Ponemon
INSTITUTE

2013 Cost of Data Breach Study: Global Analysis

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

2013[1] Cost of Data Breach Study: Global Analysis
Ponemon Institute, May 2013

Part 1. Executive Summary

Symantec Corporation and Ponemon Institute are pleased to present the *2013 Cost of Data Breach: Global Analysis*, our eighth annual benchmark study concerning the cost of data breach incidents for companies located nine countries. Since 2009, we have provided a consolidated report of the benchmark findings from all countries represented in the research. In this report, we present both the consolidated findings and country differences.

The number of global organizations represented this year has grown to 277 in nine countries. More than 1,400 individuals were interviewed for this study during a ten-month period. In last year's report, 199 organizations from eight countries participated in this benchmark research.

As the findings reveal, the average per capita cost of data breach (compiled for nine countries and converted to US dollars) differs widely among the countries. Many of these cost differences can be attributed to the types of attacks and threats organizations face as well as the data protection regulations and laws in their respective countries. In this year's global study, the average consolidated data breach increased from $130 to $136. However, German and US organizations on average experienced much higher costs at $199 and $188, respectively.

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States eight years ago. Since then, we have expanded the study to include the United Kingdom, Germany, France, Australia, India, Italy, Japan and, for the first time this year, Brazil. To date, 965 business and government (public sector) organizations have participated in the benchmarking process since the inception of this research series.

As mentioned above, this year's study examines the costs incurred by 277 companies in 16 industry sectors after those companies experienced the loss or theft of protected personal data. It is important to note the costs presented in this research are not hypothetical but are from actual data loss incidents. They are based upon cost estimates provided by the individuals we interviewed over a ten-month period in the companies that are represented in this research.

The number of breached records per incident this year ranged from 2,300 records to more than 99,000 records. This year the average number of breached records was 23,647. 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 detailed cost data for the 277 data breach cases can be found as Appendix 1 in the nine separate country reports.

The report 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.

The following are the most salient country differences measured in US dollars:

- **The most and least expensive breaches.** German and US companies had the most costly data breaches ($199 and $188 per record, respectively). These countries also experienced the highest total cost (US at $5.4 million and Germany at $4.8 million). The least costly breaches occurred in Brazil and India ($58 and $42, respectively). In Brazil total cost was $1.3 million and in India it was $1.1 million.

---

[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.

- **Size of data breaches.** On average, Australian and US companies had data breaches that resulted in the greatest number of exposed or compromised records (34,249 and 28,765 records, respectively). On average, Italian and Japanese companies had the smallest number of breached records (18,285 and 18,237 records, respectively).

- **Causes of data breaches differ among countries.** German companies were most likely to experience a malicious or criminal attack, followed by Australia and Japan. Brazilian companies were most likely to experience breaches caused by human error. Companies in India were the most likely to experience a data breach caused by a system glitch or business process failure.

- **The most costly malicious and criminal attacks.** Consolidated findings show that malicious or criminal attacks are the most costly data breaches incidents in all nine countries. US and German companies experience the most expensive data breach incidents at $277 and $214 per compromised records, respectively. Brazil and India had the least costly data breach caused by malicious or criminal attackers at $71 and $46 per capita, respectively.

- **Factors that decrease the cost.** US and UK companies received the greatest reduction in data breach costs by having a strong security posture, incident response plan and CISO appointment. The US and France received the greatest cost reduction from the engagement of consultants to support data breach remediation.

- **Factors that increase the cost.** US companies realized the greatest increase in data breach costs if caused by a third party error or quick notification of data breach victims, regulators and other stakeholders. UK companies had the greatest increase in the cost of data breach if the incident involved a lost or stolen device.

- **Countries that lose the most customers following a data breach.** France and Australia had the highest rate of abnormal customer turnover or churn following a data breach. In contrast, Brazil and India had the lowest rate of abnormal churn. In the context of this study, abnormal churn is defined as the customer turnover caused by the data breach (above the churn experienced in the normal course of business).

- **Countries that spend the most and least on detection and escalation.** On average, German and Australian organizations spent the most on such detection and escalation activities as investigating and assessing the data breach ($1.3 million and $1.2 million, respectively). Organizations in India and Brazil spent the least on detection and escalation at $359,406 and $358,478, respectively.

- **Countries that spend the most and least on notification.** Some typical notification costs include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts and other efforts to make sure victims are alerted to the fact that their personal information has been compromised. US and Germany organizations on average spent the most ($565,020 and $353,927, respectively). Brazil and India spent the least amount on notification ($53,063 and $22,232, respectively).

Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews with more than 1,400 individuals in 277 organizations conducted over a ten-month period in nine countries. Recruiting organizations for the 2012 study began in January 2012 and interviews were completed in December. In each of the 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 incurred 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 typically the individual. As discussed previously, we recruited 277 organizations to participate in this study. All of these organizations experienced a data breach ranging from a low of about 1,000 to nearly 100,000 compromised records.

Can the average cost of data breach be used to calculate the financial consequences of a mega breach such as those involving millions of lost or stolen records?

The average cost of a data breach in our research does not apply to catastrophic or mega data breaches because these are not typical of the breaches most organizations experience. In order to be representative of the population of 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 in our analysis.

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 2005, we have studied the data breach experiences of 965 organizations.

Part 2. Key Findings

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

- Frequency of data breach incidents
- Cost of data breach per record and organization
- Root causes of a data breach
- Factors that influence the cost of a data breach
- Trends in the frequency of compromised records
- Trends in customer turnover or churn
- Data breach cost components

The following table contains the list of countries and legend used in forthcoming figures. The table also provides the 04/01/2013 Wall Street Journal conversion rates used to convert cost data into one common currency (US dollars).

Table 1. Country legend	Legend	Case studies	Currency	Conversion rate to US$
Australia	AU	21	AU Dollar	0.97
Brazil	BZ	31	Real	2.00
France	FR	26	Euro	0.76
Germany	DE	31	Euro	0.76
India	IN	28	Rupee	54.12
Italy	IT	22	Euro	0.76
Japan	JP	26	Yen	98.00
United Kingdom	UK	38	GBP	0.65
United States	US	54	Dollar	1.00

Number of exposed or compromised records. Figure 1 reports the average size of data breaches for organizations in the nine countries represented in this research. At an average of 34,249, Australia has the highest number of breached records. Our sample of Japanese organizations, on the other hand, experienced the lowest average number of breach records at 18,237.

By design, the data breach cases included in this research had a minimum value of 1,000 records and a maximum value of 100,000 records. As discussed, we do not include data breach cases in excess of 100,000 records because this would affect the findings and are not representative of the data breaches most companies experience.

