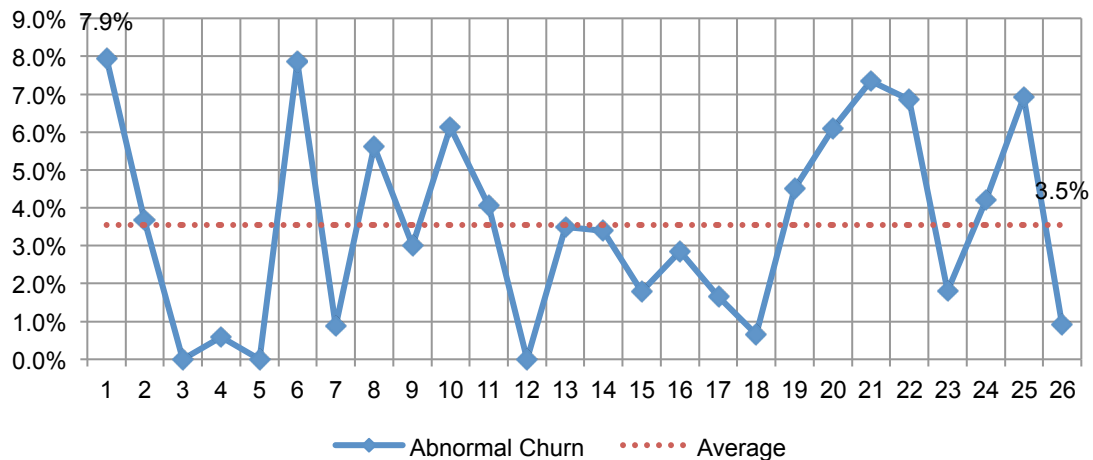
Figure 12. Total cost of data breach by size of lost or stolen records

Regression = Intercept + {Size of Breach Event} x β , where β denotes the slope.



More customers remain loyal to organizations following a data breach. Figure 13 shows the abnormal churn rates for each one of the 26 organizations included in this research. As shown, the churn rate distribution is varied, with a range of 0 (no abnormal churn) to 7.9 percent. It is important to note that the average abnormal churn decreased from 4.3 percent in the 2010 study to 3.5 percent this year.

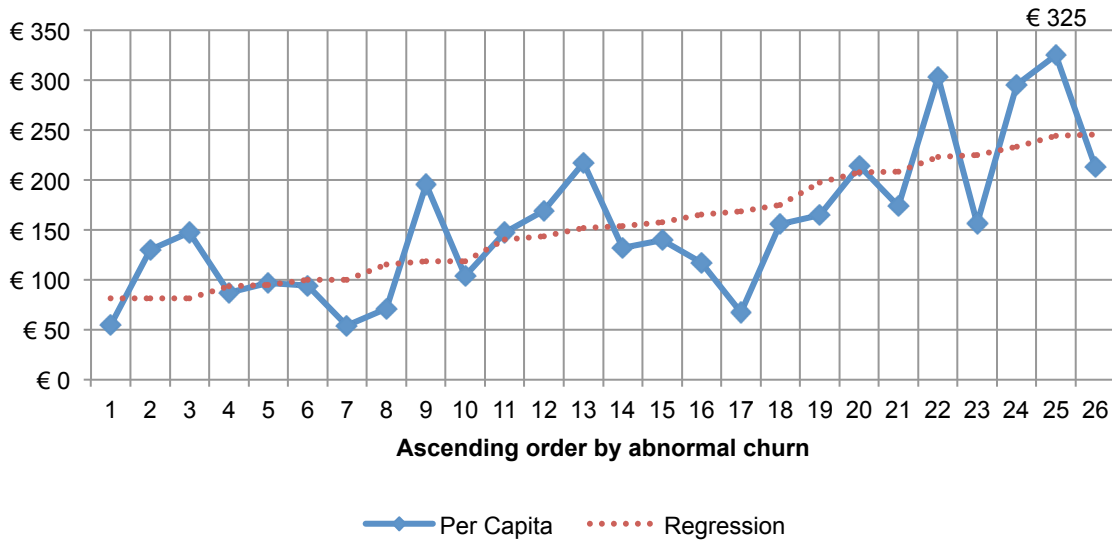
Figure 13. Distribution of abnormal churn rates for 26 benchmark companies



The more churn, the higher the cost of data breach. Figure 14 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is upward sloping, which suggests that abnormal churn is linearly related to cost. This pattern of results is consistent with benchmark studies completed in prior years.

