Final Document

Sponsored by

Symantec

2011 Cost of Data Breach Study

Italy

Benchmark Research Conducted by

Ponemon Institute LLC

Report: March 2012

2011 Cost of Data Breach Study: Italy

Ponemon Institute, March 2012

Part 1. Executive Summary

Symantec Corporation and the Ponemon Institute are pleased to present *2011 Cost of Data Breach: Italy*, our first benchmark study concerning the cost of data breach incidents for Italian-based companies. For organizations in Italy, the cost of data breach is €78 for one compromised record.

Since Ponemon Institute began studying the cost of data breach, several EU countries have enacted laws requiring the owners of personal information databases to inform affected individuals in the event of a data security breach. In an effort to reduce administrative burdens and the cost of compliance costs 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]

In 2004, Italy put into effect its new data protection code. One of the key targets for simplification was the notification process. The new system is in line with the EU Data Protection Directive that allows the notification process to be simplified in cases where data processing does not adversely affect the rights and freedoms of data subjects (see Article 18, paragraph 2 of the directive).

Under the Italian code, organizations are only required to notify when processing higher-risk categories of data. These include genetic and biometric data, data processed for the purpose of analyzing or profiling individuals, and credit-related information (see Section 37 of the code for additional details). This approach is also aimed at making the process more transparent and understandable for individuals.

Our current analysis of the actual data breach experiences of 18 Italian companies from 10 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 France, Germany, the United Kingdom 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 organizations:

- **On average, it costs Italian organizations €78 for each lost or stolen record**. We define a record as information that identifies an individual whose personal information has been compromised in a data breach. The average total organizational cost of data breach is €1,387,798.

- **Customers often abandon the organization following the data breach**. Customer churn or turnover following a data breach is 3.5 percent. However, certain industries, such as

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

financial services, pharmaceuticals and technology 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.

- **Negligence is the primary root cause of data breach**. Thirty-nine percent of organizations who say the root cause is negligence followed by 33 percent who say it is due to IT and business process failures. Twenty-eight percent say the data breach was due to a malicious or criminal attack. Accordingly, organizations need to focus on processes, policies and technologies that address threats from the negligent employee and the malicious insider or hacker.

- **Lost business costs are due to abnormal turnover in customers.** On average lost business costs were €474,793. 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.

- **Certain organizational factors reduce the overall cost**. Organizations that notify victims within 30 days of the data breach can reduce the cost of the breach by an average of €29. 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 €23 per compromised record. When considering the average number of records lost or stolen, these factors can provide significant and positive financial benefits.

  Specific attributes or factors of the data breach also can increase the overall cost. For the organizations in this study, breaches caused by third parties or lost or stolen devices have on average a higher cost of data breach. Engaging consultants and having a breach for the first time also can increase the cost.

- **Detection and escalation costs reflect the organizations investment in getting to the root cause of the breach.** Detection and escalation costs average €1,387,798. These costs refer to activities that enable a company to detect the breach and whether it occurred in storage or in motion. This increase suggests that organizations should assess what processes and technologies are needed to improve their ability to detect and investigate data breaches.

- **Notification costs are the smallest component of the average cost of data breach**. Notification refers to the steps taken to report the breach of protected information to appropriate personnel within a specified time period. The average cost to notify victims of the breach is €57,500.

Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews 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 18 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 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, outsourced hotline support, 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 18 organizations to participate in this study.

Can the average cost of 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 a 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 Italian 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.

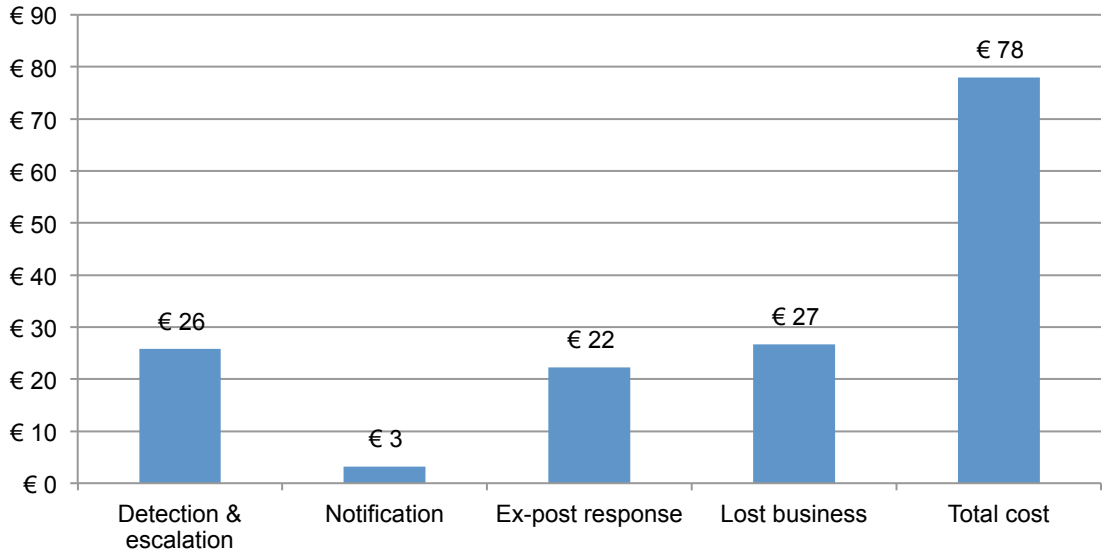
Part 2. Key Findings

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 per record and organizational cost of data breach is based upon what an organization spends to remediate the breach. Figure 1 reports the average per capita cost of data breach is €78.[2] The cost of data breach is based upon what the organization spends to investigate the breach (€26), notify victims (€3) and ex-post response (€22). The largest component is lost business (€27). Fifty-one percent of the total cost pertains to indirect costs, which includes abnormal turnover or churn of existing and future customers.

Figure 1: The average per capita cost of data breach



[2]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.

The total average cost of data breach as shown in Figure 2 is €1,387,798. The largest component of the average total organizational cost of data breach is lost business.

