2013 Cost of Data Breach Study: Germany

Benchmark research sponsored by Symantec
Independently Conducted by Ponemon Institute LLC
May 2013

2013[1] Cost of Data Breach Study: Germany

Ponemon Institute, May 2013

Part 1. Executive Summary

Symantec Corporation and Ponemon Institute are pleased to present the *2013 Cost of Data Breach Study: Germany*, our fifth annual benchmark study concerning the cost of data breach incidents for companies located in Germany. For German organizations, the cost of a data breach continues to rise. In 2012 the cost of data breach increased from €146 to €151 on a per capita basis.[2]

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States eight years ago and Germany five years ago. Since then, we have expanded the study to include France, Australia, Italy, Japan and, for the first time this year, Brazil. To date, 122 German organizations have participated in the benchmarking process since the inception of this research five years ago.

Since Ponemon Institute began studying this issue, several EU countries have enacted laws requiring the controller of databases that contain personal information to inform affected individuals in the event of data loss or theft. In an effort to reduce administrative burdens and the cost of compliance with data protection laws, including data breach notification, the European Commission announced a 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 for all EU member countries.[3]

This year's study examines the costs incurred by 31 German companies from 11 different industry sectors following the loss or theft of protected personal data and the notification of breach victims as required by various laws. It is important to note the costs presented in this research are not hypothetical but are from actual data loss incidents. The costs are based upon estimates provided by the individuals interviewed over a ten-month period in the companies represented in this research.

To calculate the cost of data breach, the research examines 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.

The number of breached records per incident this year ranged from 5,052 to 88,082 and the average number of breached records was 24,280. We do not include organizations that had data breaches in excess of 100,000 because they are not representative of most data breaches and to include them in the study would skew the results. The cost for the 31 data breach case studies in this year's report is presented in Appendix 1.

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

- **The cost of data breach increased**. For the fifth consecutive year, the average cost per compromised record for our sample of German companies has increased. In 2011, the average cost of data breach was €146 and this increased to €151 in the present study. We define a record as information that identifies an individual and regulations require notification of data breach victims.

[1] The Cost of Data Breach report is dated as a 2013 publication. Please note that all data breach incidents studied in this year's report happened in the 2012 calendar year. Thus, all figures reflect the 2012 data breach incidents.
[2] The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.
[3] See: European Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. EC.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

The organizational cost has increased from €3.40 million in 2011 to €3.67 million in this year's study. This increase can be attributed to findings that suggest certain organizations are more vulnerable to high data breach costs.

- **Fewer customers remain loyal to breached organizations.** The average abnormal churn (a higher than average loss of customers for the industry or organization) increased from 3.5 percent in 2011 to 3.8 percent this year. Certain industries, such as financial institutions and services organizations, are more susceptible to customer churn, which causes their data breach costs to be higher than the average. As shown in prior studies, 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 remain the primary root cause of a data breach**. Forty-eight percent of organizations say that their data breach was caused by the misuse or theft of data and this represents an increase from 42 percent in 2011. Thirty-six percent of data breaches involved negligent employees or contractors (a.k.a. human factor). Only 16 percent say the breach was due to a system glitch or business process failure.

  The average per capita cost of data breach relating to the theft or exfiltration of data was €163. In contrast, the average cost of data breaches relating to system glitches or human errors were €142 and €138, respectively.

- **Ex-post response costs increase.** The costs associated with ex-post response increased from approximately €.94 million in 2011 to €1.07 million in 2012. Ex-post response costs refer to all activities that attempt to address victim, regulator and plaintiff counsels' concerns about the breach incident. This cost category also includes legal and consulting fees that attempt to reduce business risk and liability. Redress, identity protection services and free or discounted products are also included in this cost category.

- **Detection and escalation costs are higher.** Data breach costs associated with detection and escalation activities increased from €.89 million to €1.00 million in 2012. This category refers to activities that enable a company to detect the breach and determine its root cause. It also includes upstream and lateral communications that are required to focus activities and keep management informed.

- **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 €.23 million in 2011 to €.29 million.

- **Certain organizational factors increase the overall cost**. If the organization has a strong security posture, the average cost of a data breach was reduced as much as €11 per compromised record. Those organizations with an incident response plan in place prior to the data breach incident experienced cost savings as much as €9 per compromised record. The appointment of a CISO with overall responsibility for enterprise data protection realized average cost savings of €5 per record. Also, engaging consultants to assist with the breach incident also generated cost savings of €4 per record.

- **Certain attributes or factors increase the overall cost.** Specifically, data breaches caused by third parties or data breaches involving lost or stolen devices increased per capita costs by €12 and €8, respectively. Quick response also increased per capita cost by as much as €6.

Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a ten-month period. Recruiting organizations for the 2012 study began in January 2012 and interviews were completed in December. In each of the 31 participating organizations, 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 organization. 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 31 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 those involving millions of lost or stolen devices?

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 122 German organizations.