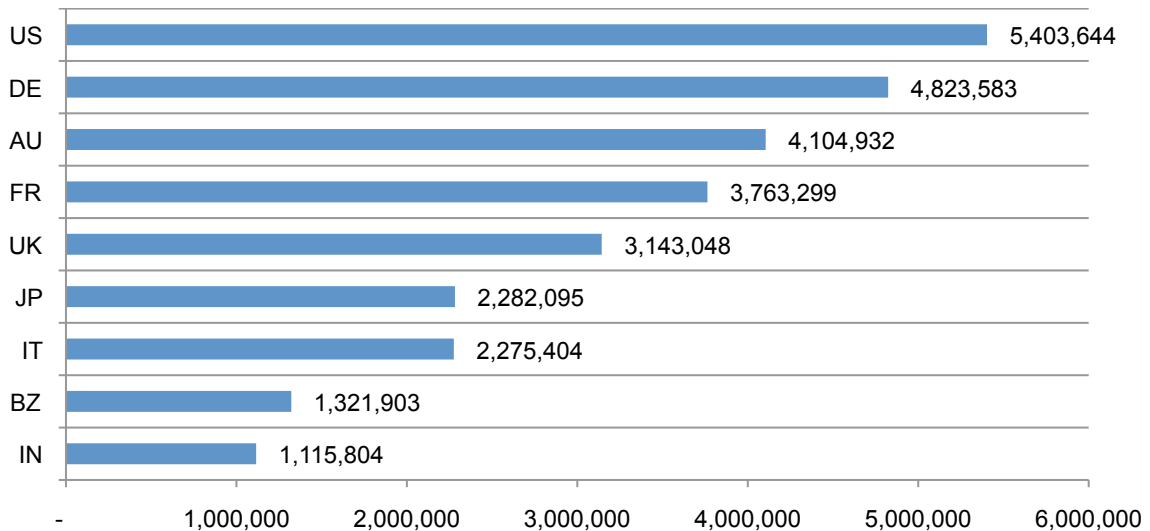**Figure 1. The average number of breached records**
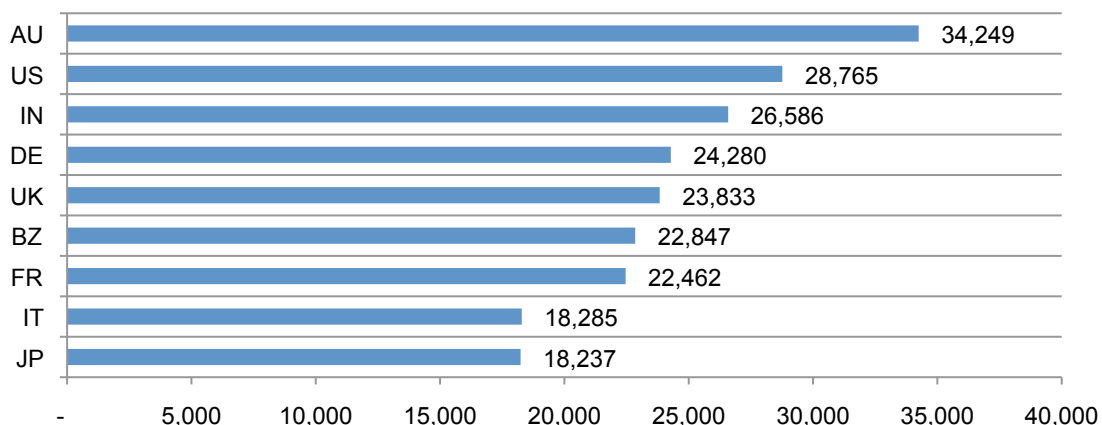
Per capita cost. Figure 2 reports the average per capita cost of a data breach expressed in US dollars for nine country studies. As shown there is marked variation among country samples.[2] The consolidated average per capita cost for all country samples was $136 compared to a $130 cost per compromised record calculated last year (excluding Brazil). Germany experienced the highest per capita cost of data breach at $199 and India experienced the lowest cost at $42 per compromised record.

Figure 2. The average per capita cost of data breach over two years
Measured in US$

■ FY 2012 (n = 277) ■ FY 2011 (n = 199)
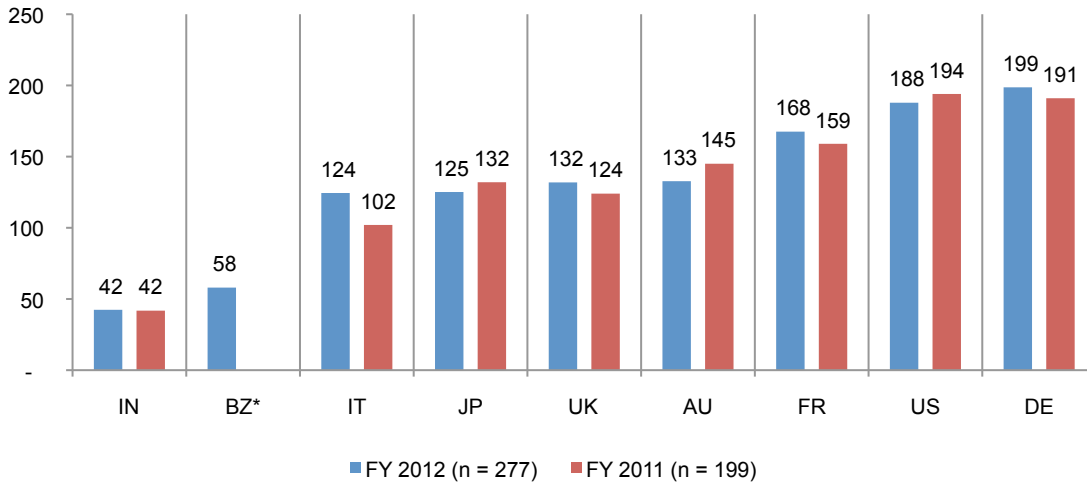
Average organizational cost of data breach varies by country. Figure 3 presents the total average cost of data breach for nine country studies in this year's study. As can be seen, the US sample experienced the highest total average cost at more than $5.4 million, followed by Germany at $4.8 million. In sharp contrast, samples of Brazilian and Indian companies experienced the lowest total average cost at $1.3 million and $1.1 million, respectively.

Figure 3. The average total organizational cost of data breach
Measured in US$

US 5,403,644
DE 4,823,583
AU 4,104,932
FR 3,763,299
UK 3,143,048
JP 2,282,095
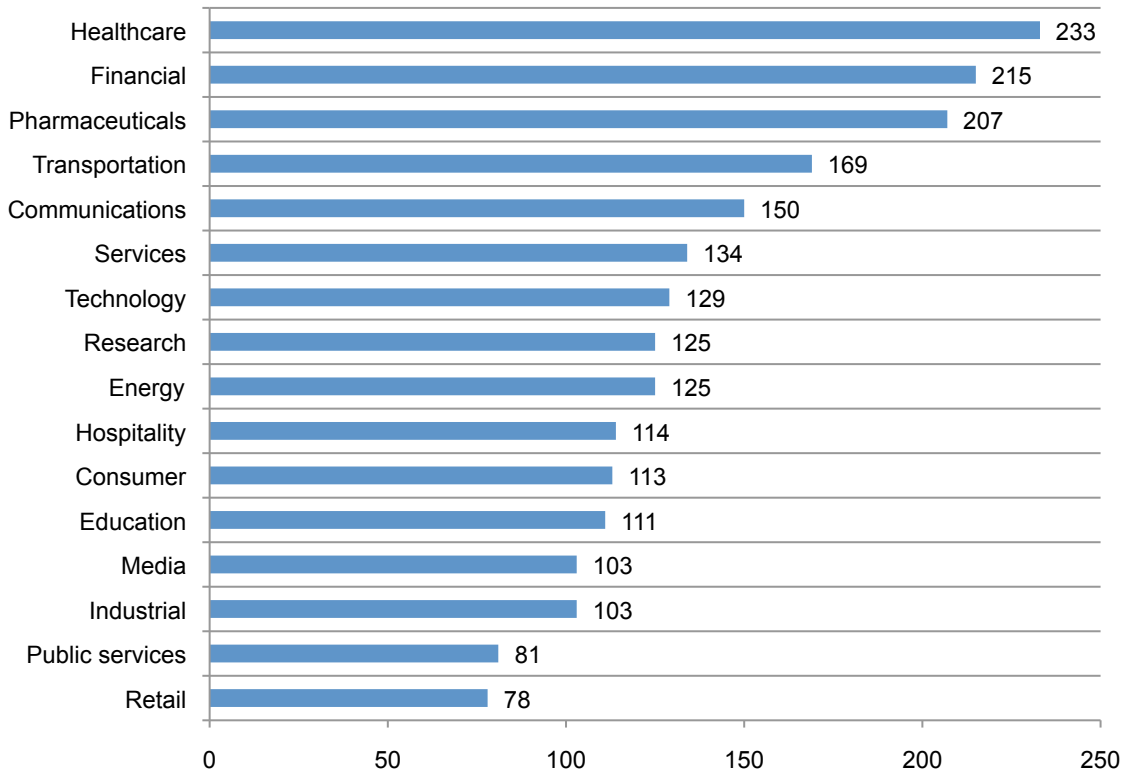IT 2,275,404
BZ 1,321,903
IN 1,115,804

---

[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 lost or stolen records.

Certain industries have higher data breach costs. Figure 4 reports the per capita costs for the consolidated sample by industry classification. Heavily regulated industries such as healthcare, financial, pharmaceuticals, transportation and communications had a per capita data breach cost substantially above the overall mean of $136. Retailers and public sector organizations had a per capita cost well below the overall mean value.