Figure 2. The average total organizational cost of data breach

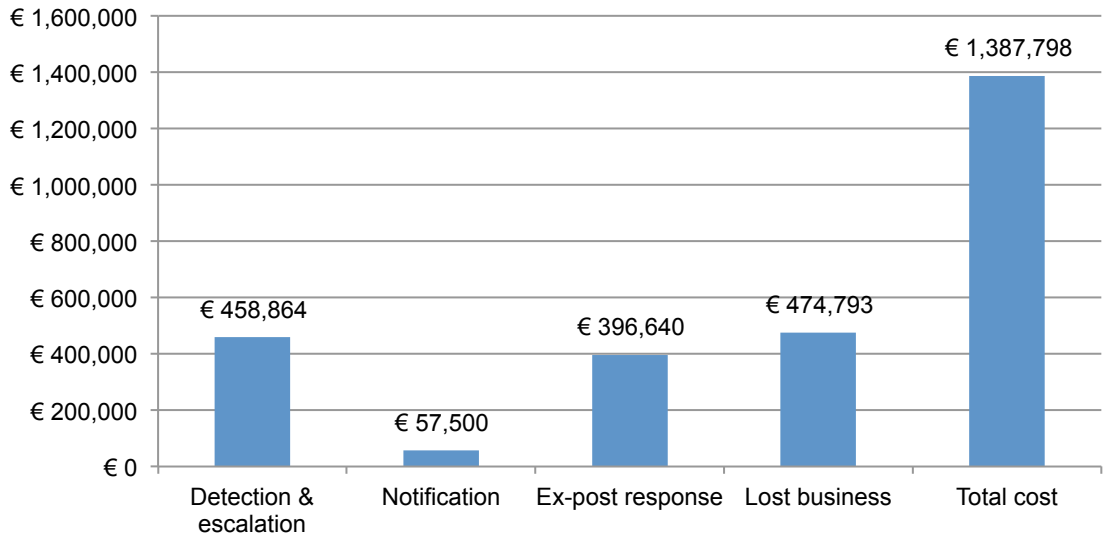
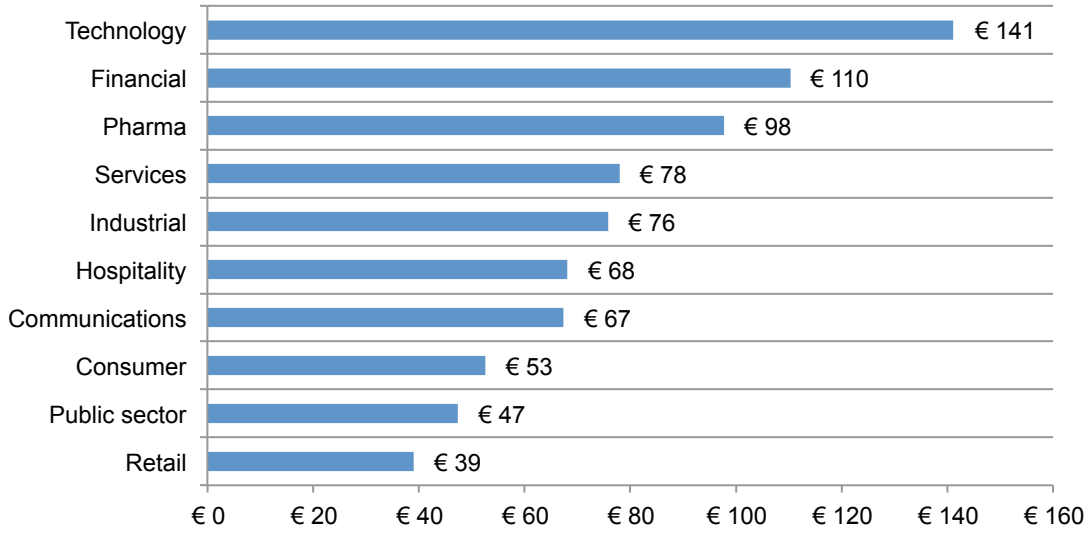


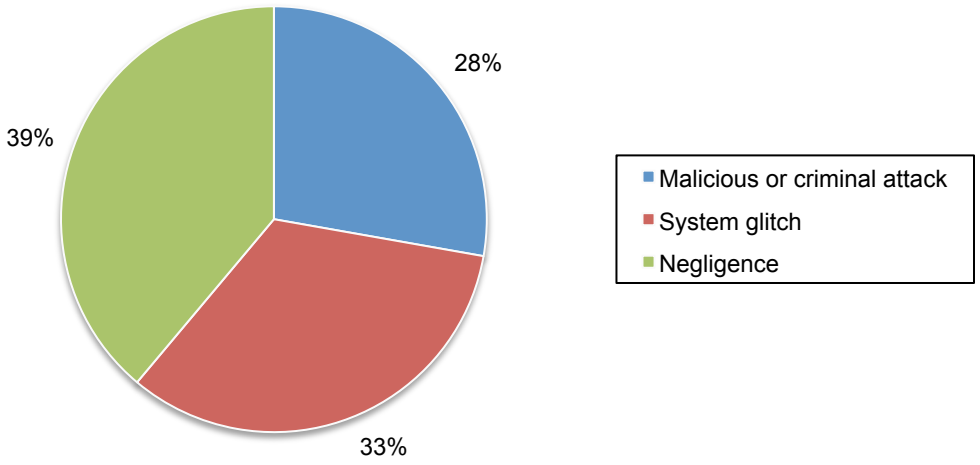
Figure 3 reports the per capita costs for the 2011 study by industry classification. While small sample size prevents us from generalizing industry cost differences, technology, financial and pharmaceutical companies tend to have a per capita cost above the mean and retail companies have a per capita cost significantly below the mean.

Figure 3. Per capita cost by industry classification of benchmarked companies



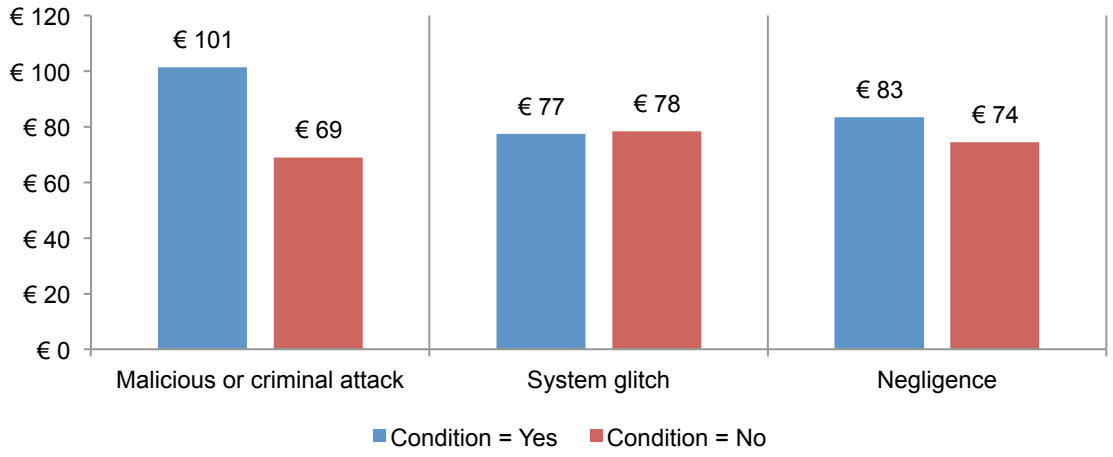
Negligence is the primary root cause of a data breach. Figure 4 provides a summary of the main root causes of a data breach for all 18 organizations. As shown, 39 percent experienced a data breach as a result of negligence. Thirty-three percent of incidents involved system glitches, including a combination of both IT and business process failures. Twenty-eight percent of respondents say it was due to a malicious or criminal attack.

Figure 4. 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 data breach as determined by the post data breach investigation. Figure 5 reports per capita cost of data breach for three conditions or root causes of the breach incident. While a smaller percentage of companies experience malicious or criminal attacks they have the highest per capital cost (€101), and companies experiencing system glitches have the lowest per capita cost (€77), which is slightly below the mean. Negligence results in a per capita cost of €83, which is slightly above the mean.