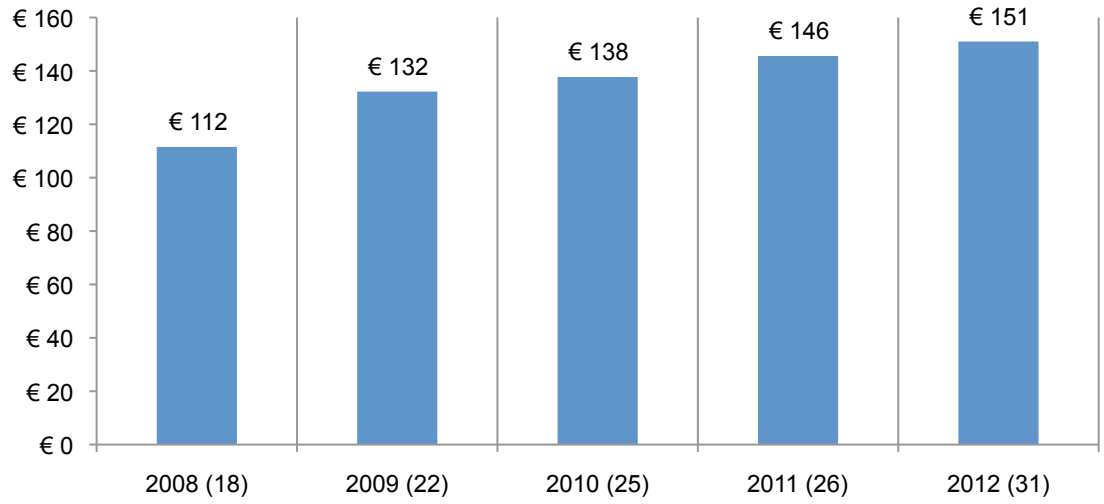
Part 2. Key Findings

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

- Cost of data breach per record and organization
- Cost of data breach by industry
- Root cause of data breach
- Factors that influence the cost of data breach
- Trends in the frequency of compromised records
- Trends in customer turnover or churn
- Trends in the following cost components: detection and escalation, notification, lost business, direct and indirect and post data breach
- Preventive measures taken after the breach
- Percentage changes in cost categories

The cost of data breach increases. Figure 1 reports the average per capita cost of a data breach.[4] As can be seen, for five consecutive years the average per capita cost has increased. According to this year's benchmark findings, data breaches cost companies an average of €151 per compromised record – of which €82 pertains to indirect costs including abnormal turnover or churn of existing and future customers. Last year's average per capita cost was €146 with an average indirect cost of €75.

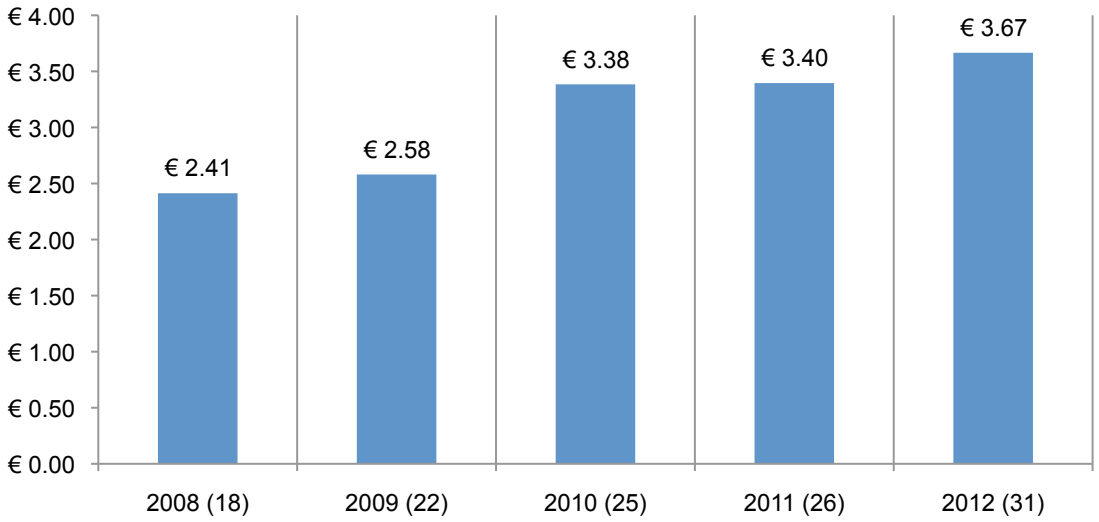
Figure 1. The average per capita cost of data breach over five years
Bracketed number defines the benchmark sample size



[4]Per 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.

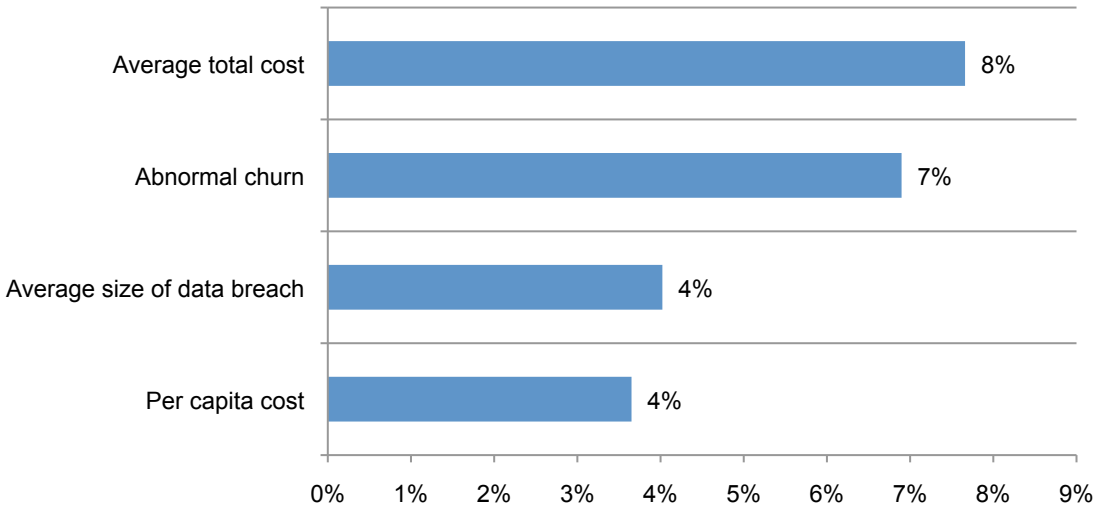
Average organizational cost of data breach increases for the fifth consecutive year. The total average cost of data breach over five years is shown in Figure 2. The total cost of data breach increased from €3.40 million in 2011 to €3.67 million in the present year.