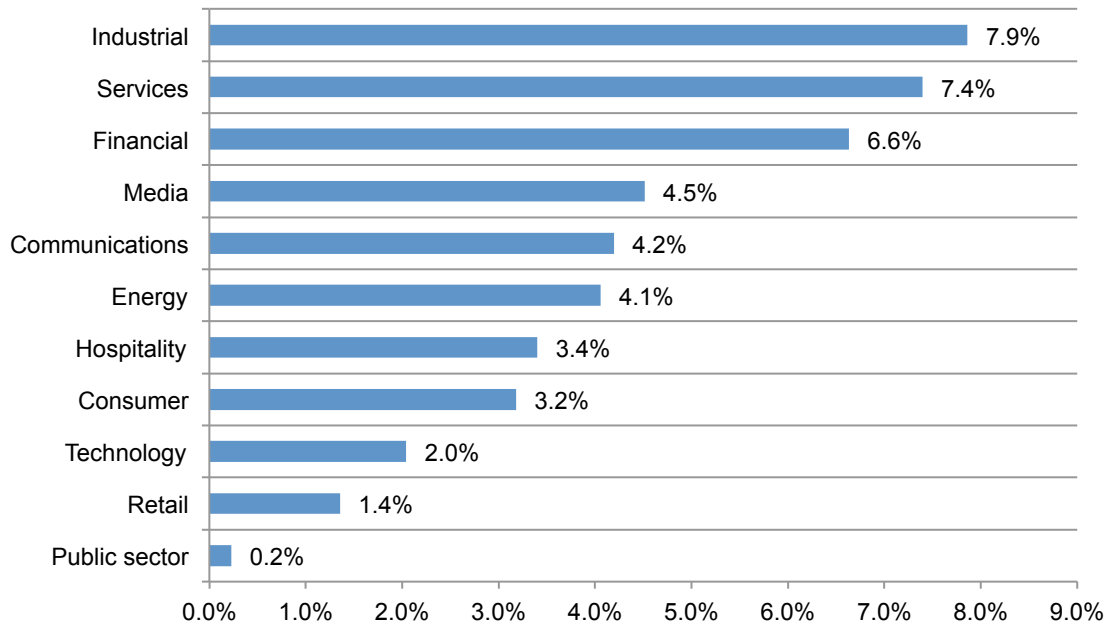
Figure 14. Distribution of per capita costs in ascending value of abnormal churn rates

Regression = Intercept + {Abnormal Churn} x β , where β denotes the slope.



Certain industries are more vulnerable to churn. Figure 15 reports the abnormal churn rate of benchmarked organizations for the 2011 study. While small sample size prevents us from generalizing the affect of industry on data breach cost, our 2011 industry results are consistent with prior years – wherein financial service organizations tend to experience relatively high abnormal churn and retail companies tend to experience a relatively low abnormal churn.⁴ In this year’s study, industrial and service companies realize the two highest churn rates. The lowest churn rate occurs in public sector organizations.

Figure 15. Abnormal churn rates by industry classification of benchmarked companies

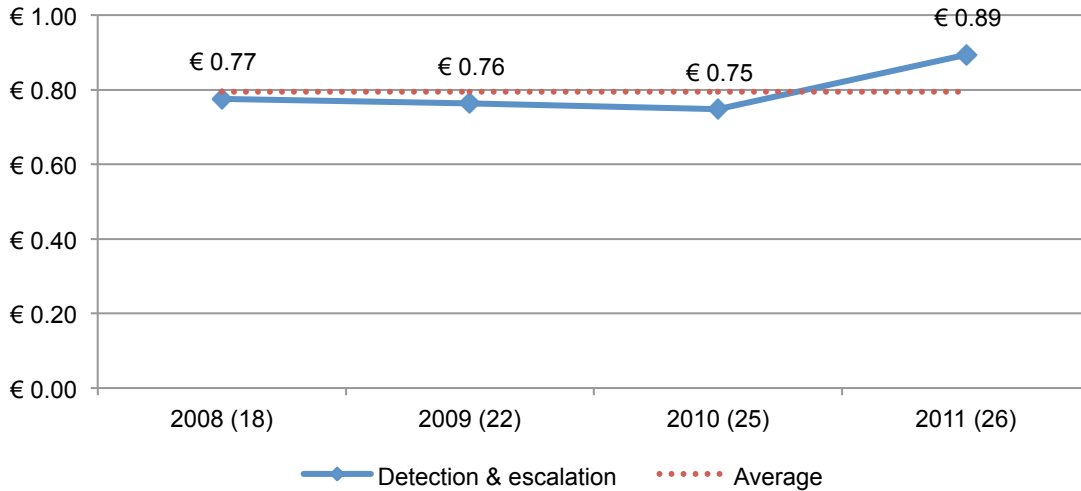


⁴Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have a alternative choice.