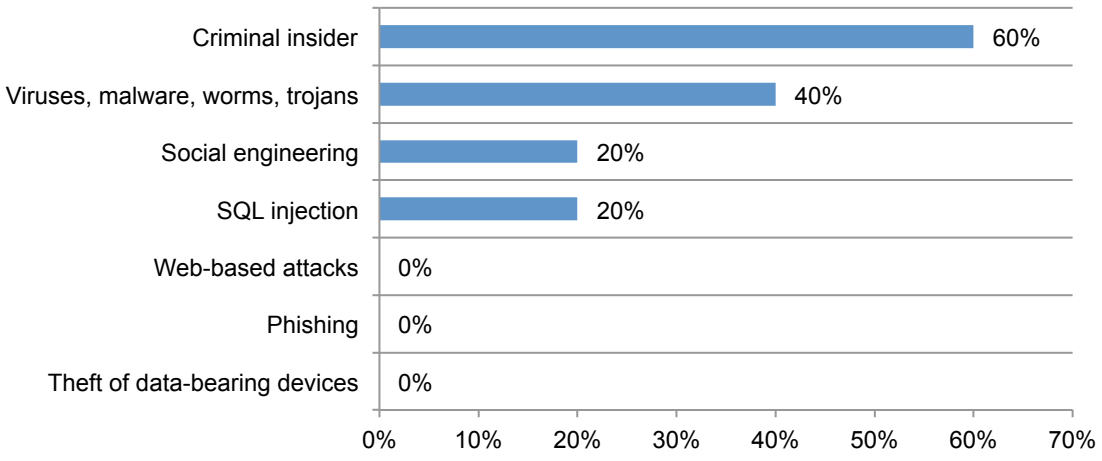
Figure 5. Per capita cost for three root causes of the data breach



Criminal attacks are mainly caused by criminal insiders. In this year's report, we analyzed the findings from the 5 organizations that report their data breach was caused by a malicious insider or hacker as previously described. Figure 6 summarizes the types of criminal attacks experienced. Please note that a given company might have experienced two or more of these attacks.

Sixty percent of the subsample experienced attacks by criminal insiders and 40 percent say the attacks were from electronic agents such as viruses, malware, worms and trojans. SQL injection and social engineering were experienced by 20 percent of this subsample.

Figure 6. Analysis of malicious or criminal attacks experienced by 5 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 in this study that have these attributes is shown in Figure 7.

- **The data breach involved lost or stolen devices**. Fifty percent say the incident involved one or more lost or stolen data-bearing devices – which included laptops, smartphones, tablets and servers.
- **First time the organization had a data breach**. Forty-four percent say the incident was their first data breach involving 1,000+ records.
- **The organization notified data breach victims quickly**. Thirty-three percent say their organizations responded and provided notice about the data breach within 30 days of discovery.
- **Data was lost or stolen due to a third-party flub**. Twenty-eight percent say their data breach involved one or more third parties – including outsourcers, cloud providers and business partners
- C**onsultant is engaged to help remediate the data breach**. As can be seen, 28 percent say their organizations engaged a consultant to assist in the data breach response or remediation.
- **CISO (or equivalent title) has overall responsibility for enterprise data protection**. Twenty-two percent of participating organizations have centralized the management of data protection with the appointment of a C-level security professional.

Figure 7. Defining attributes for the benchmark sample

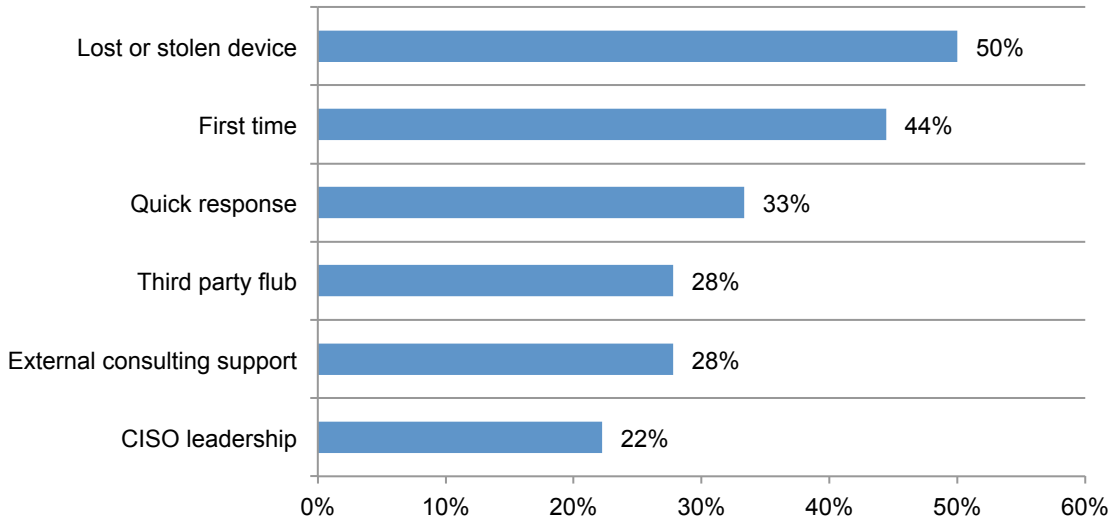


Figure 8 summarizes the per capita costs for six normatively important conditions or attributes about the benchmark sample. As previously mentioned, these attributes were selected based on learned experiences from previous cost benchmark studies.

Per capita costs are above the mean for companies experiencing a major data breach involving 1,000+ records for the first time and those quickly responding to the breach event. Data breaches involving third party mistakes or the loss or theft of a data-bearing device appear to be more expensive. In addition, engaging a external consultant increases cost. In contrast, per capita costs are below the mean for organizations that have a CISO in-charge of data protection efforts or are quick in the notification to data breach victims.