Figure 2. The average total organizational cost of data breach over five years
€000,000 omitted



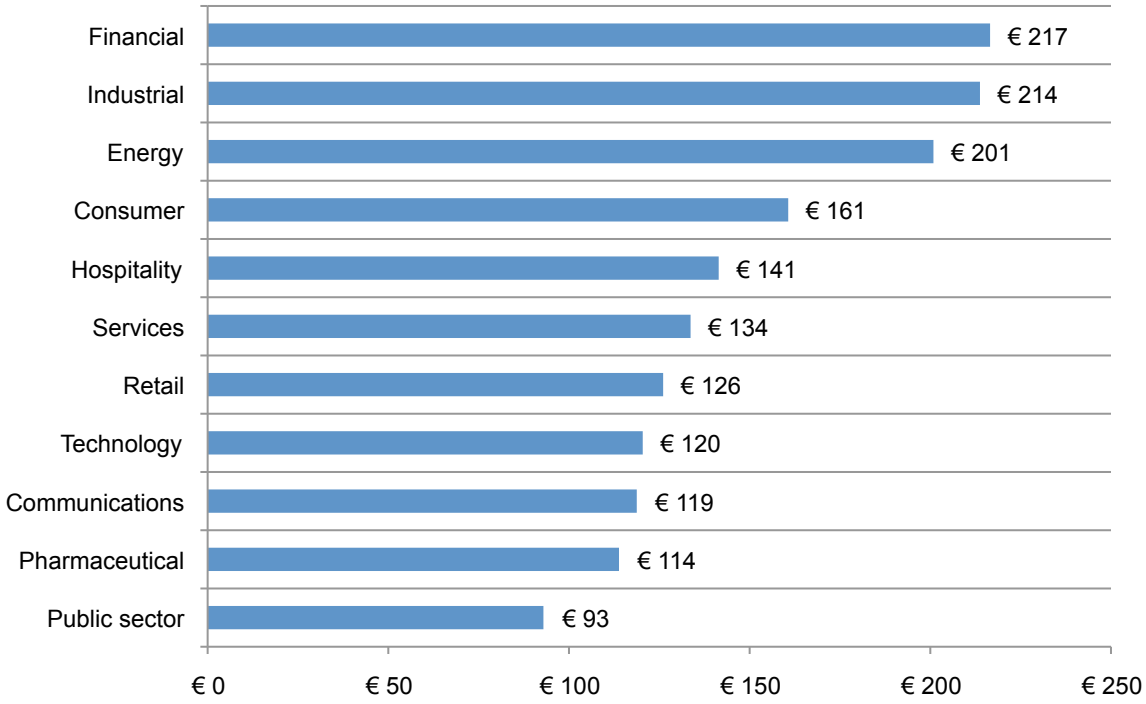
Key cost of data breach measures. Figure 3 reports four key metrics that show a consistent pattern of net change results since 2011. Both the average total cost and per capita cost of data breach increased by 8 percent and 4 percent, respectively. The 7 percent increase in abnormal churn rate suggests organizations are experiencing more negative or unfavorable responses by consumers and customers following the breach incident. Abnormal churn is defined as the greater than expected loss of customers in the normal course of business. The largest percentage increase concerns the average total cost of data breach at 8 percent. The average data breach size increased slightly by 4 percent.

Figure 3. Cost of data breach measures
Net change defined as the difference between the 2012 and 2011 results



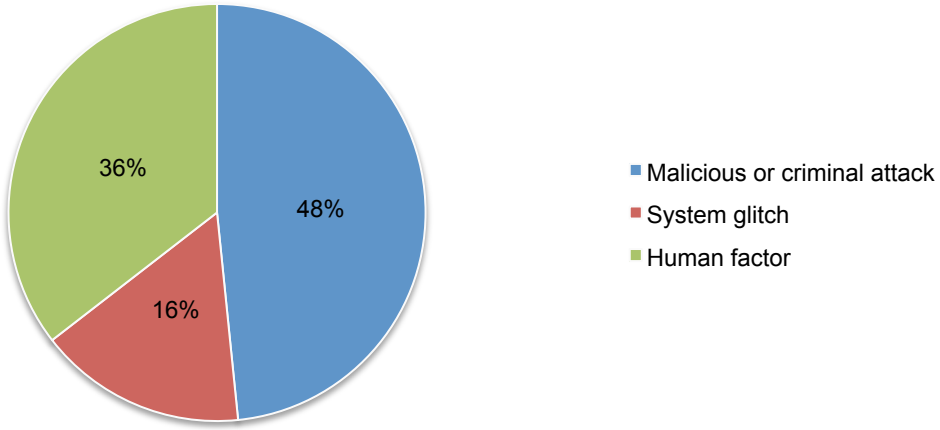
Certain industries have higher data breach costs. Figure 4 reports the per capita costs for the 2012 study by industry classification. While a small sample size prevents us from generalizing industry cost differences, the pattern of industry results is consistent with prior years. Accordingly, financial service companies tend to have a per capita cost above the mean (€217) and public sector organizations have a per capita cost below the mean (€93).

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



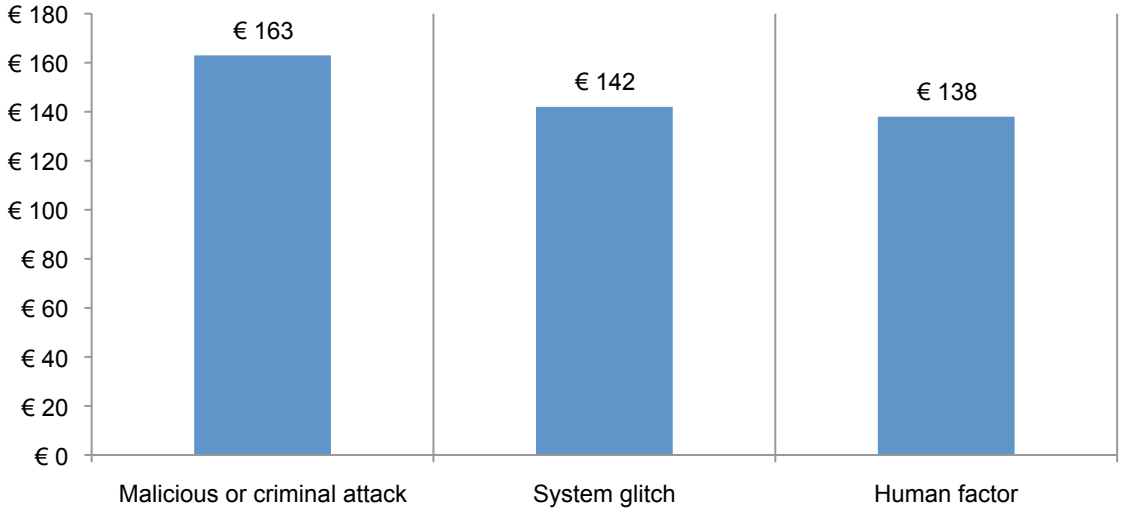
Malicious or criminal attacks are most often the cause of a data breach. Figure 5 provides a summary of the main root causes of a data breach for all 31 organizations. Forty-eight percent experienced a malicious or criminal attack. [5] Thirty-six percent of incidents involved a negligent employee or contractor[6] (human factor), and 16 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