Detection and escalation costs are higher this year. Figure 16 shows the distribution of costs associated with detection and escalation of the data breach event. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. As noted, average detection and escalation costs increased from €747,471 in 2010 to €893,409 in the present study.

Figure 16. Average detection and escalation costs over four years

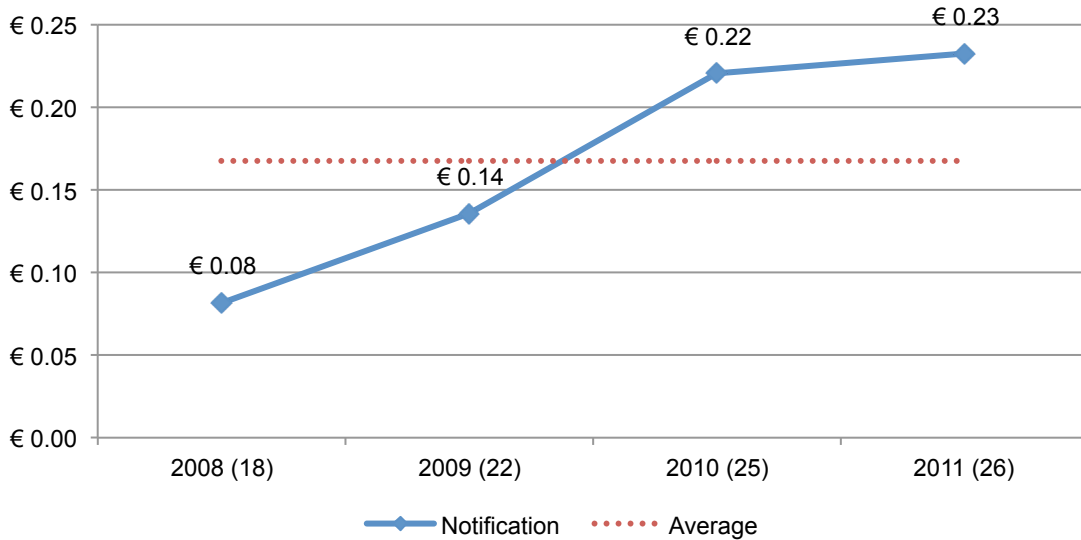
€000,000 omitted



Notification costs increase slightly. Figure 17 reports the distribution of costs associated with notification activities. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up. This year's average notification is €232,517, which is the highest value over four years. This represents an increase from €220,651 in 2010.

Figure 17. Average notification costs over four years

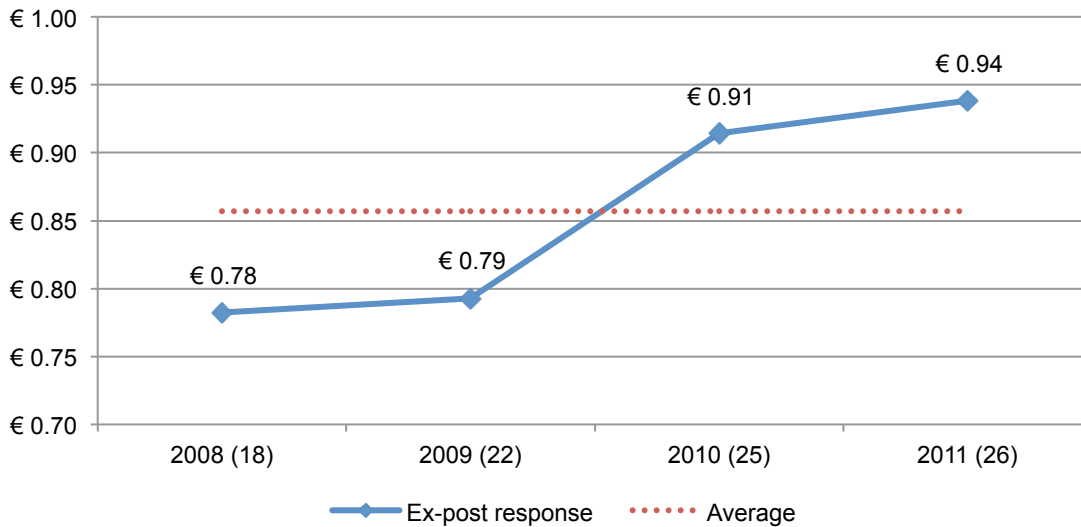
€000,000 omitted



Post data breach costs increase. Figure 18 shows the distribution of costs associated with ex-post (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex-post response cost increased from €914,170 in 2010 to a four-year high of €938,534 in this year's study.