Figure 4. Per capita cost by industry classification
Consolidated view (n=277). Measured in US$

Industry	Per capita cost
Healthcare	233
Financial	215
Pharmaceuticals	207
Transportation	169
Communications	150
Services	134
Technology	129
Research	125
Energy	125
Hospitality	114
Consumer	113
Education	111
Media	103
Industrial	103
Public services	81
Retail	78

Malicious or criminal attacks are most often the cause of data breach globally.[3] Figure 5 provides a summary of the main root causes of data breach on a consolidated basis for all nine country samples. Over 37 percent of incidents involved a malicious or criminal attack, 35 percent concerned a negligent employee or contractor (human factor), and 29 percent involved system glitches that includes both IT and business process failures.[4]

Figure 5. Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=277)

- Malicious or criminal attack
- System glitch
- Human factor
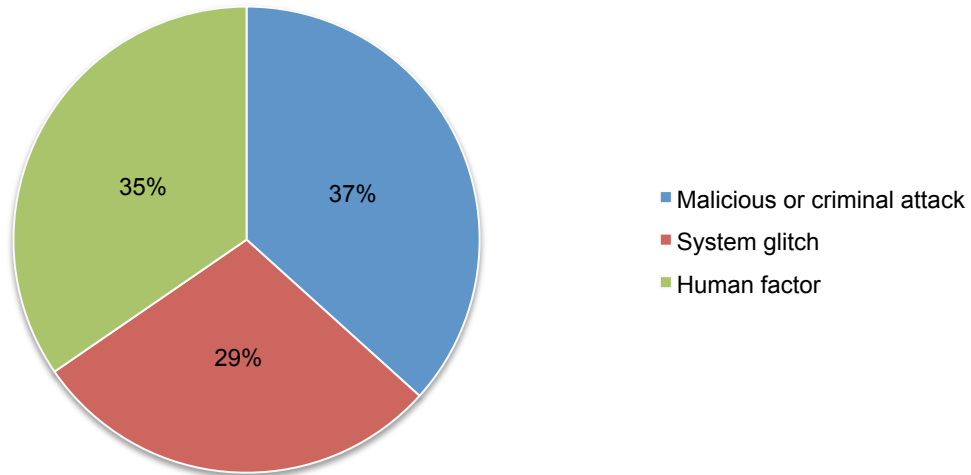
Figure 6 presents the main root causes of data breach for nine country samples. At 48 percent, German companies are most likely to experience a malicious or criminal attack. In contrast, Brazilian companies were least likely to experience such data breaches and most likely experienced a breach caused by human errors. Indian companies were most likely to experience a data breach caused by a system glitch or business process failure.

Figure 6. Distribution of the benchmark sample by root cause of the data breach

Malicious or criminal attack   System glitch   Human factor

---
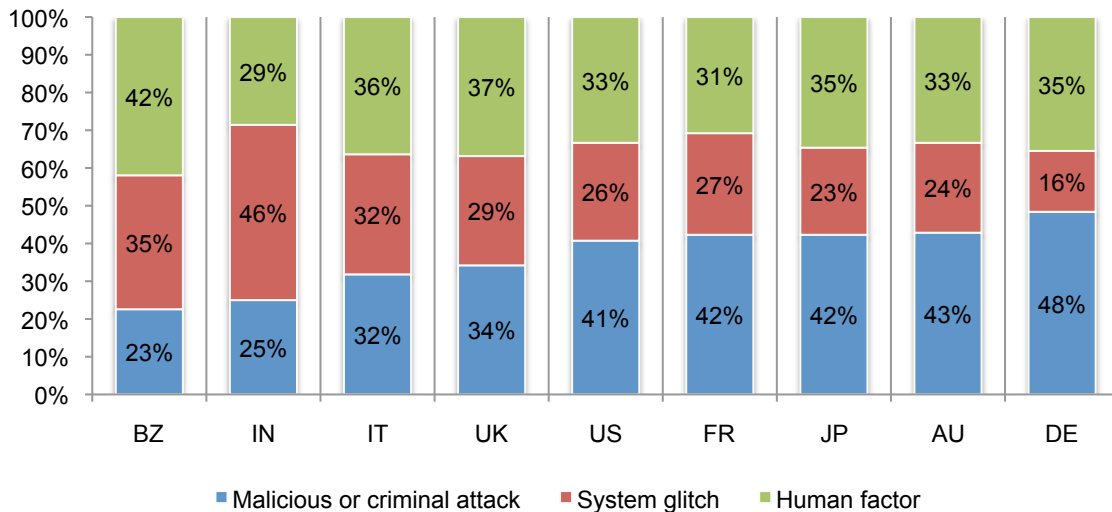
[3]Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation. Malicious attacks can be caused by hackers or criminal insiders (employees, contractors or other third parties).
[4]The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Malicious attacks are more costly globally. Figure 7 reports the per capita cost of data breach for three root causes of the breach incident on a consolidated basis. These results show data breaches due to malicious or criminal attacks cost companies an average of ($157). This is significantly above the consolidated mean of $136 per compromised record and the per capita cost for breaches caused by system glitch and human factors ($122 and $117, respectively).

Figure 7. Per capita cost for three root causes of the data breach
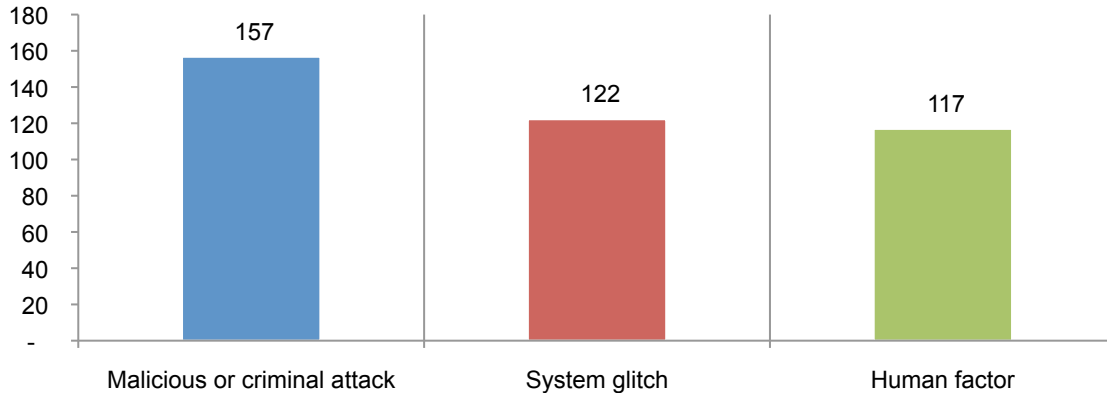Consolidated view (n=277). Measured in US$

Figure 8 reports the per capita cost of data breach by country sample for three root causes. These results clearly show data breach costs resulting from malicious or criminal attacks were consistently higher than those costs resulting from system glitches or human error. This graph also shows wide variation across country samples. That is, the US cost of a malicious or criminal data breach incident was $277 per compromised record. In India, this per capita cost was only $46.

**Figure 8. Per capita cost for three root causes of the data breach**
Measured in US$
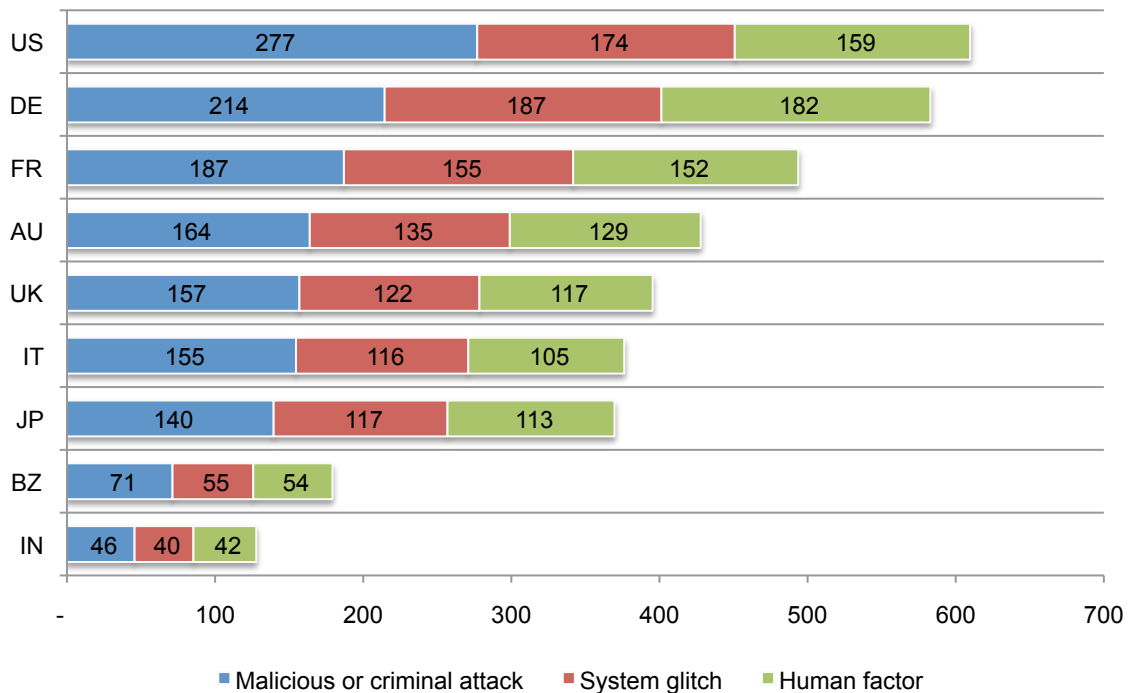
Seven factors that influence the cost of data breach. We identified seven factors that influence the cost consequences of a data breach incident. These attributes are defined as follows:

- **The company had an incident management plan**. Organizations 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**. 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.[5]

- **CISO (or equivalent title) has overall responsibility for enterprise data protection**. 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**. Organizations had a data breach caused by a third party, such as vendors, outsourcers and business partners.

- **The company notified data breach victims quickly.** Organizations notified data breach victims and/or regulators within 30 days after the discovery of data loss or theft.

- **The data breach involved lost or stolen devices.** 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**. Organizations engaged consultants to assist in their data breach response and remediation.

As shown in Figure 9, a strong security posture, incident response planning CISO appointments and consulting support decreases the per capita cost of data breach (shown as negative numbers). Third party errors, lost or stolen devices and quick notification increases the per capita cost of data breach (shown as positive numbers).

Figure 9. Impact of seven factors on the per capita cost of data breach
Consolidated view (n=277). Measured in US$

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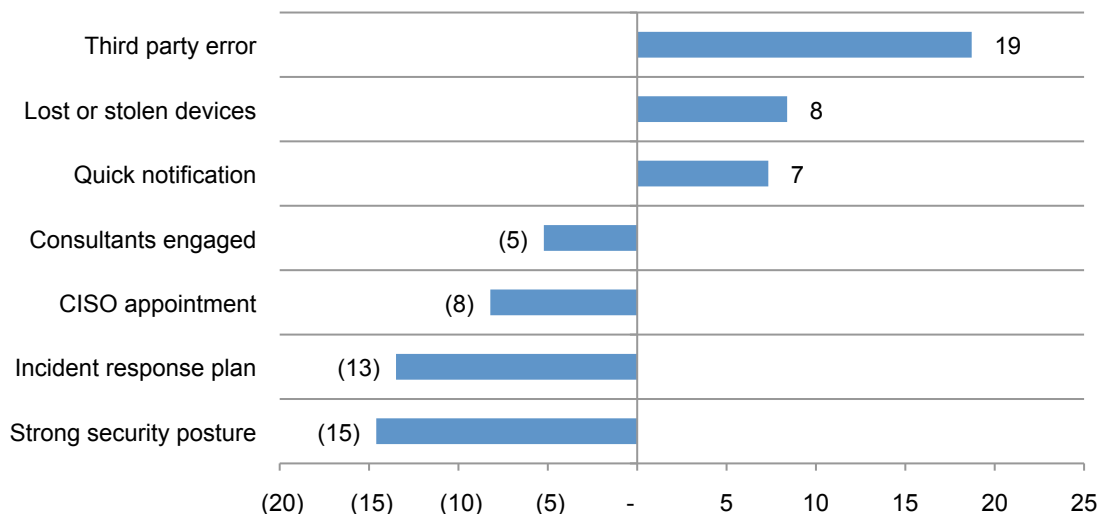
[5]The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 40 independent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

The following figures show the impact of these seven factors by country. It is clear from this analysis that the magnitude or impact of each factor on per capita data breach cost varies by country. According to Figure 10a, a strong security posture in US organizations had the potential to reduce the costs by as much as $34. Strong security postures did not have as significant an impact among Australian, Brazil and Indian organizations.

**Figure 10a. Strong security posture (US$)**
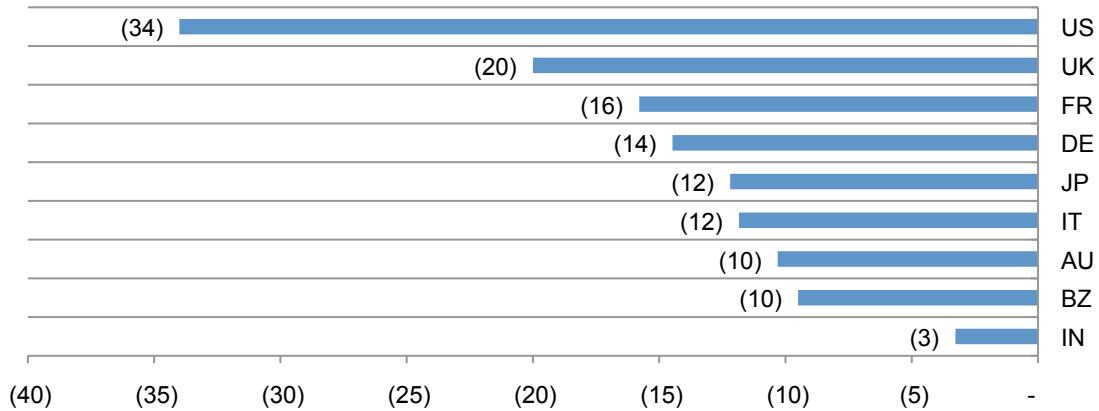
According to Figure 10b, US organizations should make sure they have an incident response plan in place because it could reduce the cost by as much as $42. Such planning did not seem to benefit organizations in Brazil, Australia and India.

**Figure 10b. Incident response plan (US$)**
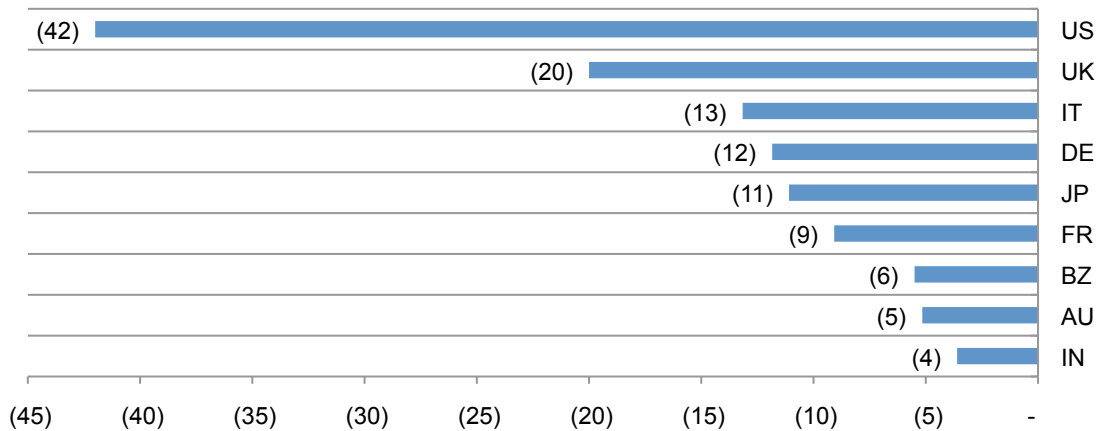
Where are CISOs most influential in reducing the cost of data breach? According to the research, US and UK organizations had a reduced cost of data breach because of the appointment of a CISO. This factor did not have the same level of impact in India and Brazil.

