2016 Cost of Data Breach Study: Global Analysis

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
June 2016

2016[1] Cost of Data Breach Study: Global Analysis

Ponemon Institute, June 2016

Part 1. Introduction

IBM and Ponemon Institute are pleased to release the *2016 Cost of Data Breach Study: Global Analysis.* According to our research, the average total cost of a data breach for the 383 companies participating in this research increased from $3.79 to $4 million[2]. The average cost paid for each lost or stolen record containing sensitive and confidential information increased from $154 in 2015 to $158 in this year's study.

Global study at a glance

- 383 companies in 12 countries
- $4 million is the average total cost of data breach
- 29% increase in total cost of data breach since 2013
- $158 is the average cost per lost or stolen record
- 15% percent increase in per capita cost since 2013

In addition to cost data, our global study looks at the likelihood of a company having one or more data breach occurrences in the next 24 months. We estimate a 26 percent probability of a material data breach involving 10,000 lost or stolen records.

According to this year's findings, organizations in Brazil and South Africa are most likely to have a material data breach involving 10,000 or more records. In contrast, organizations in Germany and Australia are least likely to experience a material data breach.

In this year's study, 383 companies located in the following 12 countries participated: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, the Arabian region (United Arab Emirates and Saudi Arabia), Canada and, for the first time, South Africa. All participating organizations experienced a data breach ranging from approximately 3,000 to slightly more than 101,500 compromised records[3]. We define a compromised record as one that identifies the individual whose information has been lost or stolen in a data breach.

Seven global megatrends in the cost of data breach research

Over the many years studying the data breach experience of 2,013 organizations in every industry, the research has revealed the following seven megatrends.

1. Since first conducting this research, the cost of a data breach has not fluctuated significantly. This suggests that it is a permanent cost organizations need to be prepared to deal with and incorporate in their data protection strategies.

2. The biggest financial consequence to organizations that experienced a data breach is lost business. Following a data breach, organizations need to take steps to retain customers' trust to reduce the long-term financial impact.

3. Most data breaches continue to be caused by criminal and malicious attacks. These breaches also take the most time to detect and contain. As a result, they have the highest cost per record.

4. Organizations recognize that the longer it takes to detect and contain a data breach the more costly it becomes to resolve. Over the years, detection and escalation costs in our research

[1] This report is dated in the year of publication rather than the fieldwork completion date. Please note that the majority of data breach incidents studied in the current report happened in the 2015 calendar year.
[2] Local currencies were converted to U.S. dollars.
[3] The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

have increased. This suggests investments are being made in technologies and in-house expertise to reduce the time to detect and contain.

5. Regulated industries, such as healthcare and financial services, have the most costly data breaches because of fines and the higher than average rate of lost business and customers.

6. Improvements in data governance programs will reduce the cost of data breach. Incident response plans, appointment of a CISO, employee training and awareness programs and a business continuity management strategy continue to result in cost savings.

7. Investments in certain data loss prevention controls and activities such as encryption and endpoint security solutions are important for preventing data breaches. This year's study revealed a reduction in the cost when companies participated in threat sharing and deployed data loss prevention technologies.

The following are the most salient findings and implications for organizations:

Data breaches cost the most in the US and Germany and the lowest in Brazil and India. The average per capita cost of data breach was $221 in the US and $213 in Germany. The lowest cost was in Brazil ($100) and India ($61). The average total organizational cost in the US was $7.01 million and in Germany $5.01 million. The lowest organizational cost was in India ($1.6 million) and South Africa ($1.87 million).

The cost of data breach varies by industry. The average global cost of data breach per lost or stolen record was $158. However, healthcare organizations had an average cost of $355 and in education the average cost was $246. Transportation ($129), research ($112) and public sector ($80) had the lowest average cost per lost or stolen record.

Hackers and criminal insiders caused the most data breaches. Forty-eight percent of all breaches in this year's study were caused by malicious or criminal attacks. The average cost per record to resolve such an attack was $170. In contrast, system glitches cost $138 per record and human error or negligence was $133 per record. Companies in the US and Canada spent the most to resolve a malicious or criminal attack ($236 and $230 per record, respectively). India spent far less ($76 per record).