Figure 18. Average ex-post response costs over four years

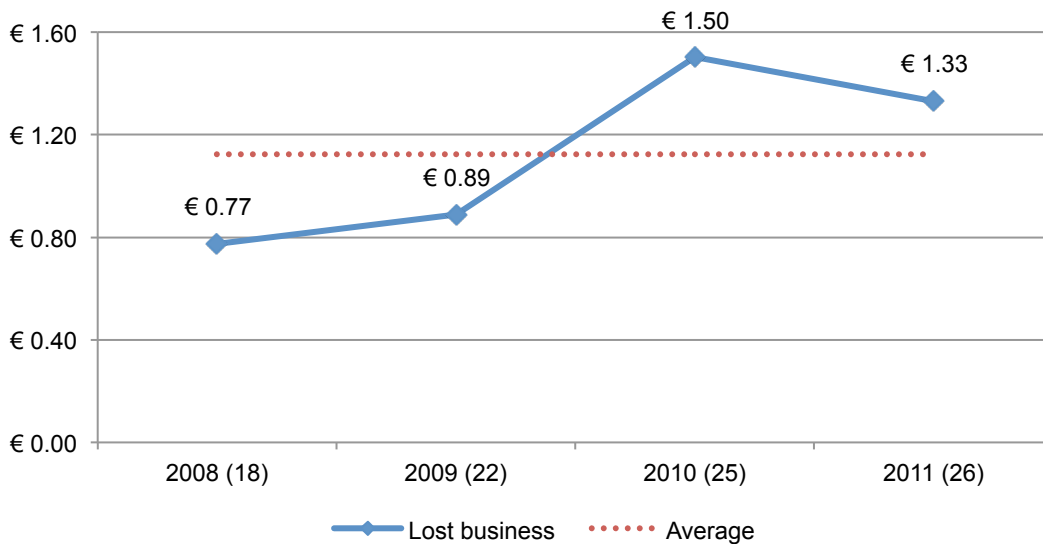
€000,000 omitted



Lost business costs declined. Figure 19 reports lost business costs associated with data breach incidents over four years. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen below, lost business costs decreased from a four-year high of €1,502,115 in 2010 to €1,331,003 in 2011.

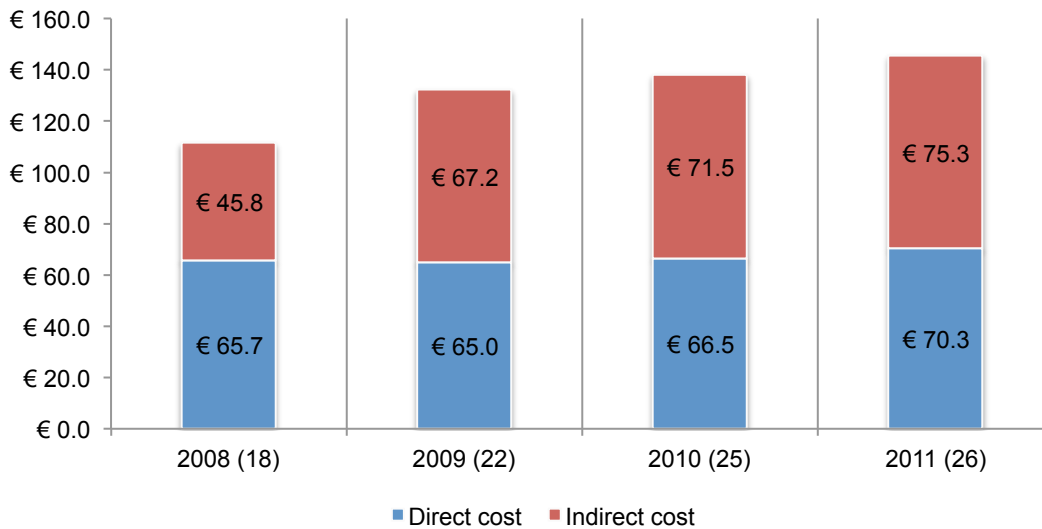
Figure 19. Average lost business costs over four years

€000,000 omitted



Both direct and indirect costs increased. Figure 20 reports the direct and indirect cost components of data breach on a per capita basis. In essence, the cost of data breach per compromised record increased by more than €8 – from €138 in 2010 to €146 in 2011. Approximately, €4 of this increase pertains to direct cost. In the present study, indirect cost represents 48 percent of total per capita cost, which is identical to the 2010 indirect cost percentage.