Figure 10c. CISO appointment (US$)
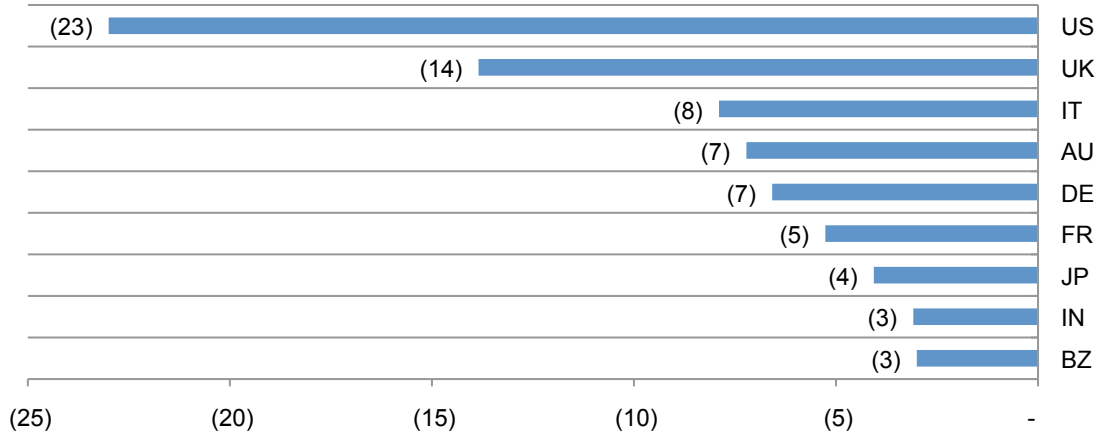
Once again, the factors that can decrease the cost of data breach benefited US organizations. In the US, those organizations that hired consultants to help them contain and resolve the incident were able to reduce the cost an average of $13 per compromised or exposed record. Organizations in Brazil and India that engage consultants did not realize as much cost savings.

**Figure 10d. Consultants engaged (US$)**
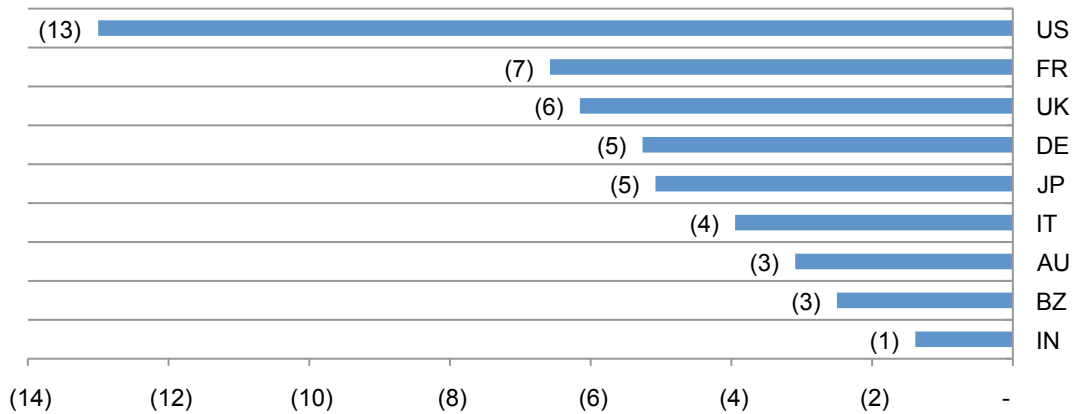
Figures 11a, 11b and 11c show the factors that increased the cost of data breach. On average, third party errors increased the cost of data breach by as much as $43 per record in the US In the case of Brazil and India, such incidents increased the cost by only $10 and $6, respectively.

Figure 11a. Third party error (US$)
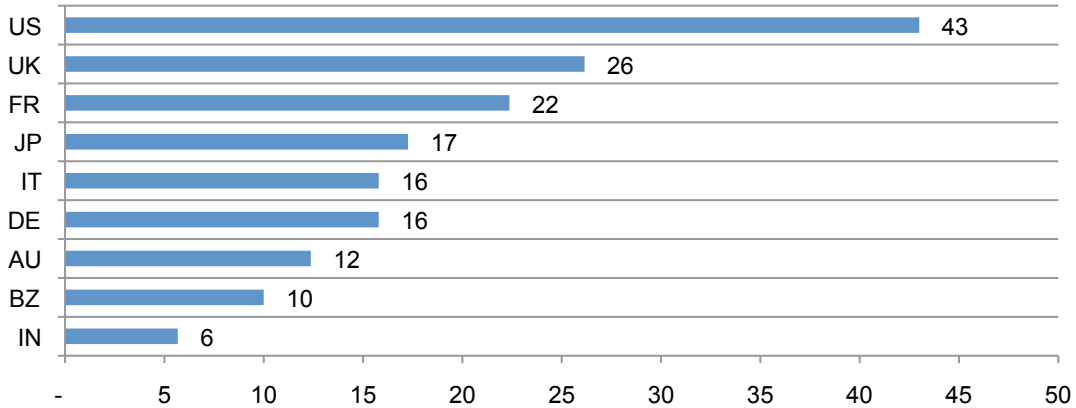

As shown in Figure 11b, if the data breach involved lost or stolen devices the cost was increased by as much as $15 per record followed by German organizations at $11. Again, Brazil and India are at the low end of increased costs.

Figure 11b. Lost or stolen devices (US$)
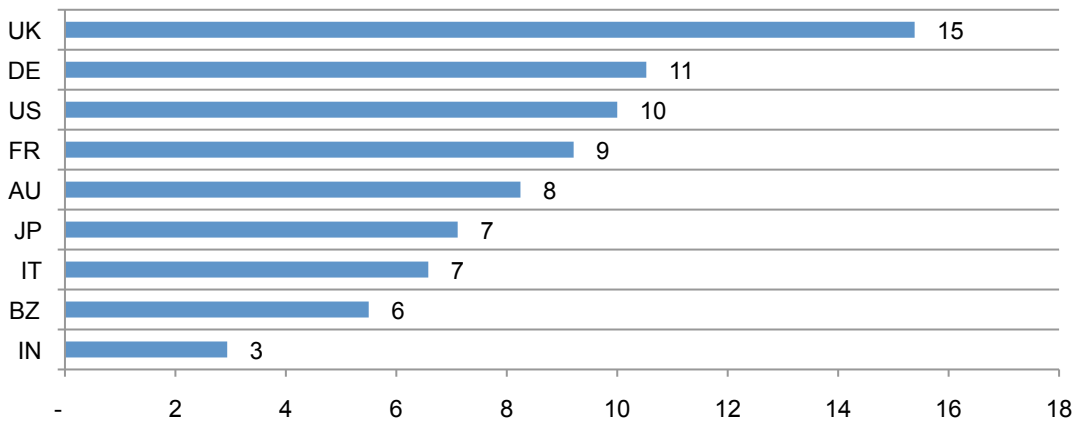
In many countries, regulations dictate the notification of data breach victims. However, if organizations are too fast in contacting individuals it can actually result in higher costs. In this year's study, in the US quick notification added as much as $37 per record, as shown in Figure 11c. It is understandable that this factor would have little impact on Brazil and India, because data breach notification regulations are non-existent.

Figure 11c. Quick notification (US$)

Country	Value
US	37
DE	8
IT	5
FR	5
AU	5
JP	4
BZ	3
IN	1
UK	(3)
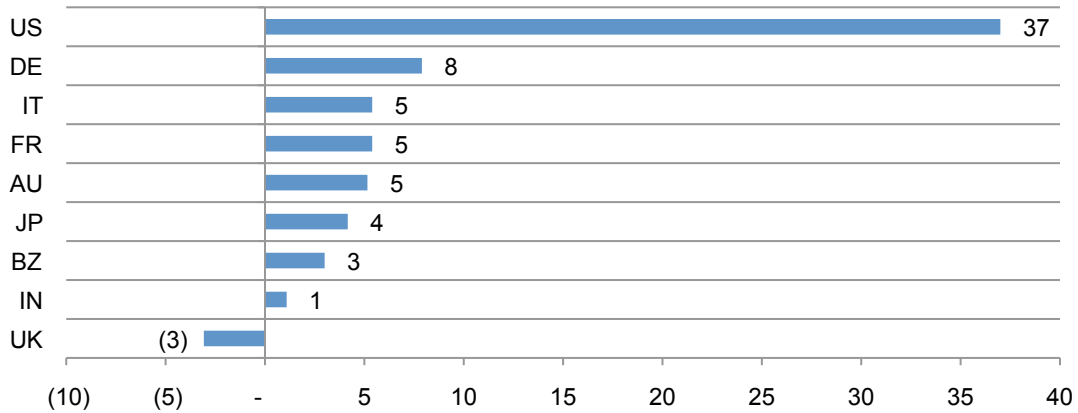
The more records lost, the higher the cost of the data breach. Figure 12 shows the relationship between the total cost of data breach and the size of the incident for 277 organizations in ascending order by the size of the breach incident. The regression line clearly indicates that the size of the data breach incident and total costs are linearly related.