Malicious or criminal attacks vary significantly by country. Sixty percent of all breaches in the Arabian Cluster and 54 percent of all breaches in Canada were due to hackers and criminal insiders. Only 37 percent of all data breaches occurring in South Africa were due to malicious attacks. Instead, South African companies had the highest percentage of human error data breaches and Indian organization were most likely to experience a data breach caused by a system glitch or business process failure (37 percent and 35 percent, respectively).

Incident response teams and extensive use of encryption decreased the cost of data breach. An incident response team reduced the cost of data breach by $16 per record, from $158 to $142. In contrast, data breaches caused by third party involvement resulted in an increase of $14, from $158 to $172 per record.

Measures reveal why the cost of data breach increased. The average total cost of a data breach increased 5.4 percent and the per capita or record cost increased 2.9 percent. The average size of the data breach (number of records lost or stolen) increased 3.2 percent. Abnormal churn grew 2.9 percent, which is defined as the greater than expected loss of customers in the normal course of business.

The loss of customers increased the cost of data breach. Certain countries had more problems retaining customers following a data breach and, therefore, had higher costs. These are

France, Japan and Italy. Countries with the lowest churn rate are Brazil, South Africa and India. Industries with the highest churn are financial, health and services.

Certain countries and industries are more vulnerable to churn. France continued to experience the highest rate of churn followed by Japan. Public and retail experienced the lowest abnormal churn or turnover. While a small sample size prevents us from generalizing the affect of industry on customer churn rates, financial, health and service organizations experienced relatively high abnormal churn and public sector and education organizations experienced a relatively low abnormal churn.

The more records lost, the higher the cost of the data breach. In this year's study of 383 organizations, the cost ranged from $2.1 million for a loss of less than 10,000 records to $6.7 million for more than 50,000 lost or stolen records.

Detection and escalation costs were the highest in Canada and lowest in India. Data breach costs associated with detection and escalation are forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. The average detection and escalation costs for Canada was $1.60. In contrast, the average costs were $0.53.

Notification costs were the highest in the US. Lost business costs are abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished good will. In the US, the cost was $0.59 and in India the cost was $0.02.

Post data breach response costs were highest in US and Germany. The costs associated with post data breach response and detection in the US was $1.72 and $1.54 in Germany. Ex-post costs include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions.

US organizations paid the highest price for losing customers after a data breach. The cost of lost business was particularly high for US organizations ($3.97). This cost component includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.

The Arabian Region had the highest direct costs and the US has the highest indirect costs. 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 employees' assistance in the data breach notification efforts or in the investigation of the incident. Indirect costs also include the loss of goodwill and customer churn. The Arabian Region had the highest percentage (57 percent) of direct costs and the US had the highest percentage (66 percent) of indirect costs.

Certain countries are more likely to have a data breach. For the past three years, the research has studied the likelihood of one or more data breach occurrences. Brazil and South Africa appear to have the highest estimated probability of occurrence. Germany and Australia have the lowest probability of data breach.

Time to identify and contain a data breach affects the cost. For the second year, our study shows the relationship between how quickly an organization can identify and contain data breach incidents and financial consequences. Both the time to identify and time to contain was highest for malicious and criminal attacks (229 and 82 days, respectively) and much lower for data breaches caused by human error (162 and 59 days, respectively).

Cost of Data Breach FAQs

What is the purpose of this research? Our goal is to quantify the economic impact of data breaches and observe cost trends over time. We believe a better understanding of the cost, the root causes and factors that influence the cost will assist organizations in determining the appropriate amount of investment and resources needed to prevent or mitigate the consequences of an attack.

What is a data breach? A breach is defined as an event in which an individual's name plus a medical record and/or a financial record or debit card is potentially put at risk—either in electronic or paper format. In our study, we have identified three main causes of a data breach: a malicious or criminal attack, system glitch or human error. The costs of a data breach can vary according to the cause and the safeguards in place at the time of the data breach.

What is a compromised record? We define a record as information that identifies the natural person (individual) whose information has been lost or stolen in a data breach. Examples can include a retail company's database with an individual's name associated with credit card information and other personally identifiable information. Or, it could be a health insurer's record of the policyholder with physician and payment information. In this year's study, the average cost to the organization if one of these records is lost or stolen is $158.

How do you collect the data? Ponemon Institute researchers collected in-depth qualitative data through more than 1,500 separate interviews conducted over a ten-month period. Recruiting organizations for the 2016 study began in January 2015 and interviews were completed in March 2016. In each of the 383 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? 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 customer acquisition rates.