Malicious attacks are most costly. Hackers or criminal insiders (employees, contractors and other third parties) typically cause the malicious data breach as determined by the post data breach investigation. Figure 6 reports the per capita cost of data breach for three conditions or root causes of the breach incident. The most costly breaches typically involve malicious acts against the company rather than negligence or system glitches. Accordingly, companies that experienced malicious or criminal attacks had the highest per capita cost (€163), and negligence resulted in a per capita cost of €138, which is substantially below the overall mean.

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



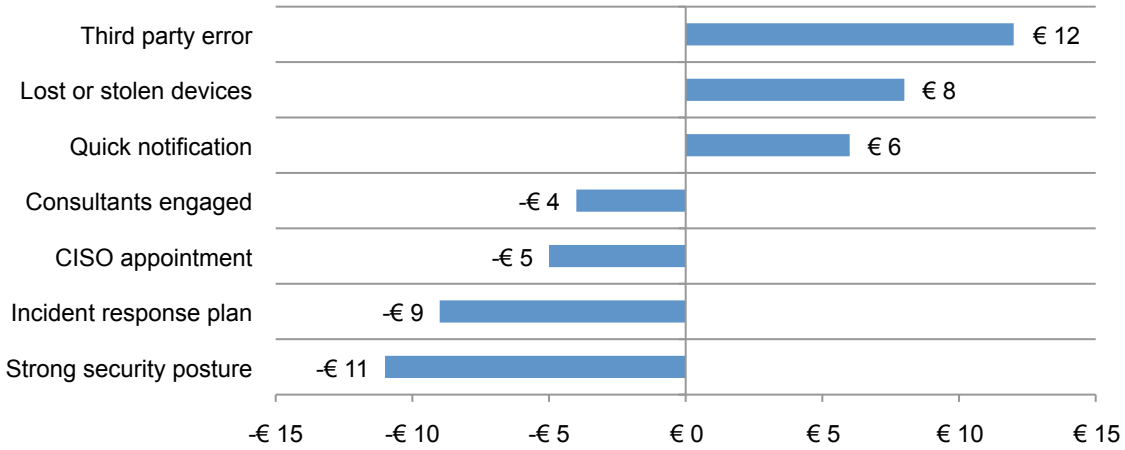
[5]Malicious and criminal attacks increased from 42 percent in our 2011 study. The most common types of attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.
[6] Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation.

Seven factors that influence the cost of data breach. We identified seven factors that influence the cost consequences of a data breach incident. These attributes are as follows:

- **The company had an incident management plan**. Sixty-one percent of organizations in our benchmark sample had a data breach incident management plan in place at the time of the data breach event.
- **The company had a relatively strong security posture at the time of the incident**. Fifty-five percent of organizations had a security effectiveness score (SES) at or above the normative average. We measured the security posture of each participating company using the Security Effective Score (SES) as part of the benchmarking process.[7]
- **CISO (or equivalent title) has overall responsibility for enterprise data protection**. Fifty-eight percent of organizations have centralized the management of data protection with the appointment of a C-level information security professional.
- **Data was lost due to third party error**. Thirty-nine percent of organizations had a data breach caused by a third party, such as vendors, outsourcers, cloud providers and business partners
- **The company notified data breach victims quickly.** Forty-five percent of organizations notified data breach victims within 30 days after the discovery of data loss or theft.
- **The data breach involved lost or stolen devices.** Thirty-five percent of organizations had a data breach as a result of a lost or stolen mobile device, which included laptops, desktops, smartphones, tablets, servers and USB drives containing confidential or sensitive information.
- **Consultants were engaged to help remediate the data breach**. Thirty-five percent of organizations hired consultants to assist in their data breach response and remediation.

As shown in Figure 7, strong security posture, incident response planning, CISO appointment and consulting support decreased the per capita cost of data breach. Third party error, lost or stolen devices and quick notification increased the per capita cost of data breach. Hence, a strong security posture reduced the average cost of data breach from €151 to €140 (decreased cost = €11). In contrast, a third party error increased the average cost to as much as €163 (increased cost = €12).

Figure 7. Impact of seven factors on the per capita cost of data breach



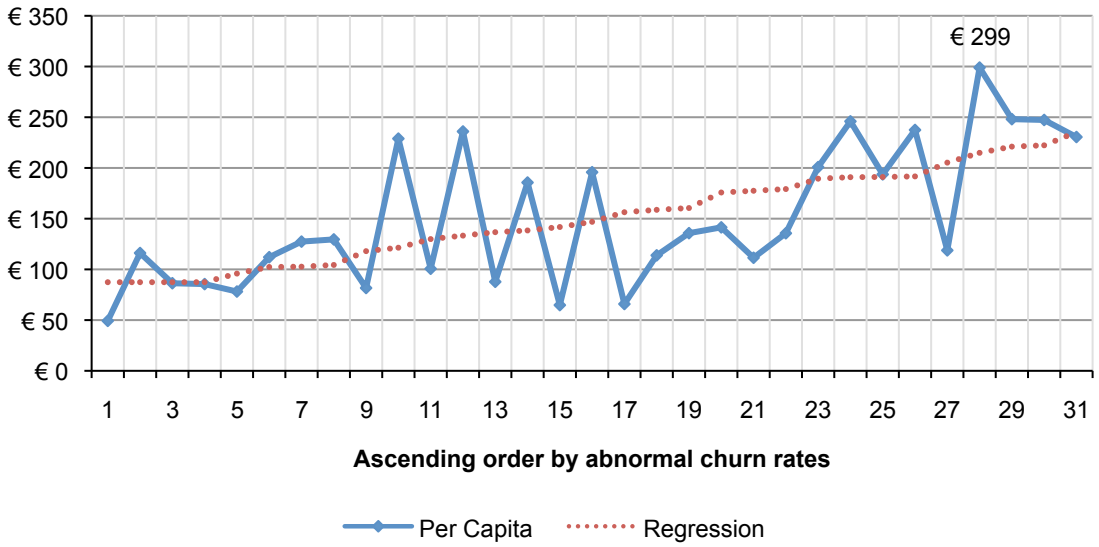
[7]The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 40 independent 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.