Figure 20. Direct and indirect per capita data breach cost over four years



We measured the security posture of each participating company using the Security Effectiveness Score (SES) as part of the benchmarking process.⁵ Figure 21 reports the SES Index for 26 organizations. 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 +1.68 to a low of -1.82, with a mean value at +0.25.

Figure 21. Distribution of Security Effectiveness Scores for 26 benchmark companies

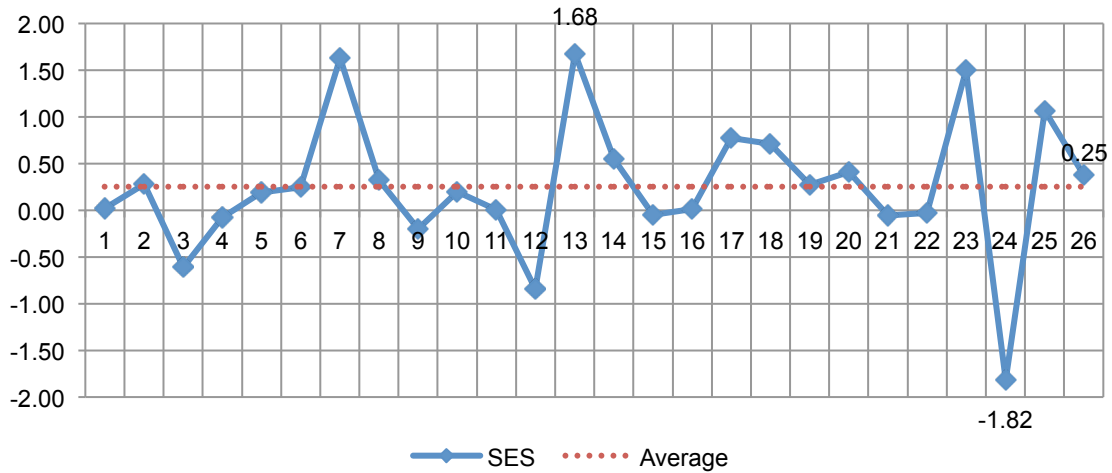
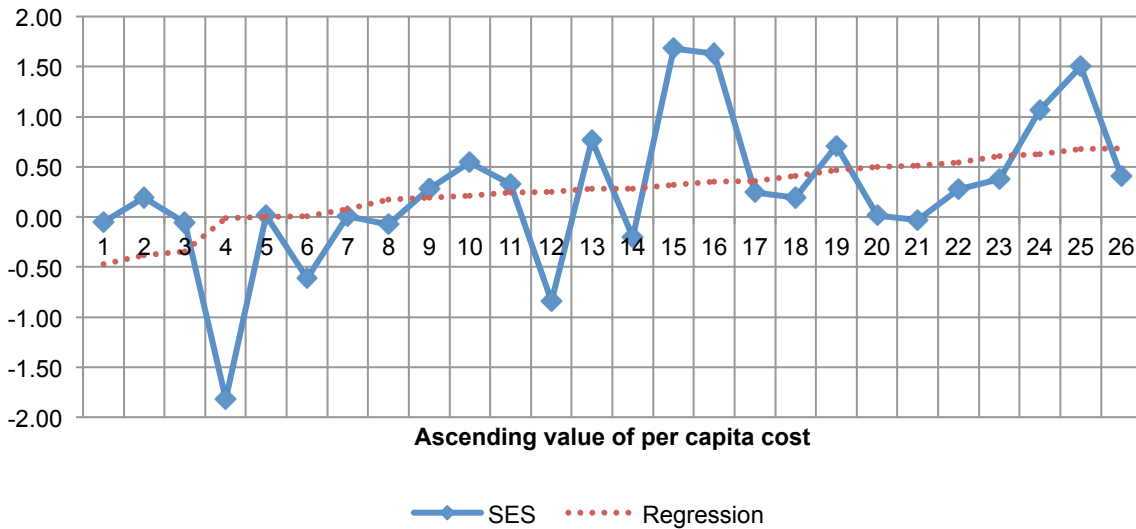


Figure 22 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is upward sloping, suggesting that the security effectiveness score (SES) for each organization is inversely related to their per capita data breach cost. In other words, a strong security posture appears to moderate data breach costs.

Figure 22. Security Effectiveness Score (SES) in ascending value of per capita cost

Regression = Intercept + {Per Capita Cost} x β , where β denotes the slope.



⁵ The Security Effectiveness Score was developed by 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 40 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.

After the Breach

In addition to measuring specific cost activities relating to the leakage of personal information, we report in Table 1 the preventive measures implemented by companies after the data breach. The top preventive measures or steps taken after the data breach are: the implementation of endpoint security solutions (68 percent), the expanded use of encryption (65 percent), the instillation of security intelligence systems such as SIEM (62 percent), the strengthening of perimeter controls (61 percent) and the deployment of DLP solutions (56 percent).