Figure 8. Per capita cost for six sample attributes or conditions

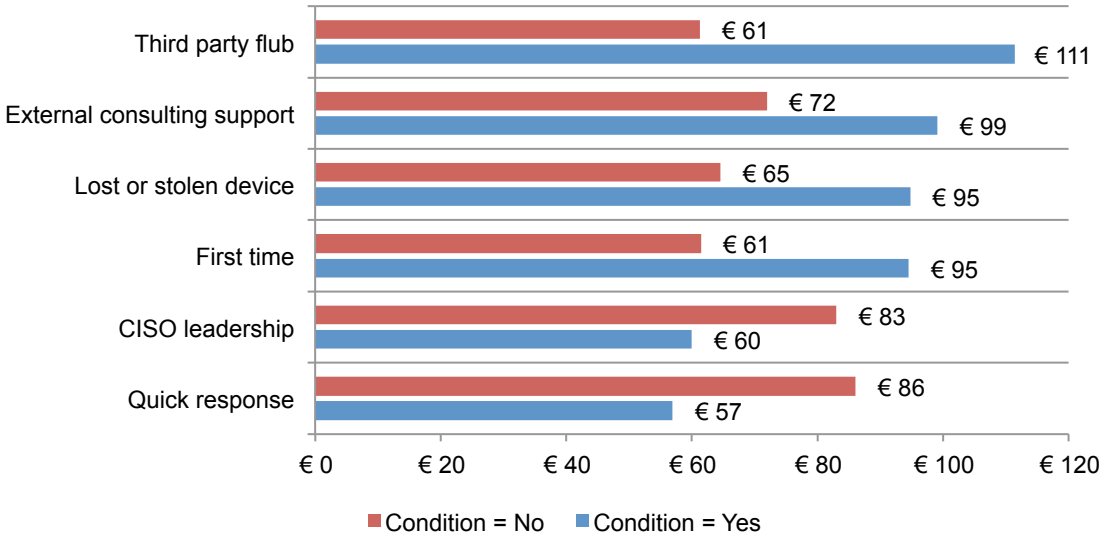
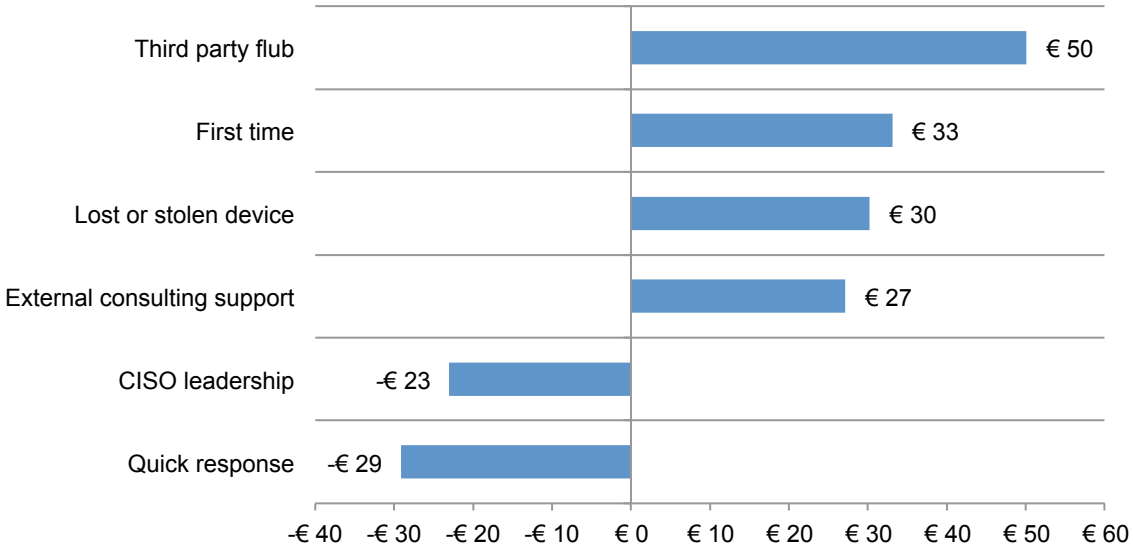


Figure 9 summarizes the per capita cost differences for six normatively important conditions or attributes about the benchmark sample. In this analysis, a positive difference means that the attribute or condition moderates or lessens data breach costs. A negative difference has the opposite meaning.

As can be seen, organizations that respond quickly to the breach and notify victims within 30 days save an average of €29 per compromised record. Companies that employ a CISO with enterprise-wide responsibility for data protection experience a €23 cost saving per compromised record. The other four attributes increase the average cost of data breach.

Figure 9. Per capita cost differences for six attributes or conditions



The average number of records lost or stolen among organizations varies significantly. 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 72,450 records. The smallest breach involved 2,600 records.

Figure 10. Size of data breach

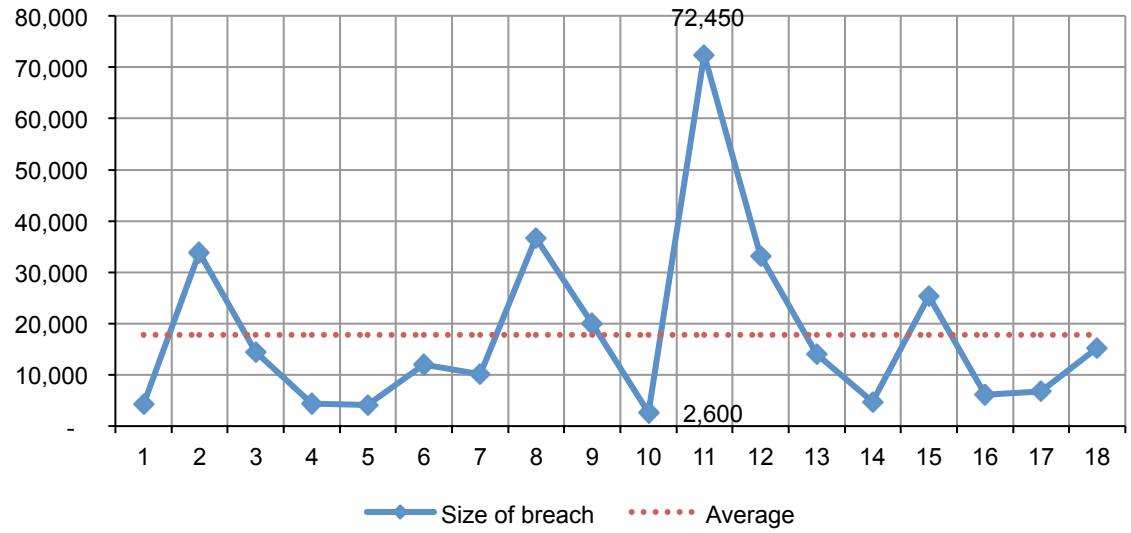


Figure 11 shows the relationship between the total cost of data breach and the size of the incident for 18 benchmarked companies in ascending order by the size of the breach incident. The regression line clearly indicates that the size of the data breach incident and total costs are linearly related. In this year's study, the cost ranged from €211,733 to €4,010,407.

Figure 11. 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.

Customers often abandon the organization following a data breach. Figure 12 shows the abnormal churn rates for each one of the 18 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.