The more records lost, the higher the cost of the data breach. Figure 8 shows the relationship between the total cost of a data breach and the size of the incident for 31 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 €258,803 to €10,460,552.

Figure 8. 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.

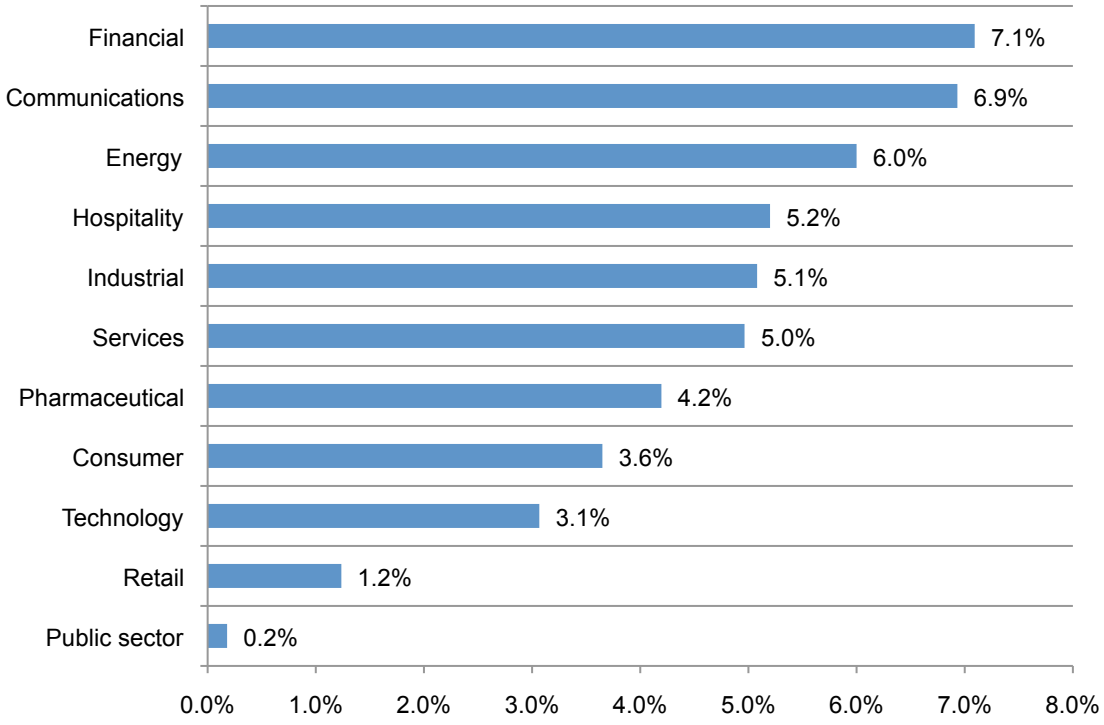
The more churn, the higher the cost of data breach. Figure 9 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is upward sloping, which suggests that abnormal churn is linearly related to cost. This pattern of results is consistent with benchmark studies completed in prior years.

Figure 9. 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 10 reports the abnormal churn rate of benchmarked organizations for the 2012 study. While a small sample size prevents us from generalizing the affect of industry on churn, our 2012 industry results are consistent with prior years – wherein financial service organizations tend to experience relatively high abnormal churn and public sector and retail companies tend to experience a relatively low abnormal churn.[8]

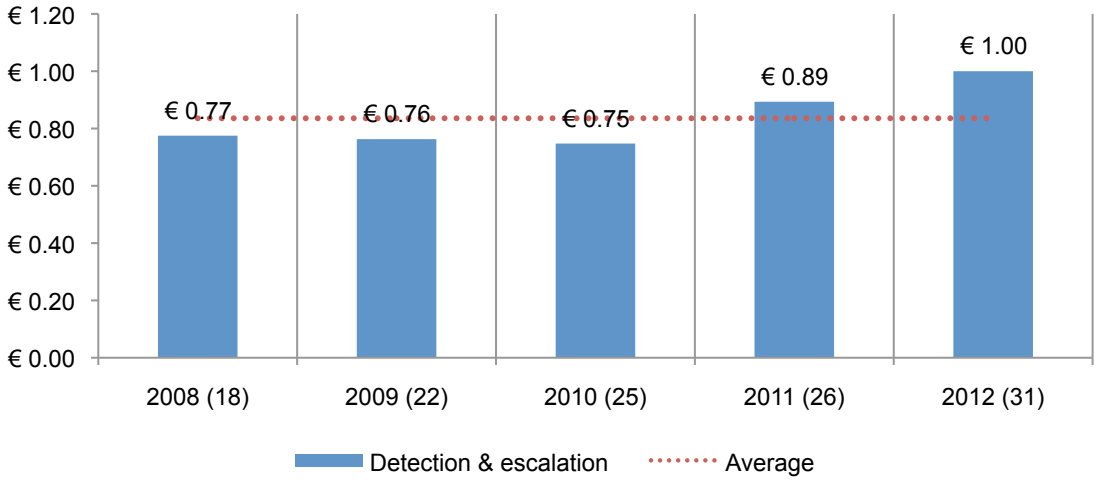
Figure 10. Abnormal churn rates by industry classification of benchmarked companies