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. We recruited 383 organizations to participate in this study. Data breaches ranged from a low of 3,000 to slightly more than 101,500 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 such as Sony because these are not typical of the breaches most organizations experience. In order to be representative of the population of global 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 approximately 100,000 compromised records in our analysis.

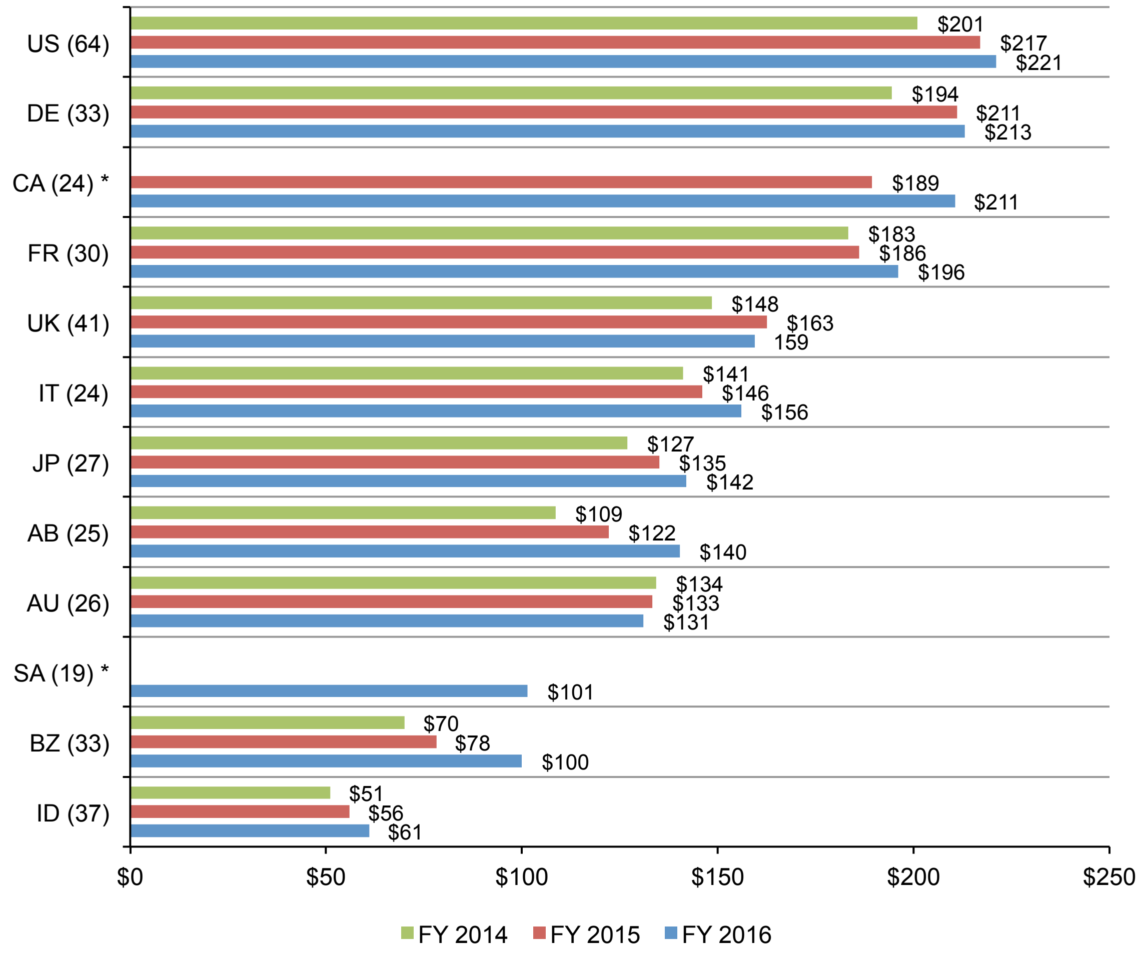
Are you tracking the same organizations each year? Each annual study involves a different sample of companies. In other words, we are not tracking the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach. Since starting this research in 2005, we have studied the data breach experiences of 2,013 organizations globally.

Global at a glance

This year's annual study was conducted in 12 countries: United States, Germany, Canada, France, United Kingdom, Italy, Japan, Australia, Arabian Cluster, Brazil, India and, for the first time, South Africa. A total of 383 organizations participated. Country-specific results are presented in 12 separate reports.