Figure 12. Distribution of abnormal churn rates for 18 benchmark companies

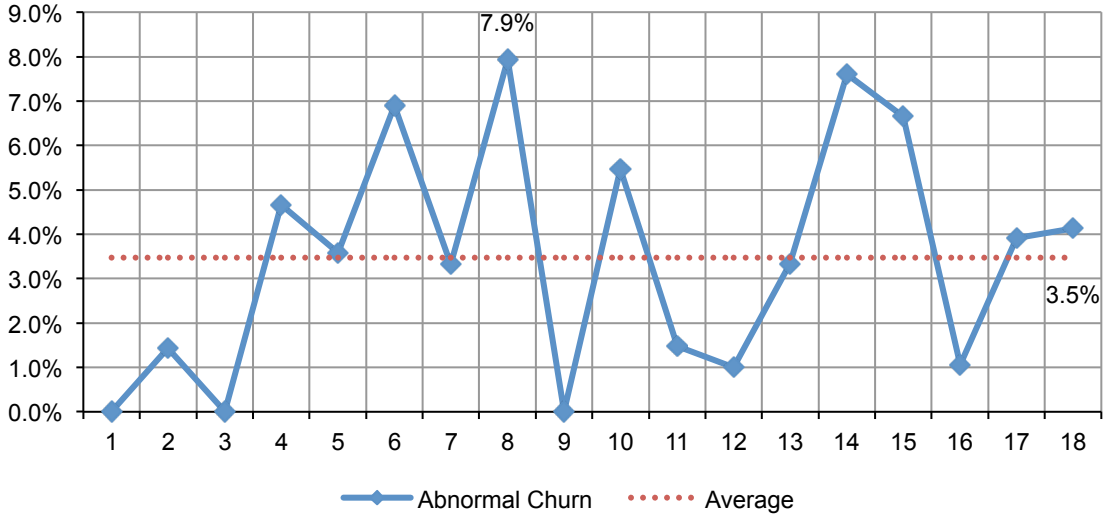
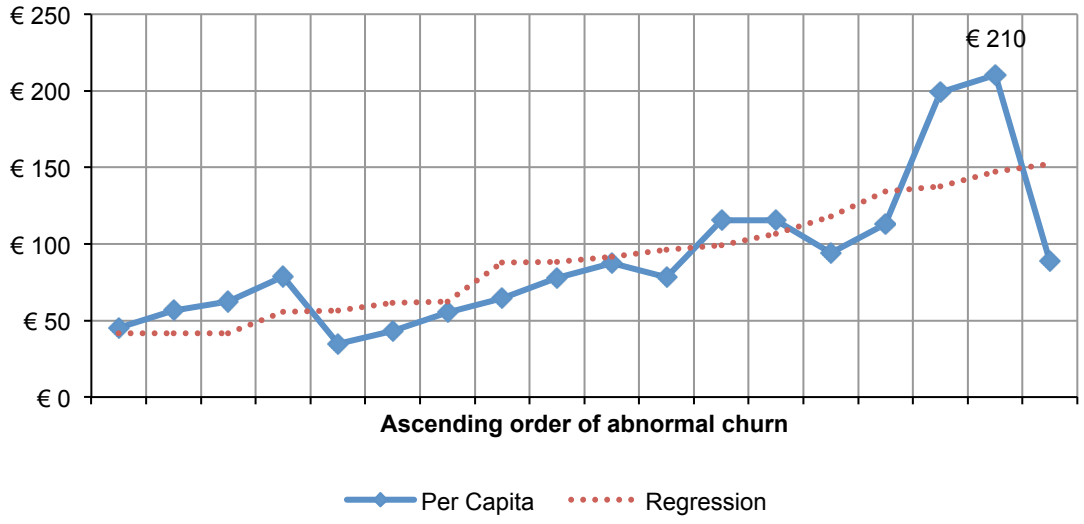


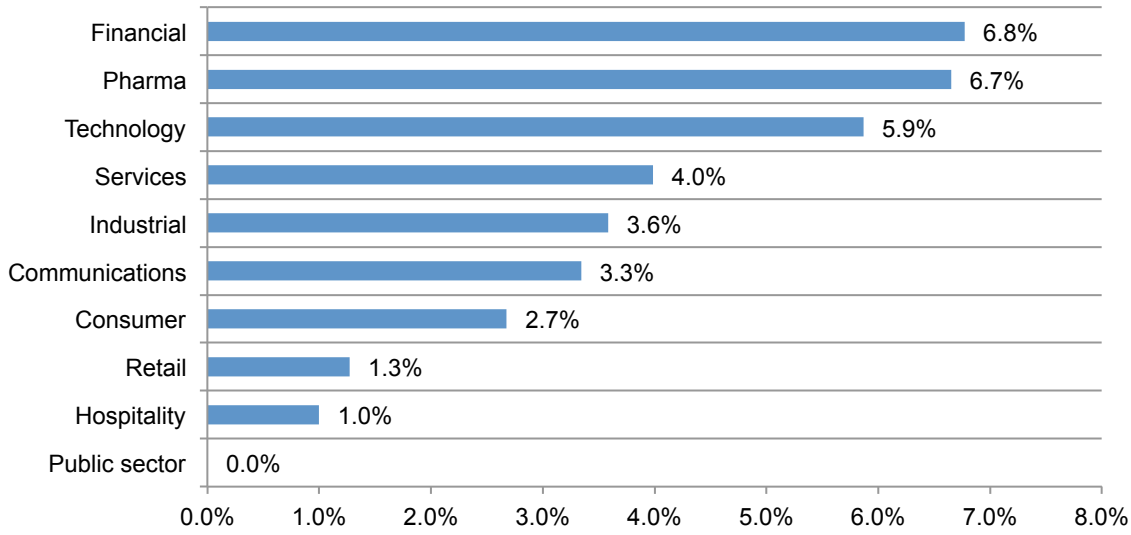
Figure 13 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is upward sloping, which suggests that abnormal churn is linearly related to cost. The highest per capita cost as a result of customer churn is €210 and the lowest is €35.

Figure 13. Distribution of per capita costs in ascending value of abnormal churn rates
Regression = Intercept + {Abnormal Churn} x β, where β denotes the slope.



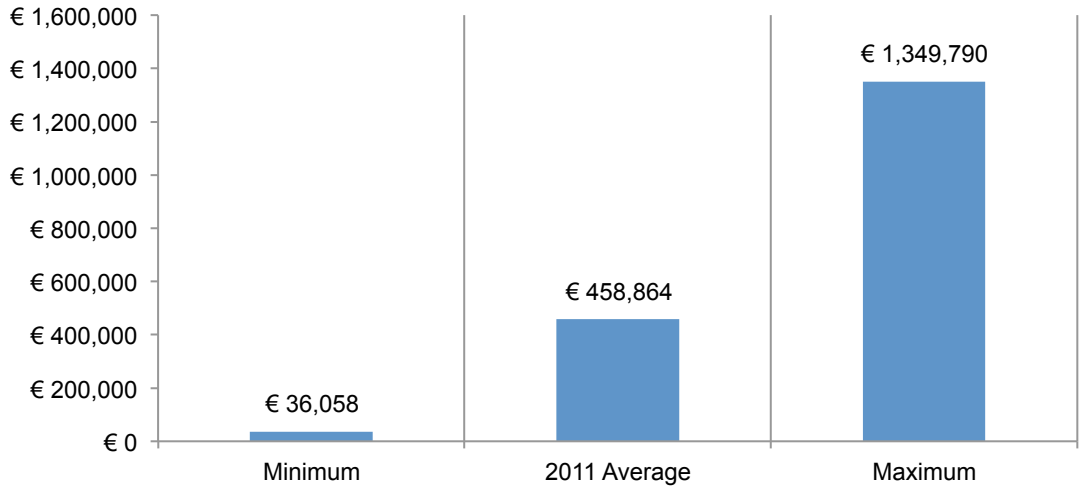
Certain industries are more vulnerable to churn. Figure 14 reports the abnormal churn rate of benchmarked organizations for the 2011 study. While small sample size prevents us from generalizing the affect of industry on data breach cost, financial service organizations and pharmaceutical companies tend to experience relatively high abnormal churn and hospitality companies tend to experience a relatively low abnormal churn.[3] In this year's study, public sector (government) organizations realize no churn.