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

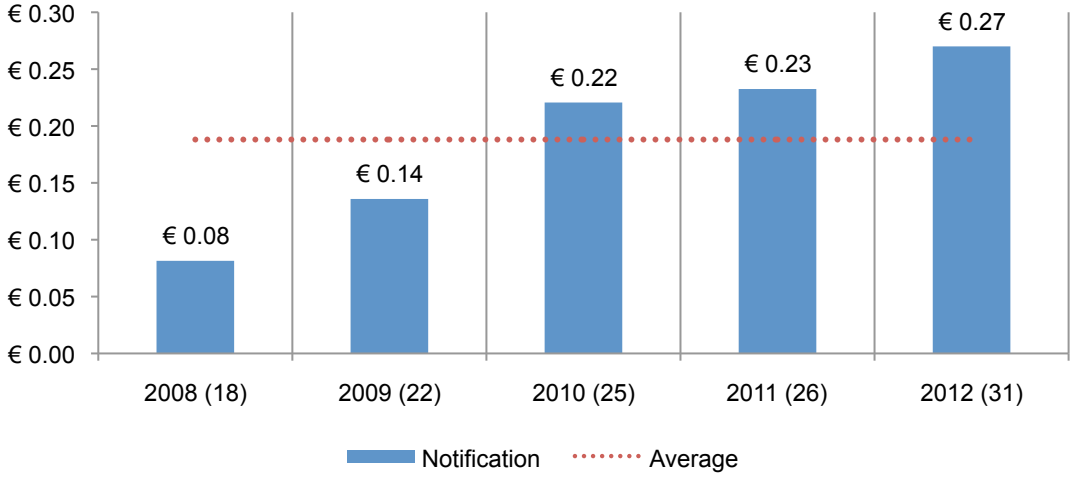
Detection and escalation costs are higher this year. Figure 11 shows the distribution of costs associated with detection and escalation of the data breach event. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. As noted, average detection and escalation costs increased from €.89 million in 2011 to €1.00 million in the present study.

Figure 11. Average detection and escalation costs over five years
€000,000 omitted



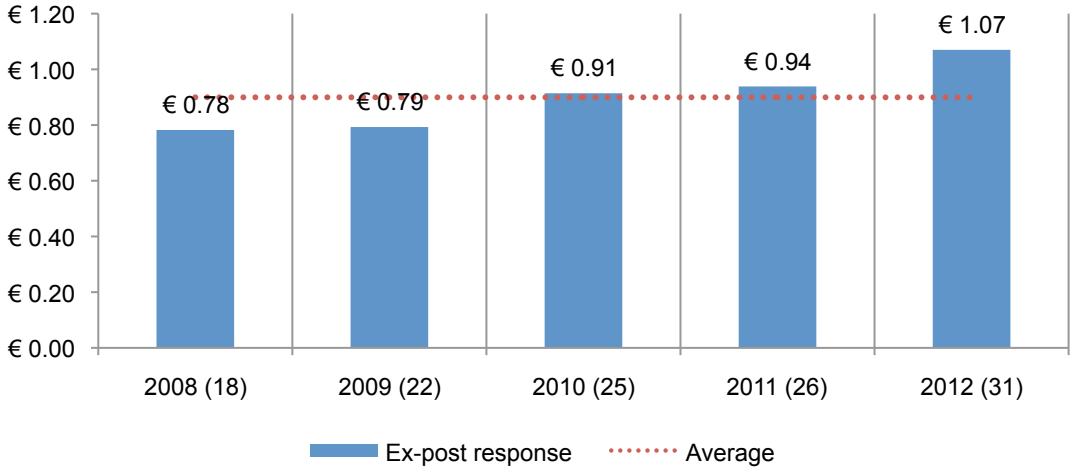
Notification costs increase slightly. Figure 12 reports the distribution of costs associated with notification activities. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up. This year's average notification cost was €.27 million, which is the highest value over four years. This represents an increase from €.23 million in 2011.

Figure 12. Average notification costs over five years
€000,000 omitted



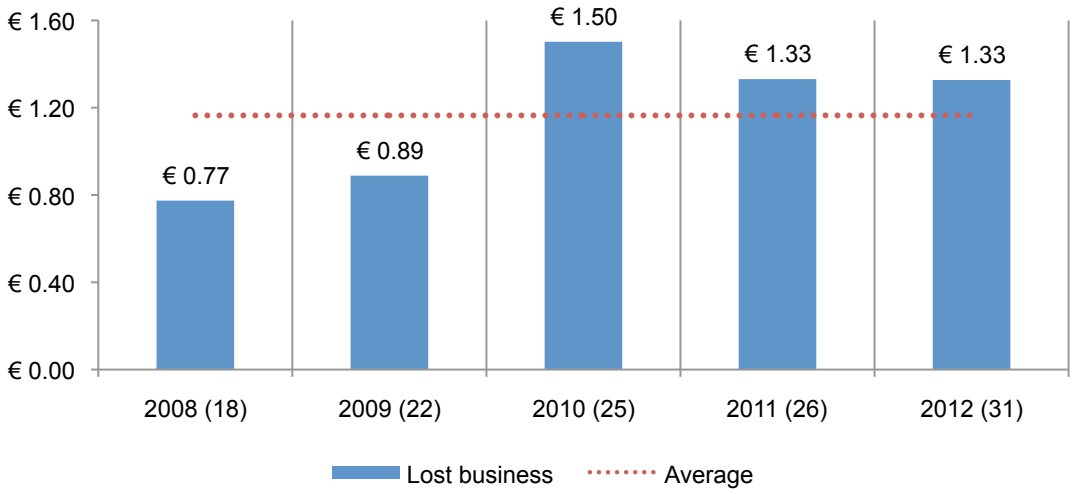
Post data breach costs increase. Figure 13 shows the distribution of costs associated with ex-post (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex-post response cost increased from €.94 million in 2011 to a four-year high of €1.07 in this year's study.