Figure 12. Total cost of data breach by size of the data breach
Regression = Intercept + {Size of Breach Event} x β, where β denotes the slope.
Measured in US$

Ascending order by size of breach

Total cost .... Regression
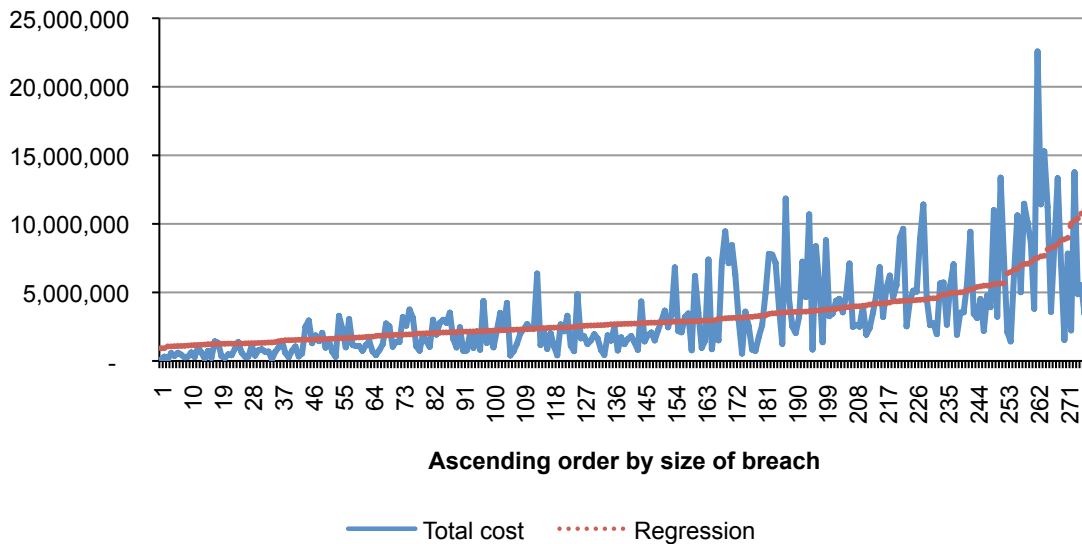
The more churn, the higher the per capita cost of data breach. Figure 13 reports the distribution of per capita data breach costs in ascending rate of abnormal churn for 277 organizations in nine countries. The regression line is upward sloping, which suggests that abnormal churn and per capita costs are linearly related. This pattern of results is consistent with benchmark studies completed in prior years.

Figure 13. Distribution of abnormal churn rates in ascending order by per capita costs
Regression = Intercept + {abnormal churn rate} x β, where β denotes the slope.
Measured in US$

**Ascending order by abnormal churn rates**

Per capita cost   Regression
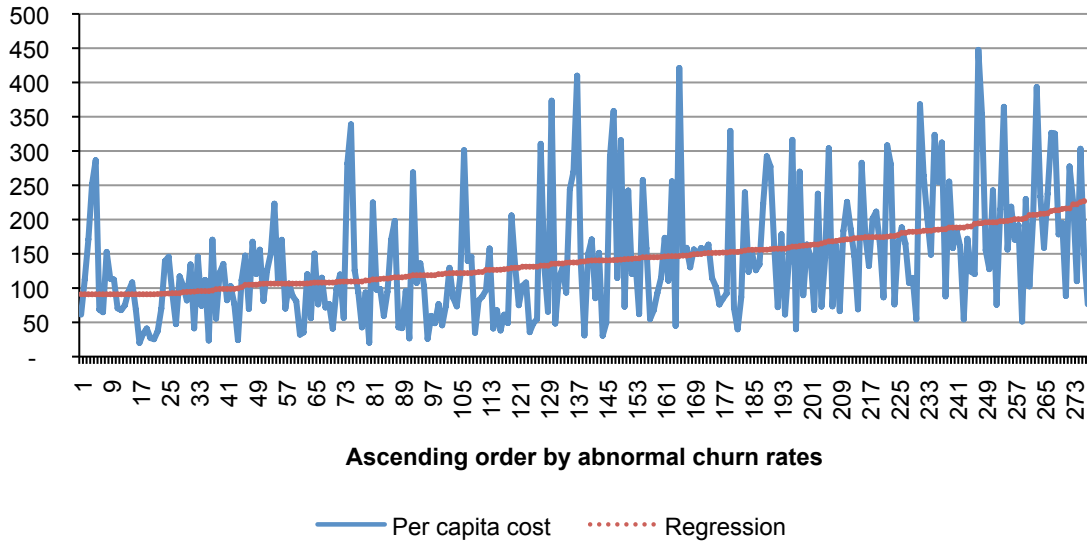
Certain countries are more vulnerable to churn. Figure 14 reports the average abnormal churn rates for nine country samples. Our 2012 global results show marked differences among countries. Specifically, France experienced the highest rate of abnormal churn at 4.4 percent and Brazil experienced the lowest churn rate.[6]

The implications of this analysis is that countries with the highest churn rates could significantly reduce the costs of a data breach by putting an emphasis on customer retention and activities to preserve reputation and brand value.

**Figure 14. Abnormal churn rates by country sample**

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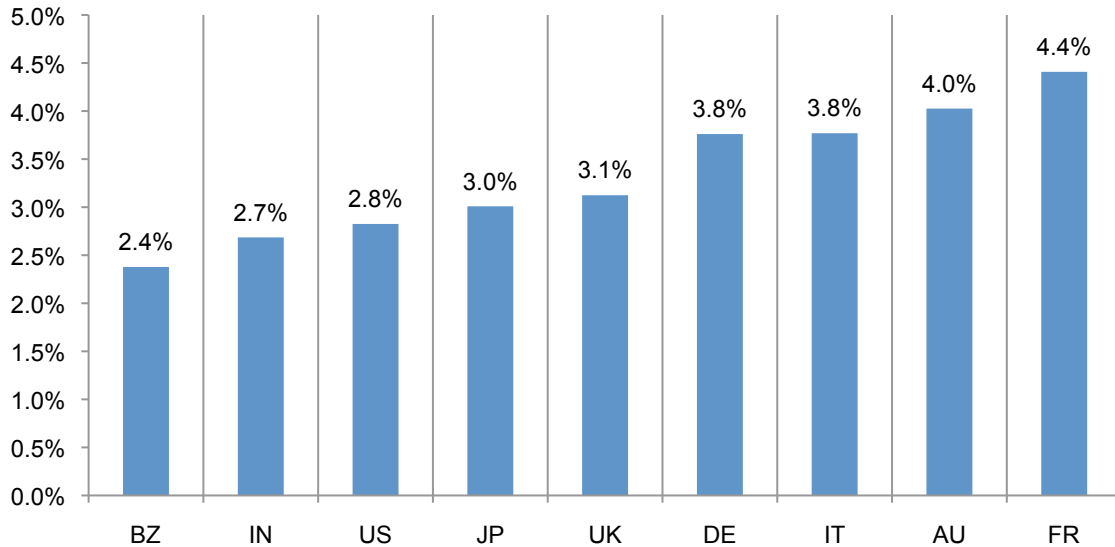
[6]Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have an alternative choice.

Detection and escalation costs. Figure 15 shows the costs associated with detection and escalation of data breach incidents for nine countries. 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, German companies experienced the highest detection and escalation costs and Brazil and India experienced the lowest cost.