Figure 14. Abnormal churn rates by industry classification of benchmarked companies



Detection and escalation costs in organizations vary significantly. Figure 15 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 are €458,864.

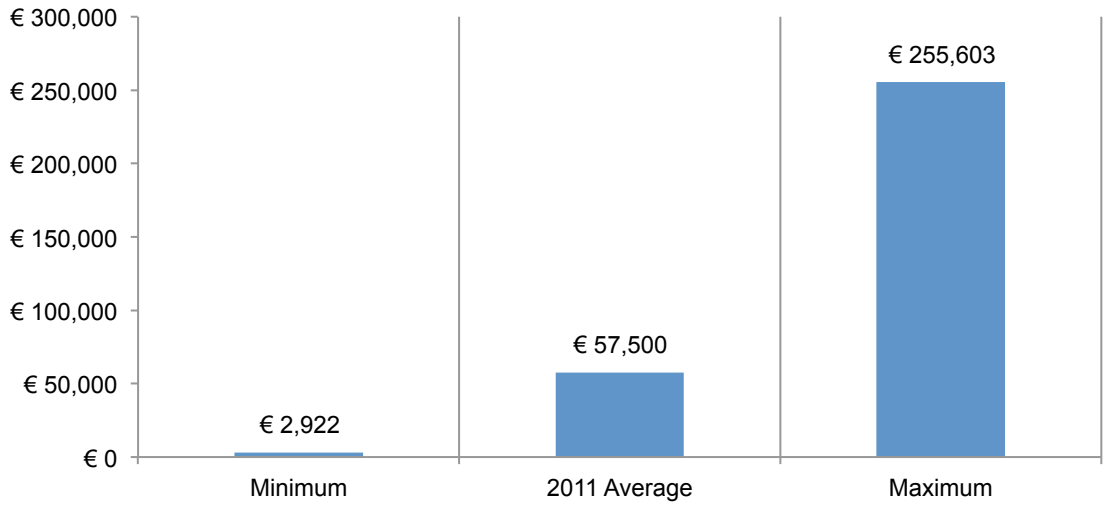
Figure 15. Average, minimum and maximum cost for detection and escalation



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

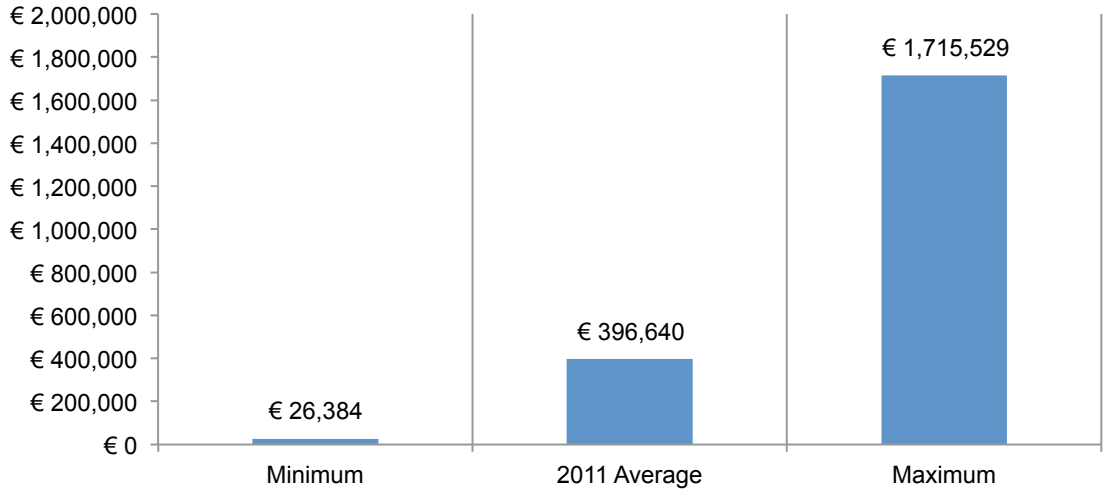
Notification costs are the smallest component of data breach costs. Figure 16 reports the distribution of costs associated with notification activities. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up. This year's average notification is €57,500.

Figure 16. Average, minimum and maximum cost for notification



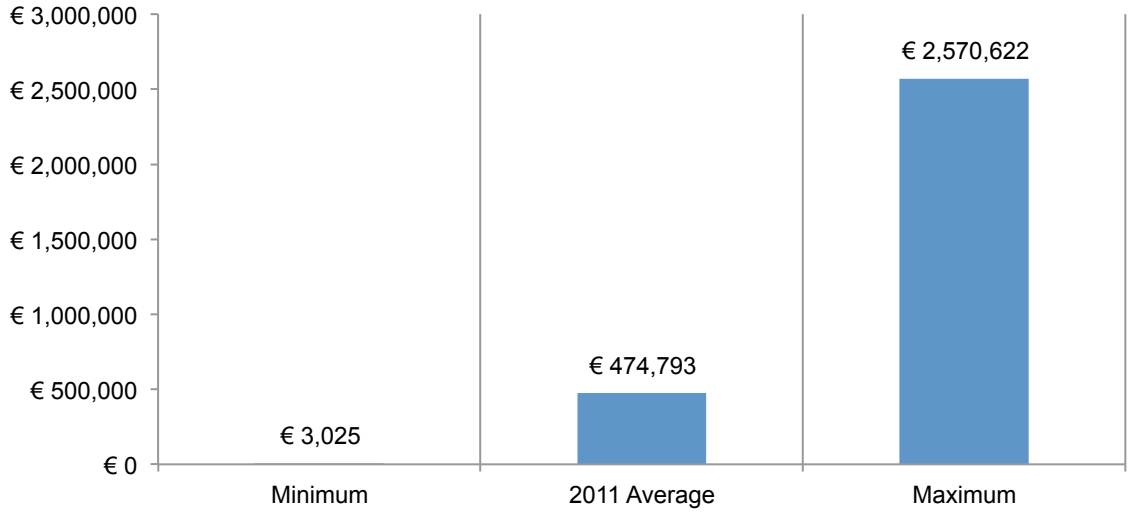
Post data breach costs vary considerably among companies. Figure 17 shows the distribution of costs associated with ex-post (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex-post response cost is €396,640.