Figure 13. Average ex-post response costs over five years
€000,000 omitted



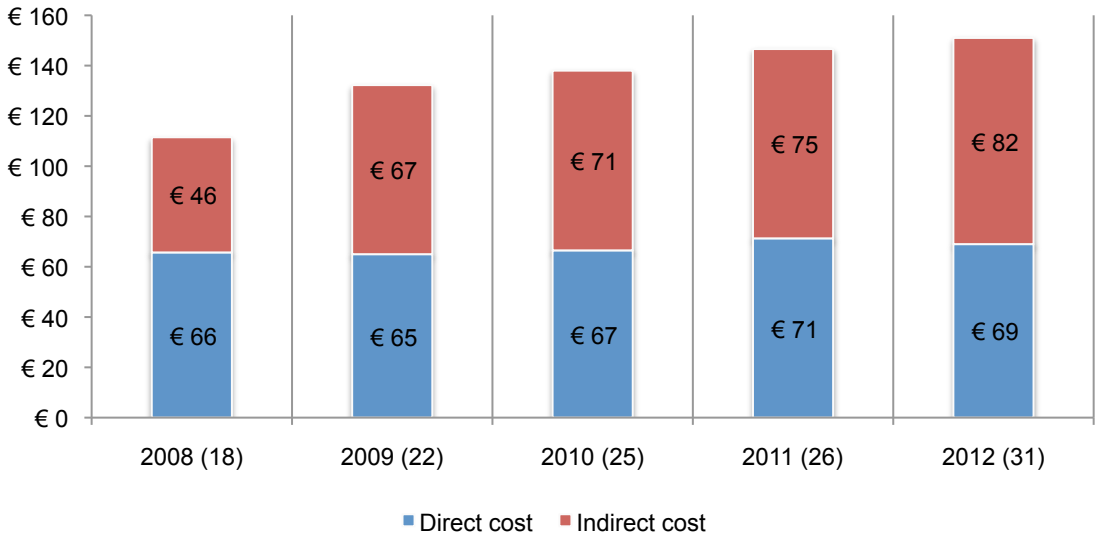
Lost business costs declined. Figure 14 reports lost business costs associated with data breach incidents over four years. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As shown, lost business costs remained at approximately the same level as in 2011. The five-year high of €1.50 occurred in 2010.

Figure 14. Average lost business costs over five years
€000,000 omitted



Indirect costs increased and direct cost decreased. Figure 15 reports the direct and indirect cost components of data breach on a per capita basis. In essence, the indirect cost of data breach per compromised record increased by €7 – from €75 in 2011 to €82 in 2012. Direct costs decreased slightly by €2 – from €71 in 2011 to €69 in 2012.

Figure 15. Direct and indirect per capita data breach cost over five years



Preventive measures taken 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 most popular measures or steps taken are: expanded use of encryption (67 percent), implementation of endpoint security solutions (64 percent), implementation of security intelligence systems such as SIEM (59 percent), strengthening of perimeter controls (55 percent) and deployment of data loss prevention (DLP) solutions (53 percent). Security certification or audit increased slightly (3 percent), while strengthening of perimeter controls decreased significantly (6 percent).

Table 1. Preventive measures and controls implemented after the data breach	2009	2010	2011	2012
Expanded use of encryption	77%	70%	65%	67%
Endpoint security solutions	59%	75%	68%	64%
Security intelligence systems	68%	58%	62%	59%
Strengthening of perimeter controls	73%	69%	61%	55%
Data loss prevention (DLP) solutions	59%	51%	56%	53%
Security certification or audit	41%	34%	45%	48%
Identity and access management solutions	27%	24%	30%	28%
Training and awareness programs	27%	26%	23%	21%
Manual control practices	14%	11%	9%	9%

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

Cost changes of data breach categories over time

Table 2 provides the percentage changes for 11 cost categories over five 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. Percentage data breach cost categories	2008	2009	2010	2011	2012
Investigations & forensics	31%	29%	29%	32%	34%
Audit and consulting services	10%	8%	9%	10%	9%
Outbound contact costs	9%	10%	10%	9%	7%
Inbound contact costs	6%	6%	6%	5%	4%
Public relations/communications	1%	1%	1%	0%	0%
Legal services – defense	2%	3%	3%	2%	4%
Legal services - compliance	5%	4%	4%	6%	5%
Free or discounted services	2%	1%	1%	1%	2%
Identity protection services	0%	0%	0%	1%	1%
Lost customer business	29%	32%	33%	29%	29%
Customer acquisition cost	5%	6%	6%	5%	5%

Part 3. Concluding observations and description about participating companies

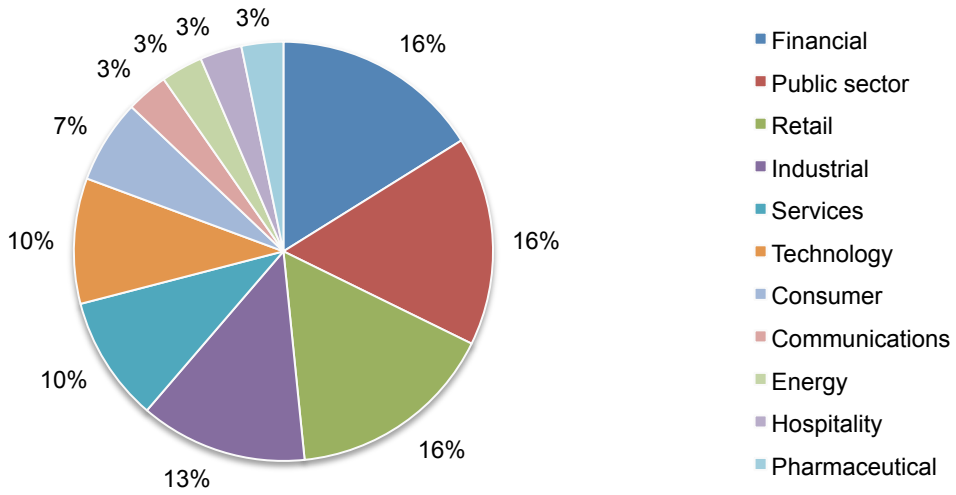
The companies participating in our annual study report that their data breaches were higher in scale and resulted in a higher rate of consumer or customer churn. We conclude that companies' investment in improving their data protection practices is important. A strong security posture, incident response planning, the appointment of a CISO with enterprise-wide responsibility and the engagement of consultants for data breach support all appear to reduce data breach costs for German companies.

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

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 16 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 11 industries are represented. Financial, public sector, retail, and industrial represent the four largest segments.

Figure 16. 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.[9]
- 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.[10] 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

[9]In 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.

[10]In this study, we consider citizen, patient and student information as customer data.

of customer or consumer information. It also required these practitioners to estimate opportunity costs associated with program activities.