Figure 15. Average detection and escalation costs
Measured in US$
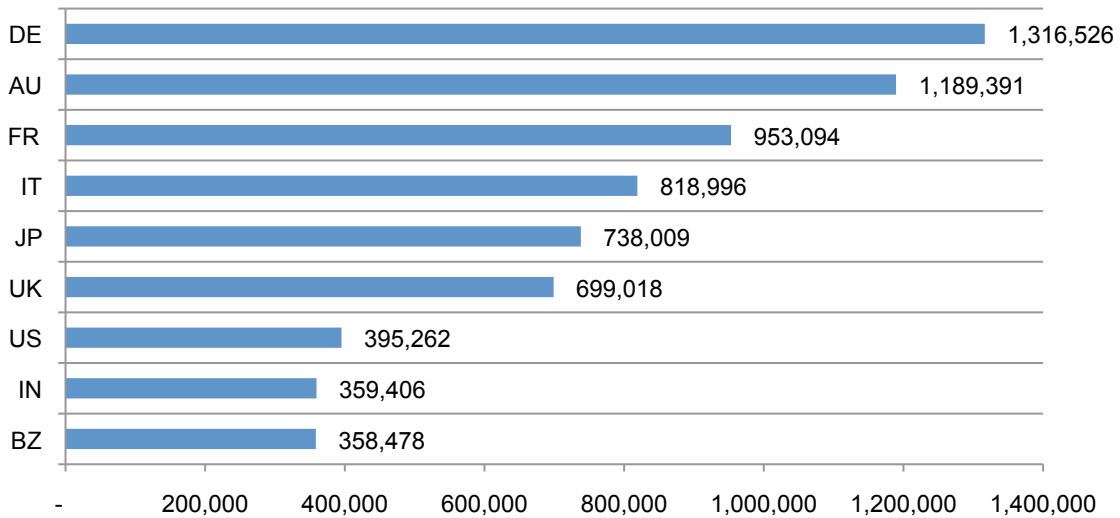
Notification costs. Figure 16 reports the distribution of costs associated with notification activities for nine countries. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up. The US sample experienced the highest notification cost.

Figure 16. Average notification costs
Measured in US$
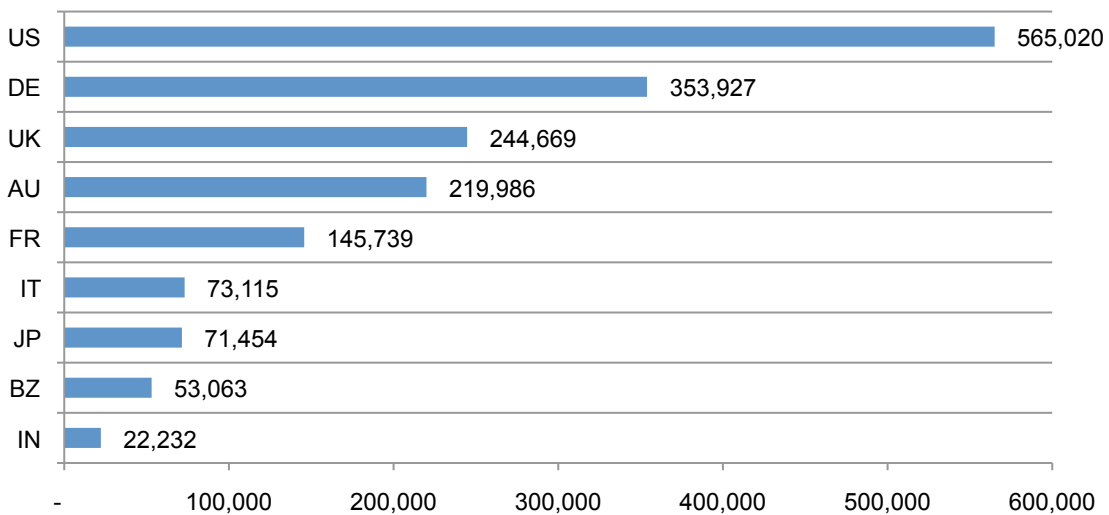
Post data breach costs. Figure 17 shows the distribution of costs associated with ex-post (after-the-fact) activities for nine countries. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Here again, US organizations experienced the highest ex-post response costs.

Figure 17. Average ex-post response costs
Measured in US$

Country	Value
US	1,412,548
DE	1,406,663
AU	1,101,437
FR	1,094,514
UK	782,245
JP	728,294
IT	592,394
IN	450,825
BZ	395,419

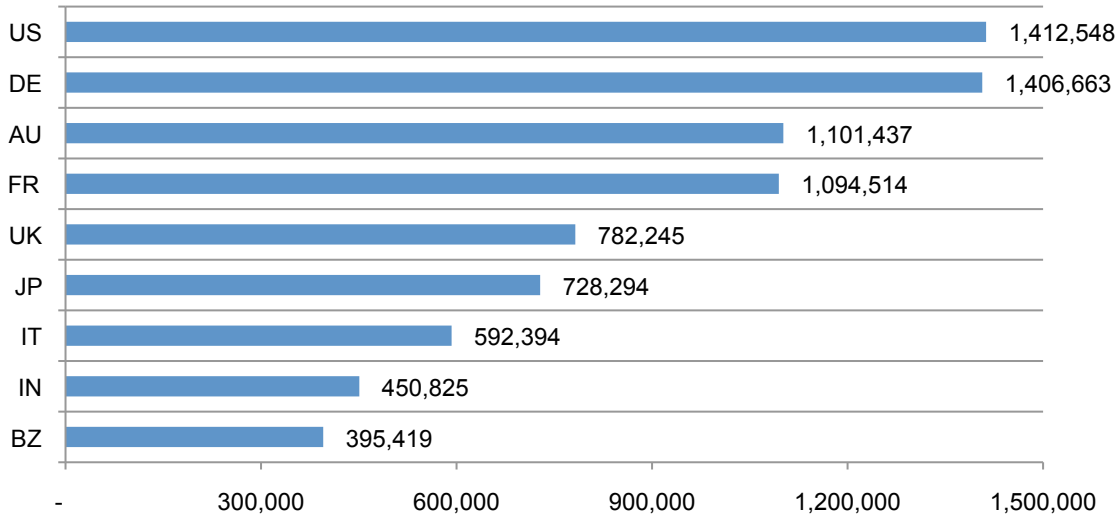**Lost business costs.** Figure 18 reports lost business costs associated with data breach incidents for nine countries. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen, lost business costs over the past few years appear to be trending downward. The highest lost business cost of over $3.03 million was experienced by US organizations.

Figure 18. Average lost business costs
Measured in US$

| Country	Value
US	3,030,814
AU	1,957,966
DE	1,746,467
FR	1,569,953
UK	1,417,116
IT	790,899
JP	744,338
BZ	514,944
IN	283,341
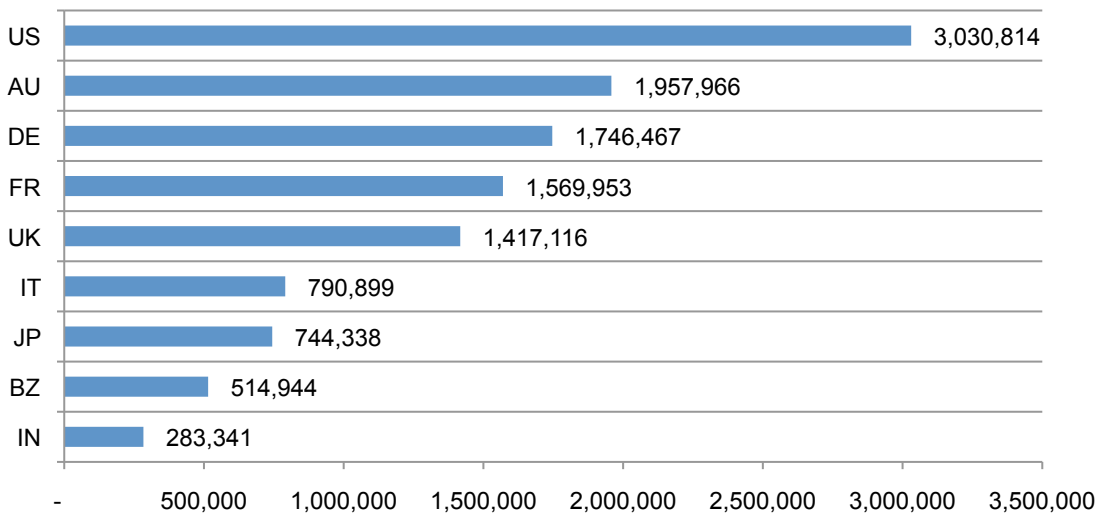
Net change in lost business costs. Figure 19 reports lost business costs as a percent of total average cost for nine countries. As can be seen, three countries experienced a net percentage increase over two years, while five countries experienced a net percentage decrease. The largest percentage increases over two years occurred in India (+13 percent) and France (+11 percent). Australian companies experienced the largest percentage decrease between the 2012 and 2013 lost business costs (-10 percent).