Table 1. Preventive measures and controls implemented after the data breach	2009	2010	2011
Endpoint security solutions	59%	75%	68%
Expanded use of encryption	77%	70%	65%
Security intelligence systems	68%	58%	62%
Strengthening of perimeter controls	73%	69%	61%
Data loss prevention (DLP) solutions	59%	51%	56%
Security certification or audit	41%	34%	45%
Identity and access management solutions	27%	24%	30%
Training and awareness programs	27%	26%	23%
Manual control practices	14%	11%	9%

*Please note that a company may be implementing more than one preventive measure.

Table 2 provides the percentage changes for 11 cost categories over four years. As can be seen, most cost categories appear to be relatively stable over time. The two highest cost categories pertain to investigation and forensics and lost customer business.

Table 2. Cost changes over four years	2008	2009	2010	2011
Investigations & forensics	31%	29%	29%	32%
Audit and consulting services	10%	8%	9%	10%
Outbound contact costs	9%	10%	10%	9%
Inbound contact costs	6%	6%	6%	5%
Public relations/communications	1%	1%	1%	0%
Legal services – defense	2%	3%	3%	2%
Legal services - compliance	4%	4%	4%	6%
Free or discounted services	2%	1%	1%	1%
Identity protection services	0%	0%	0%	1%
Lost customer business	29%	32%	33%	29%
Customer acquisition cost	5%	6%	6%	5%

Part 3. Concluding observations and description about participating companies

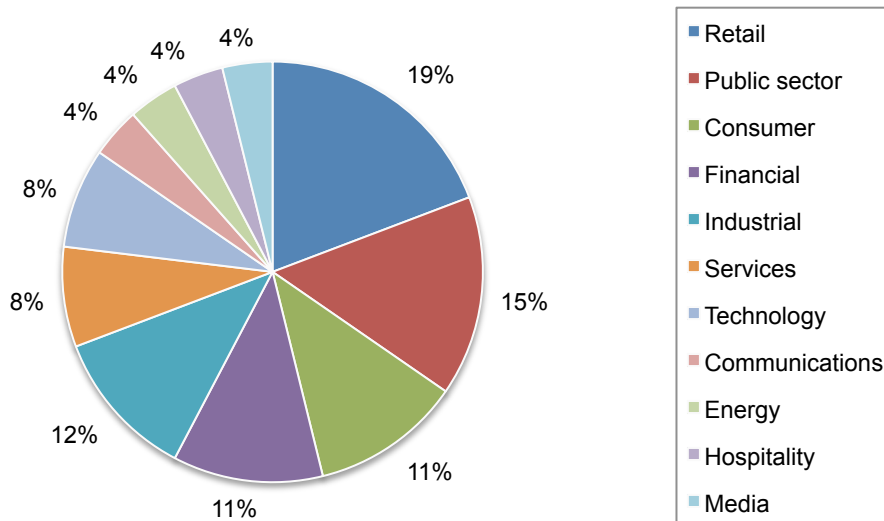
For the first time, companies participating in our annual study report that their data breaches were smaller in scale and resulted in a lower rate of churn. We conclude that companies' investment in improving their data protection practices is paying off. The most profitable investments as evidenced by the lower cost of a data breach are: the appointment of a CISO with enterprise-wide responsibility and the engagement of external consultants.

The study also reveals the severe financial consequences from malicious or criminal acts. These data breaches can prove to be the most costly. We hope this study is helpful to understanding what the potential costs of a data breach could be based on certain characteristics and how best to allocate resources to the prevention, detection and resolution of a data breach.

In this report, we compare the results of the present study to those from prior years. It is important to note that each annual study involves a different sample of companies. In other words, we are not tracking the same sample of companies over time. To be consistent, we attempt to recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint, and size of data breach.

Figure 23 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 11 industries are represented. Retail, public sector (government), consumer products and financial services represent the four largest segments.

Figure 23. Distribution of the benchmark sample by industry segment



Part 4. How we calculate the cost of a data breach

Our study addresses core process-related activities that drive a range of expenditures associated with an organization's data breach detection, response, containment and remediation. The four cost centers are:

- Detection or discovery: Activities that enable a company to reasonably detect the breach of personal data either at risk (in storage) or in motion.
- Escalation: Activities necessary to report the breach of protected information to appropriate personnel within a specified time period.
- Notification: Activities that enable the company to notify data subjects with a letter, outbound telephone call, e-mail or general notice that personal information was lost or stolen.
- Ex-post response: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimize potential harms. Redress activities also include ex-post response such as credit report monitoring or the reissuing of a new account (or credit card).