Figure 17. Average, minimum and maximum cost for ex-post response



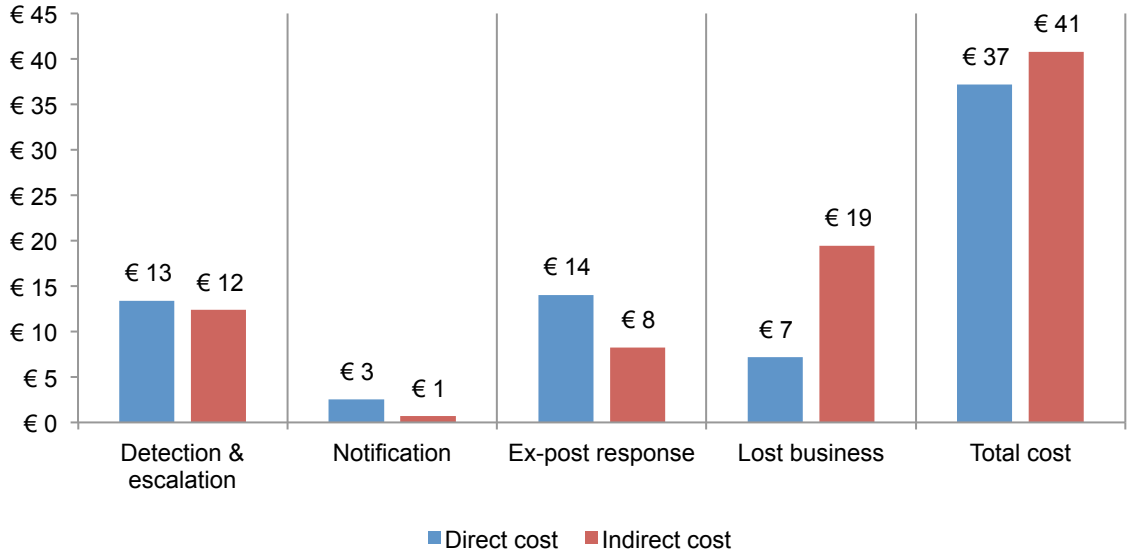
Lost business is the largest component of the cost of data breach. Figure 18 reports lost business costs associated with data breach incidents. The cost category typically includes the turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen below, lost business costs average €474,793.

Figure 18. Average, minimum and maximum cost for lost business



Indirect costs represent a greater proportion of the total cost. Figure 19 reports the direct and indirect cost components of data breach on a per capita basis. In the present study, indirect costs represent approximately 51 percent of total per capita cost and direct costs represent 49 percent of the total costs.

Figure 19. Direct and indirect per capita data breach cost by activity



We measured the security posture of each participating company using the Security Effective Score (SES) as part of the benchmarking process. [4] Figure 20 reports the SES Index for 18 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 +1.195 to a low of -1.352, with a mean value at -0.32.

Figure 20. Distribution of Security Effectiveness Scores for 18 benchmark companies

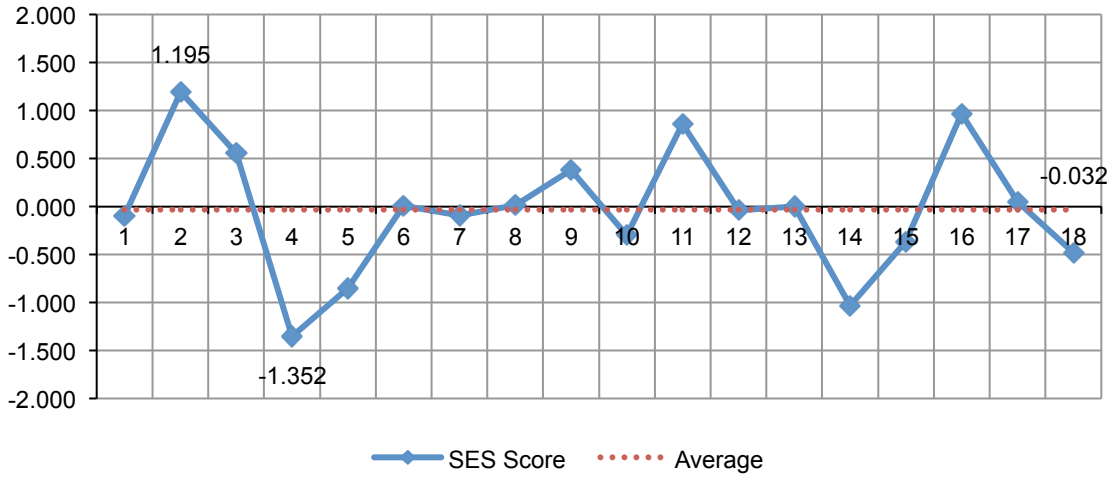
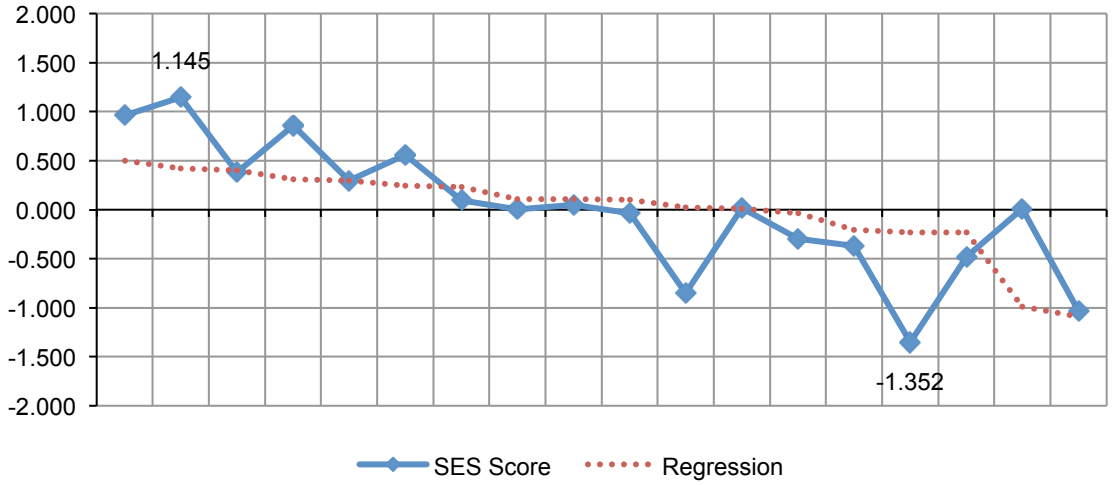


Figure 21 reports the distribution of per capita data breach cost in descending value of abnormal churn. The regression line is upward sloping, suggesting that the security effectiveness score (SES) for each organization is inversely related to their per capita data breach cost. In other words, a strong security posture appears to moderate data breach costs.

Figure 21. Security Effectiveness Score (SES) in descending value of per capita cost
Regression = Intercept + {Per Capita Cost} x β, where β denotes the slope.



[4] 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 include: additional manual procedures and controls (64 percent), training and awareness programs (50 percent), the expanded use of encryption (29 percent) and security certification or audit (29 percent).

Table 1. Preventive measures Implemented after the incident	FY 2011
Additional manual procedures and controls	64%
Training and awareness programs	50%
Expanded use of encryption	29%
Security certification or audit	29%
Other system control practices	26%
Strengthening of perimeter controls	25%
Identity and access management solutions	16%
Data loss prevention (DLP) solutions	13%
Endpoint security solutions	13%
Security intelligence systems	8%

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

Table 2 summarizes the 11 cost categories measured in the average cost of data breach. The two highest cost categories pertain to investigation and forensics and lost customer business.