Figure 1 presents the average per capita cost of data breach over three years expressed in US dollars for 12 country studies. As shown, there is significant variation among country samples.[4] The consolidated average per capita cost for all countries was $158 compared to an average of $154 average last year (excluding South Africa). The US and Germany continue to have the highest per capita costs at $221 and $213, respectively. India and Brazil had the lowest costs at $61 and $100, respectively.

Figure 1. The average per capita cost of data breach over three years
Grand average for FY 2016=$158, FY 2015=$154, FY 2014=$145
*Historical data is not available in all years
(FY 2016=383, FY 2015=350, FY 2014=315)
Measured in US$



[4] Per capita cost is defined as the total cost of data breach divided by the size of the data breach (i.e., the number of lost or stolen records).

Part 2. Key Findings

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

- Global and industry differences in cost of data breach
- Root causes of a data breach
- Factors that influence the cost of data breach
- Trends in the frequency of compromised records and customer turnover or churn
- Trends in the cost components of data breach
- The likelihood an organization will have a data breach
- Mean time to identify and contain a data breach
- The impact of business continuity management on the cost of data breach

The following table lists 12 countries, legend, sample sizes and currencies used in this global study. It also shows the number of years of annual reporting for each country ranging from one year for Canada to 11 years for the United States.

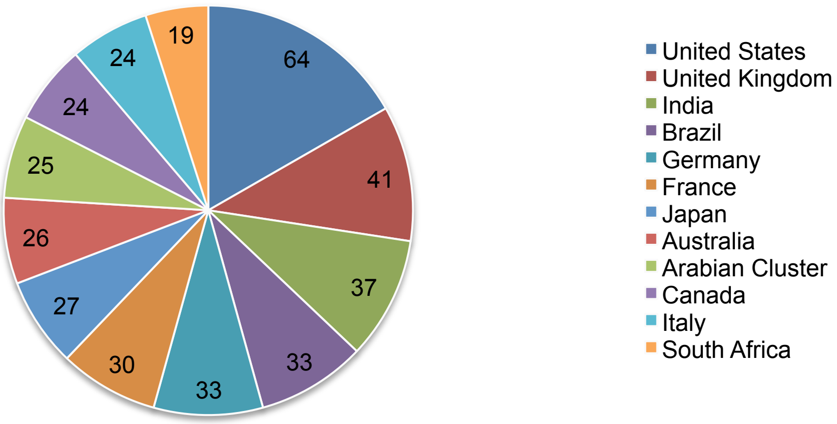
Table 1. Global Study at a Glance

Legend	Countries	Sample	Pct%	Currency	Years of study
AB	Arabian Cluster*	25	7%	AED/SAR	3
AU	Australia	26	7%	AU Dollar	7
BZ	Brazil	33	9%	Real	4
CA	Canada	24	6%	CA Dollar	2
DE	Germany	33	9%	Euro	8
FR	France	30	8%	Euro	7
ID	India	37	10%	Rupee	5
IT	Italy	24	6%	Euro	5
JP	Japan	27	7%	Yen	5
SA	South Africa	19	5%	ZAR	1
UK	United Kingdom	41	11%	GBP	9
US	United States	64	17%	US Dollar	11
	Total	383	100%		

*AB is a combined sample of companies located in Saudi Arabia and the United Arab Emirates

The following chart shows the distribution of 383 participating organizations within 12 countries. As can be seen, the US represents the largest segment with 64 organizations and South Africa had the smallest sample with 19 organizations.