In addition to the above process-related activities, most companies experience opportunity costs associated with the breach incident, which results from diminished trust or confidence by present and future customers. Accordingly, our Institute's research shows that the negative publicity associated with a data breach incident causes reputation effects that may result in abnormal turnover or churn rates as well as a diminished rate for new customer acquisitions.

To extrapolate these opportunity costs, we use a cost estimation method that relies on the "lifetime value" of an average customer as defined for each participating organization.

- Turnover of existing customers: The estimated number of customers who will most likely terminate their relationship as a result of the breach incident. The incremental loss is abnormal turnover attributable to the breach incident. This number is an annual percentage, which is based on estimates provided by management during the benchmark interview process.⁶
- Diminished customer acquisition: The estimated number of target customers who will not have a relationship with the organization as a consequence of the breach. This number is provided as an annual percentage.

We acknowledge that the loss of non-customer data, such as employee records, may not impact an organization's churn or turnover.⁷ In these cases, we would expect the business cost category to be lower when data breaches do not involve customer or consumer data (including payment transactional information).

All participating organizations experienced one or more data breach incidents sometime over the past year. Our benchmark instrument captured descriptive information from IT, compliance and information security practitioners about the full cost impact of a breach involving the loss or theft of customer or consumer information. It also required these practitioners to estimate opportunity costs associated with program activities.

⁶In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organization, but the volume of customer activity actually declines. This partial decline is especially salient in certain industries – such as financial services or public sector entities – where termination is costly or economically infeasible.

⁷In this study, we consider citizen, patient and student information as customer data.

Estimated data breach cost components were captured on a rating form. In most cases, the researcher conducted follow-up interviews to obtain additional facts, including estimated abnormal churn rates that resulted from the company’s most recent breach event involving 1,000 or more compromised records.⁸

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	<hr style="border: 0; border-top: 1px solid black; margin: 0;"/>	UL
----	--	----

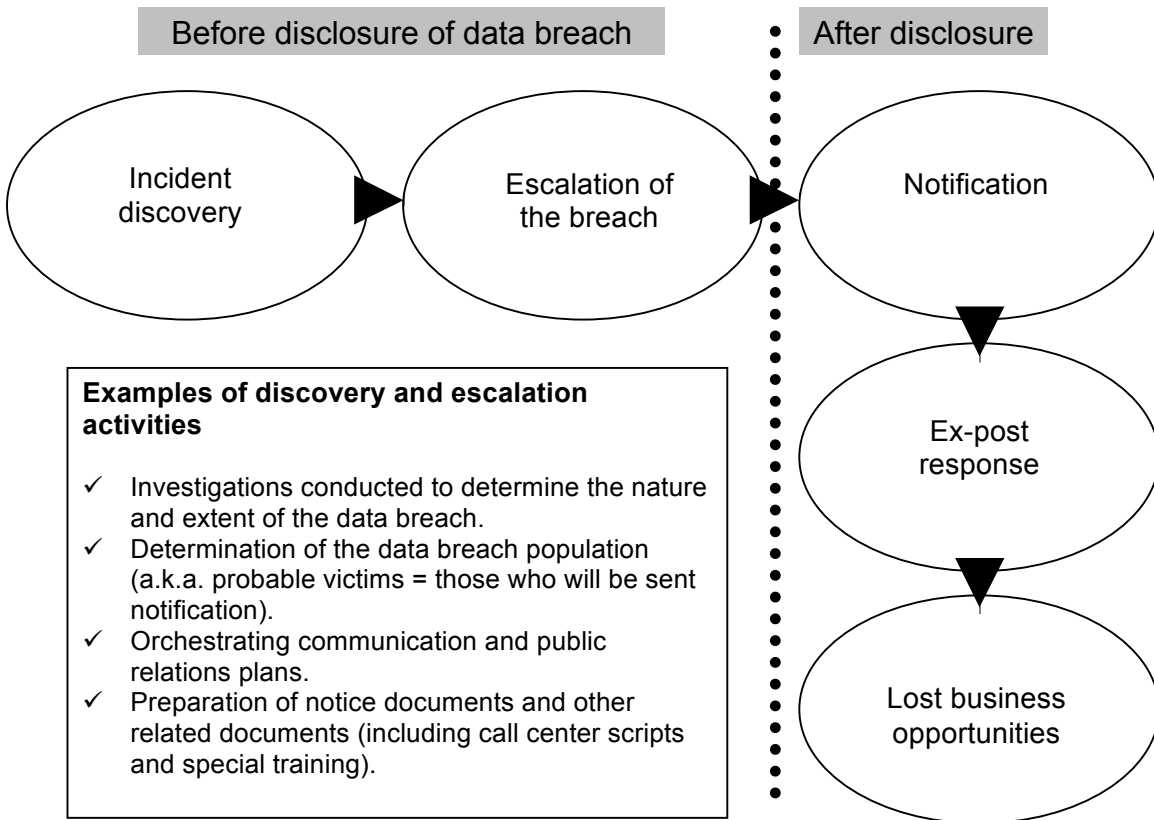
The numerical value obtained from the number line rather than a point estimate for each presented cost category preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