Table 2. Summary of cost categories	FY 2011
Investigations & forensics	31%
Audit and consulting services	15%
Outbound contact costs	4%
Inbound contact costs	8%
Public relations/communications	3%
Legal services - defense	4%
Legal services - compliance	3%
Free or discounted services	5%
Identity protection services	0%
Lost customer business	19%
Customer acquisition cost	7%
Total	100%

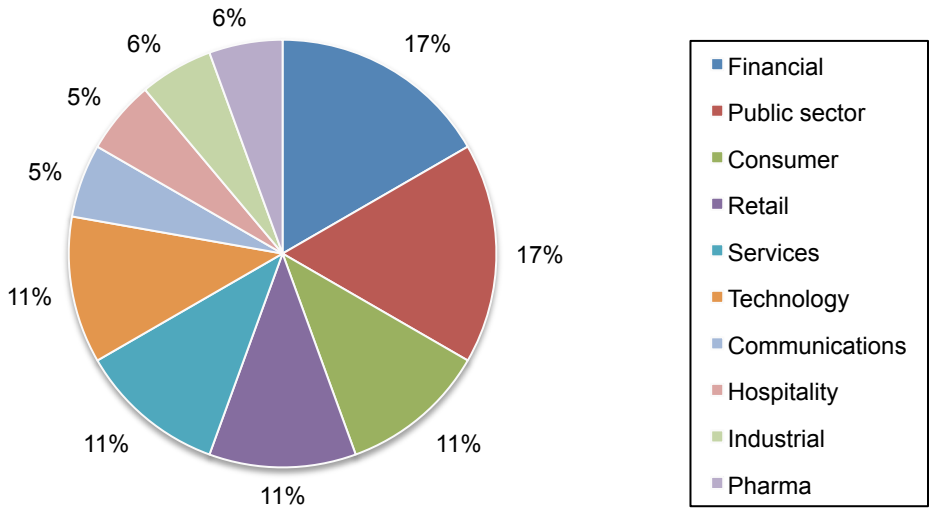
Part 3. Concluding observations and description about participating companies

This is the first study calculating the cost of data breach in Italian organizations. As the research reveals, the most profitable investments, as evidenced by the lower cost of data breach, are the organization's efforts to report the breach quickly and the appointment of a CISO with enterprise-wide responsibility.

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.

Figure 22 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 10 industries are represented. Financial services, public sector (government), retail and hospitality represent the four largest segments.

Figure 22. 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.[5]
- 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.[6] 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.

[5]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.

[6]In 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.[7]

Data collection methods did not include actual accounting information, but instead relied upon a numerical estimation based upon 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

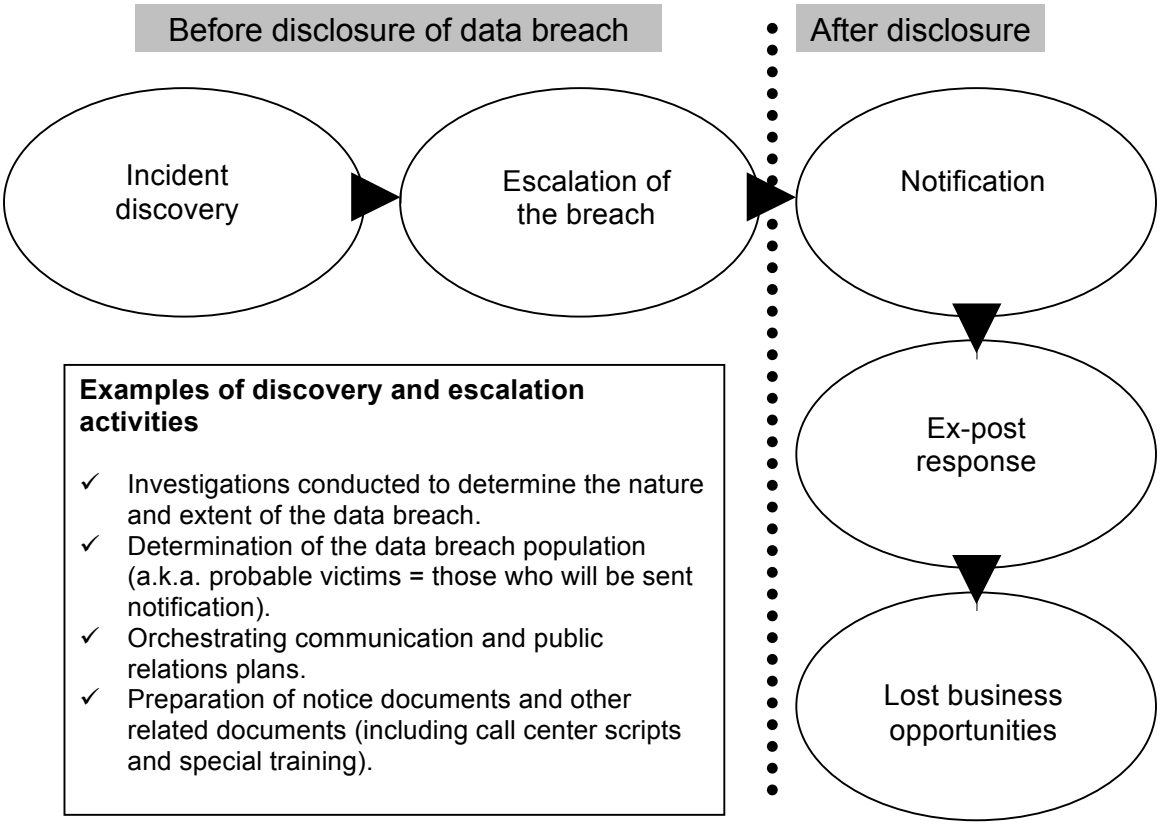
The numerical value obtained from the number line rather than a point estimate for each presented cost category preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

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

[7]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 23 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 23: 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 Italian-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. Eighteen 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 18 Data Breach Case Studies

Appendix: Data Table for Italy Sample						
Cases	Size of breach	Detection & escalation	Notification	Ex-post response	Lost business	Abnormal Churn
1	4,280	103,532	8,133	127,796	3,025	0.0%
2	33,800	524,262	143,221	680,853	110,840	1.4%
3	14,500	542,807	2,922	329,832	28,291	0.0%
4	4,395	394,315	11,109	96,788	5,288	4.7%
5	4,100	195,057	18,114	85,594	59,829	3.6%
6	12,000	1,284,819	27,276	257,769	821,267	6.9%
7	10,100	274,310	25,865	249,090	101,508	3.3%
8	36,730	863,099	103,574	1,715,529	574,618	7.9%
9	20,000	504,202	82,994	250,039	65,361	0.0%
10	2,600	100,555	55,907	60,972	26,904	5.5%
11	72,450	460,269	132,141	847,376	2,570,622	1.5%
12	33,265	914,371	155,603	711,176	834,553	1.0%
13	14,000	322,369	38,769	424,803	303,092	3.3%
14	4,724	49,077	13,979	240,066	689,634	7.6%
15	25,400	1,349,790	137,822	336,262	1,040,052	6.7%
16	6,100	36,058	5,427	26,384	143,865	1.1%
17	6,700	176,373	16,709	90,366	240,166	3.9%
18	15,200	164,295	55,436	608,825	927,365	4.1%