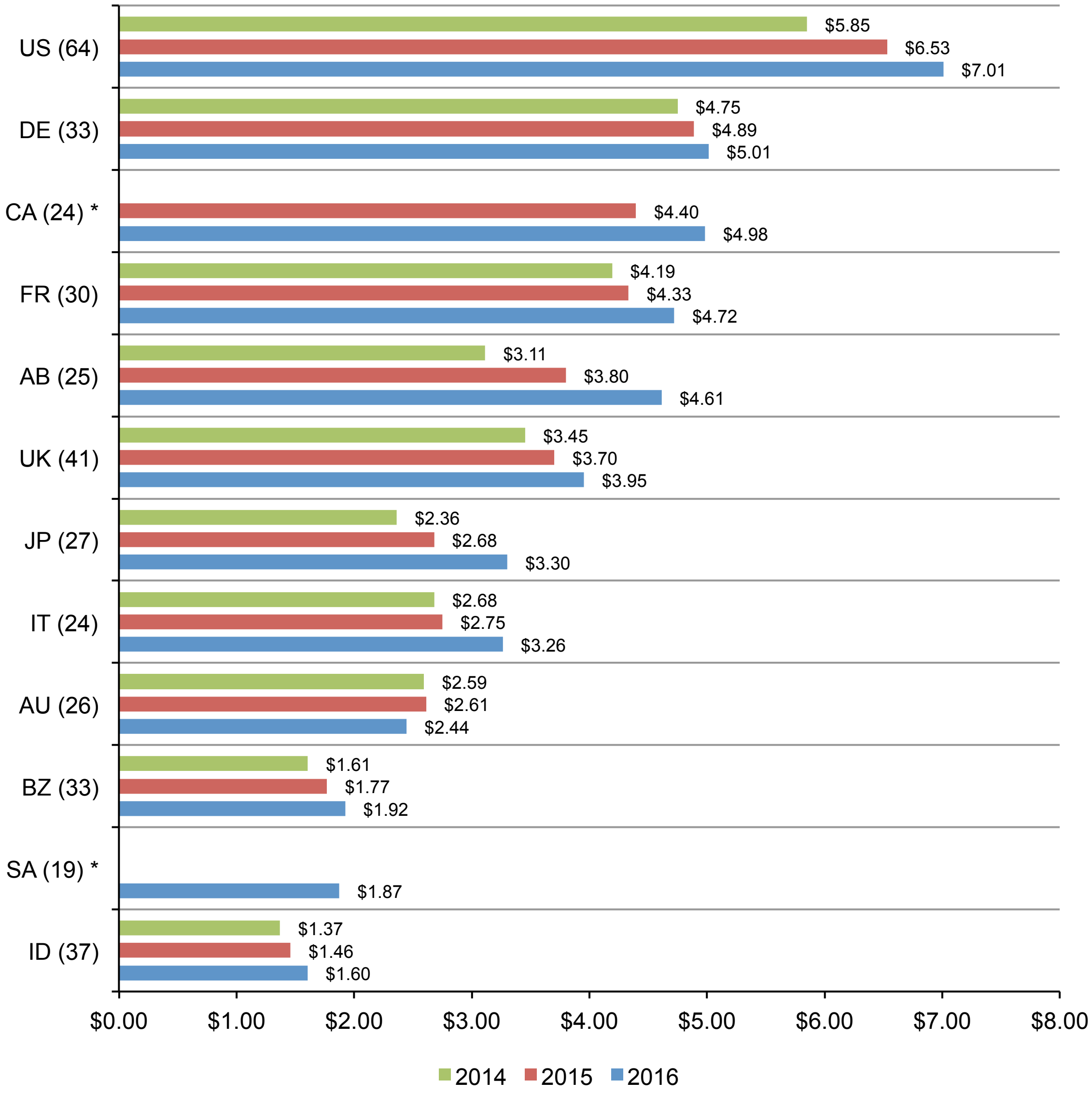
Pie Chart 1. Frequency of benchmark samples by country
(n=383)