The scope of data breach cost items contained within our benchmark instrument was limited to known cost categories that applied to a broad set of business operations that handle personal information. We believed that a study focused on business process – and not data protection or privacy compliance activities – would yield a better quality of results.

⁸Our sampling criteria only included companies experiencing a data breach between 1,000 and 100,000 lost or stolen records sometime during the past 12 months. We excluded catastrophic data breach incidents to avoid skewing overall sample findings.

Figure 24 illustrates the activity-based costing schema used in our benchmark study. The cost centers we examine sequentially are: incident discovery, escalation, notification, ex-post response and lost business.

Figure 24: Schema of the data breach process



Within each cost center, the research instrument required subjects to estimate a cost range to capture estimates of 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 negative reputation effects after the breach has been reported to victims (and publicly revealed to the media).

To maintain complete confidentiality, the benchmark instrument did not capture any company-specific information. Subject materials contained no tracking codes or other methods that could link responses to participating companies.

To keep the benchmarking process to a manageable size, we carefully limited items to only those cost activity centers that we considered crucial to data breach cost measurement. Based upon discussions with learned experts, the final set of items included a fixed set of cost activities. Upon collection of the benchmark information, each instrument was re-examined carefully for consistency and completeness.

Limitations

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

- Non-statistical results: Our study draws upon a representative, non-statistical sample of German-based entities experiencing a breach involving the loss or theft of customer or consumer records during the past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.
- Non-response: The current findings are based on a small representative sample of benchmarks. Twenty-six companies completed the benchmark process. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of underlying data breach cost.
- 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 privacy or 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.
- Unmeasured factors: To keep the interview script 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 determined.
- Extrapolated cost results. The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

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 49686 USA
1.800.887.3118
research@ponemon.org

Ponemon Institute LLC
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.

Appendix 1: Cost for 26 Data Breach Case Studies

Cases	Size of breach	Detection & escalation*	Notification*	Ex-post response*	Lost business*	Abnormal Churn
1	27,300	1,610,340	531,423	2,706,216	958,058	7.9%
2	4,850	107,221	36,256	96,858	437,042	3.7%
3	28,010	1,510,384	58,268	2,065,346	19,042	0.0%
4	17,796	573,498	183,945	285,855	507,392	0.6%
5	3,000	333,002	48,599	38,794	23,000	0.0%
6	20,779	933,183	266,318	372,404	5,184,059	7.9%
7	5,800	127,661	32,407	139,335	248,347	0.9%
8	37,000	408,222	618,359	2,113,656	2,967,915	5.6%
9	13,476	241,652	372,298	1,392,803	279,193	3.0%
10	41,862	546,452	523,391	2,844,672	3,365,586	6.1%
11	39,000	1,132,903	34,775	1,910,997	1,492,255	4.1%
12	8,500	240,876	11,515	169,912	43,653	0.0%
13	8,900	556,000	6,500	256,000	355,100	3.5%
14	11,302	1,009,547	73,009	204,628	1,166,430	3.4%
15	31,000	3,338,845	473,771	1,285,146	960,892	1.8%
16	28,701	660,243	59,820	74,019	3,448,308	2.9%
17	21,900	549,755	130,482	591,034	281,619	1.7%
18	4,600	215,085	132,510	45,346	53,707	0.7%
19	53,537	2,996,343	718,467	2,206,693	2,417,823	4.5%
20	12,200	386,109	356,404	426,105	1,445,202	6.1%
21	3,600	110,376	124,488	100,003	728,452	7.3%
22	8,850	1,252,026	50,032	363,657	1,018,040	6.9%
23	20,500	394,788	185,154	670,074	883,964	1.8%
24	75,000	1,024,905	57,928	2,475,878	1,502,214	4.2%
25	58,928	2,752,972	525,000	1,166,881	4,784,793	6.9%
26	20,000	216,257	434,329	399,567	34,000	0.9%

*Measured in Euros ((€))