Figure 19. Percentage of lost business costs relative to total average cost
Brazil (BZ) is not included because 2013 is the first year of this study

■ 2012 Lost business costs as a percentage to total cost
■ 2013 Lost business costs as a percentage to total cost
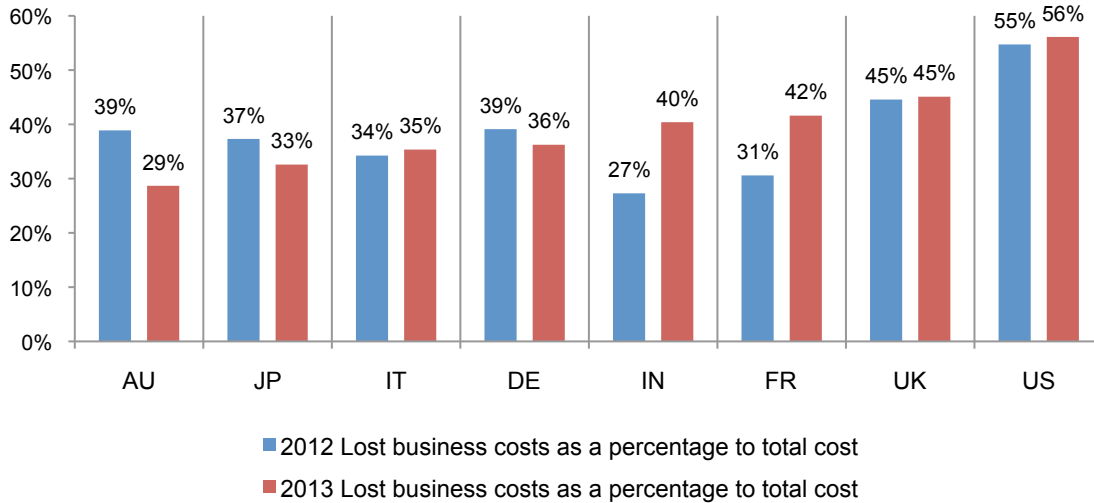
The proportion of direct and indirect costs of data breach varies by country. Direct costs refer to the direct expense outlay to accomplish a given activity such as engaging forensic experts, hiring a law firm or offering victims identity protection services. Indirect costs include the time, effort and other organizational resources spent during the data breach resolution. It includes the use of existing employees to help in the data breach notification efforts or in the investigation of the incident. Indirect costs also include the loss of goodwill and customer churn.

Figure 20 reports the direct and indirect per capita cost components of a data breach on a percentage basis for nine countries. As shown, US companies have the highest percentage of indirect cost and Brazil has the highest percentage direct cost.

Figure 20. Percentage direct and indirect per capita data breach cost

■ Indirect ■ Direct
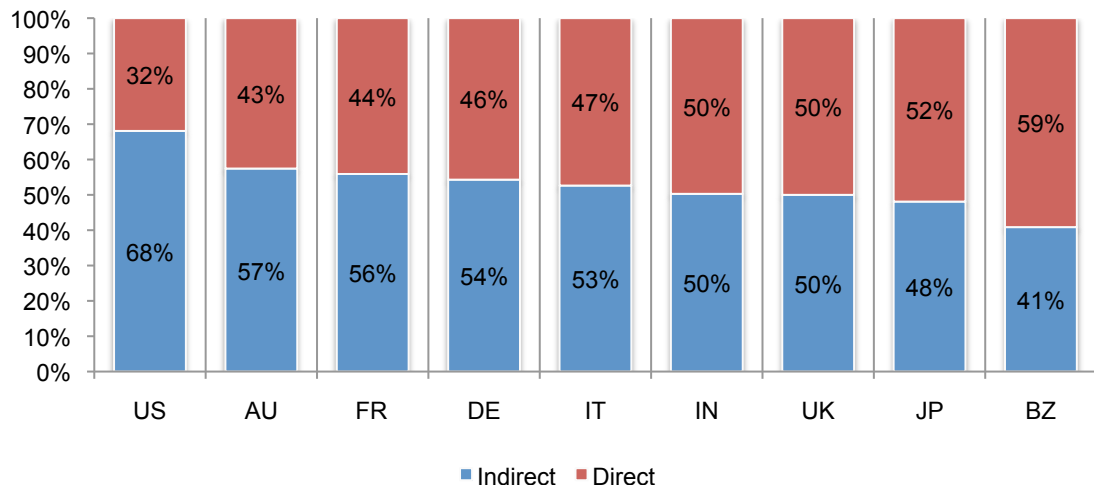
Part 3. Observations and description about participating companies

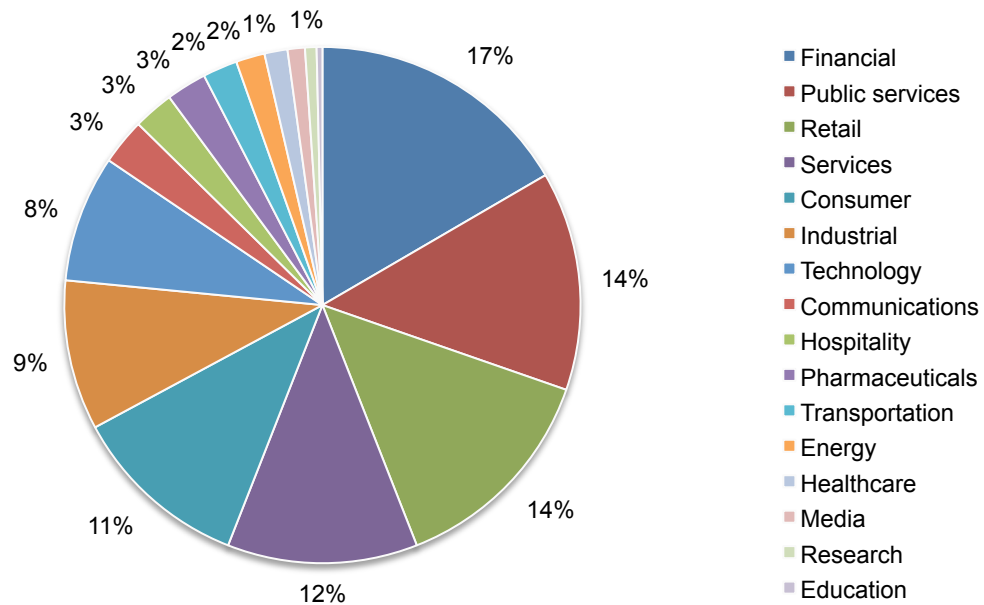We conclude that companies' efforts in improving their data protection practices are paying off. As evidenced by the nine global studies, the most profitable investments companies can make seem to be an incident response plan, a strong security posture, the appointment of a CISO with enterprise-wide responsibility and the engagement of outside consultants.

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 nine separate country studies. 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 recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint, and size of data breach.

Figure 21 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 16 industries are represented. The largest sector is financial services, which includes banks, insurance, investment management and payment processors.

Figure 21. Distribution of the benchmark sample by industry segment
Consolidated (n = 277 organizations)

Legend:
- Financial
- Public services
- Retail
- Services
- Consumer
- Industrial
- Technology
- Communications
- Hospitality
- Pharmaceuticals
- Transportation
- Energy
- Healthcare
- Media
- Research
- Education

Part 4. How we calculate the cost of 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.[7]

- 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.[8] 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).

---

[7] 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.

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

Benchmark methods

All participating organizations experienced one or more data breach incidents sometime over the past year, often requiring notification according various regulations and laws. 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.

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.[9]

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.

---

[9]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 22 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 22. Schema of the data breach process

| Before disclosure or notification of the incident | After disclosure |

Incident discovery → Escalation → Notification

Examples of discovery and escalation activities:

Investigating the incident to determine the root causes of the data breach.

Determining the data breach population (a.k.a. probable victims).

Organizing the incident response team.

Orchestrating communication and public relation plans.

Preparing notice documents and other required disclosures to data breach victims and regulators

Implementing call center procedures and specialized training.

Ex post response

Lost business opportunities

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.

Part 5. 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 organizations experiencing a breach involving the loss or theft of confidential data 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. In total, 277 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

<div style="border:1px solid black; padding:10px;">

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.

</div>