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.[11]

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

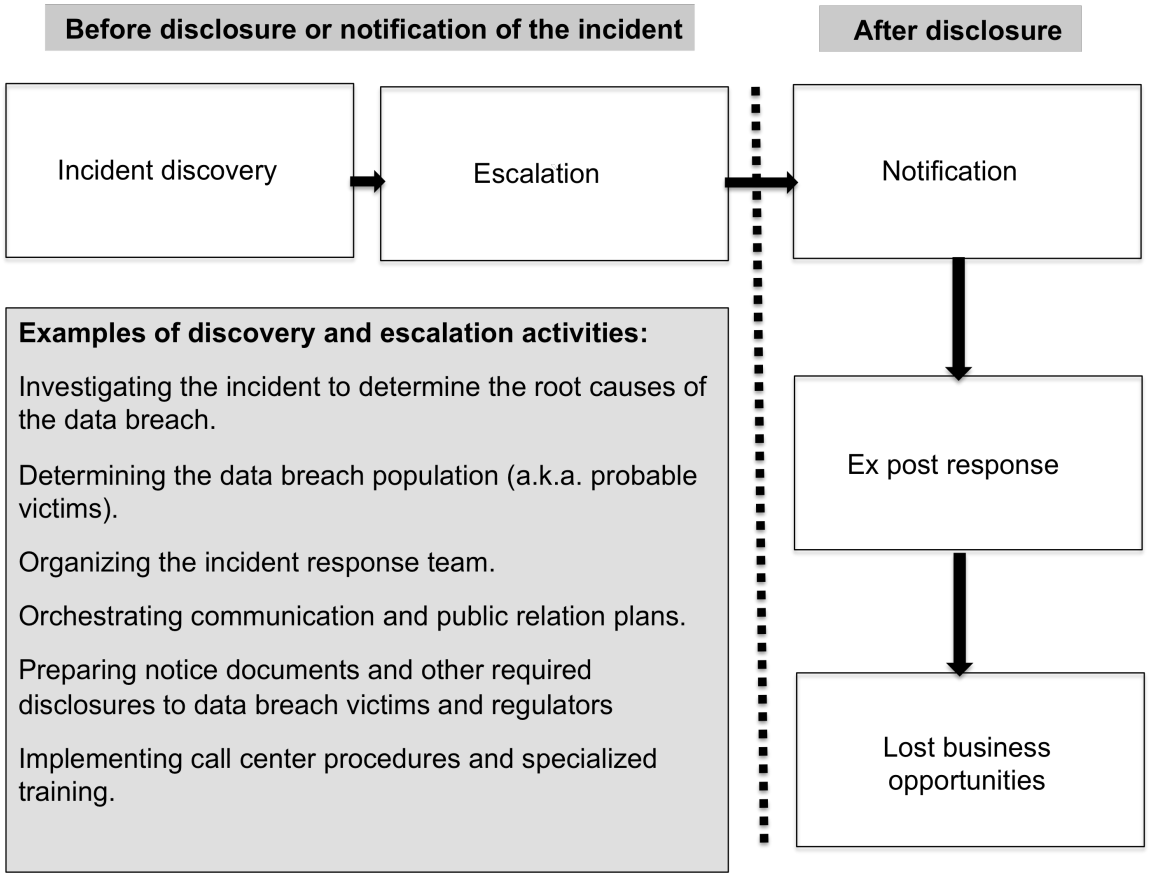
The numerical value obtained from the number line rather than a point estimate for each presented cost category preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

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.

[11] Our 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 17 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 17: 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. Thirty-one 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.

Appendix 1: Cost for 31 Data Breach Case Studies

Cases	Size of breach	Detection & escalation*	Notification*	Ex-post response*	Lost business*	Total*
1	34,810	794,753	199,660	2,612,865	3,134,700	6,741,978
2	27,178	1,651,660	55,201	1,958,894	4,459,612	8,125,367
3	9,042	477,087	756,115	212,232	325,081	1,770,515
4	88,082	3,503,824	621,467	1,005,806	5,329,455	10,460,552
5	14,362	269,316	418,315	1,681,138	297,324	2,666,093
6	11,587	326,784	339,260	859,354	1,324,242	2,849,640
7	37,775	936,938	53,307	1,861,408	1,448,792	4,300,445
8	57,843	873,175	31,931	1,833,682	1,071,517	3,810,305
9	15,030	100,957	37,462	389,644	1,511,801	2,039,864
10	22,180	1,918,100	444,674	2,169,025	953,415	5,485,214
11	16,335	690,142	174,055	283,809	495,812	1,643,818
12	13,553	504,330	115,540	287,840	602,768	1,510,478
13	8,546	162,299	133,944	344,853	466,122	1,107,218
14	28,186	834,743	578,777	2,779,107	2,500,160	6,692,787
15	28,710	1,386,153	63,733	1,872,213	11,872	3,333,971
16	5,254	153,046	46,800	47,682	11,275	258,803
17	20,428	547,823	48,950	973,469	3,138,405	4,708,647
18	5,952	105,550	57,075	330,276	16,018	508,919
19	34,000	2,199,930	687,000	2,550,900	1,391,555	6,829,385
20	19,975	1,228,765	459,404	837,063	19,439	2,544,671
21	8,544	216,457	129,571	384,064	7,709	737,801
22	20,301	588,154	98,868	634,760	264,961	1,586,743
23	19,739	957,189	92,565	509,755	1,232,268	2,791,777
24	64,030	3,361,496	834,182	1,927,245	2,561,182	8,684,105
25	14,862	387,159	32,989	103,271	439,468	962,887
26	28,272	1,352,268	49,236	269,192	810,745	2,481,441
27	8,013	396,577	866,018	221,217	406,965	1,890,777
28	24,330	401,531	155,337	509,230	920,478	1,986,576
29	25,745	3,338,099	440,593	1,164,122	950,472	5,893,286
30	5,052	133,296	39,061	108,933	284,630	565,920
31	34,960	1,219,748	277,441	2,417,921	4,758,523	8,673,633

*Measured in Euros ((€))

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.