Global and industry differences in the cost of data breach

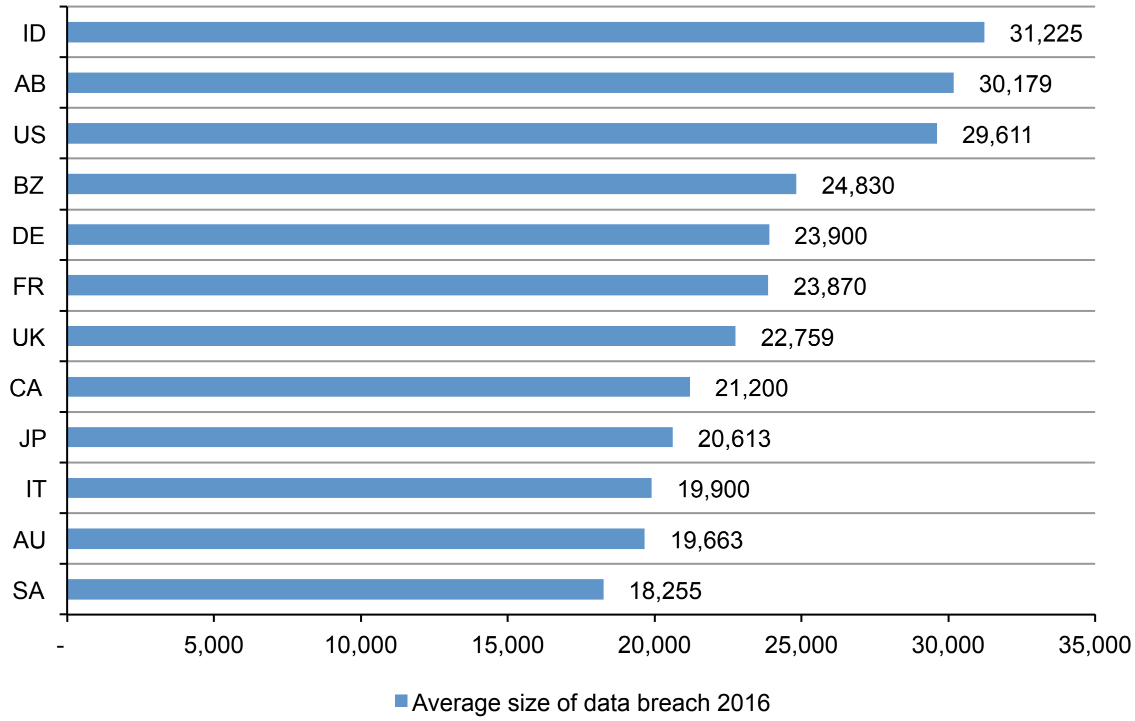
The average organizational cost of data breach varies by country. Figure 2 presents the total average cost of a data breach for 12 countries in this year's study. With the exception of Australia and South Africa, all countries experienced an increase in the average total cost over the past year. The US sample experienced the highest total average cost at more than $7.01 million, followed by Germany at $5.01 million. In contrast, Indian and South Africa companies experienced the lowest total average cost at $1.60 million and $1.87 million, respectively.

Figure 2. The average total organizational cost of a data breach over three years
Grand average for FY 2016=$4.0, FY 2015=$3.8, FY 2014=$3.50
*Historical data is not available in all years
(FY 2016=383, FY 2015=350, FY 2014=315)
Measured in US$ (millions)



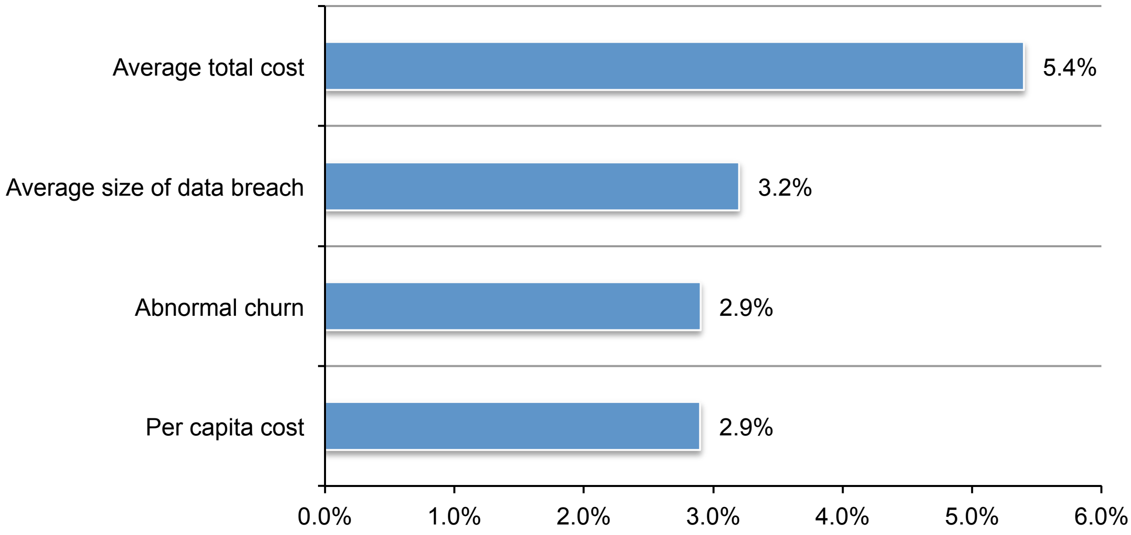
Number of exposed or compromised records. Figure 3 reports the average size of data breaches for organizations in the 12 countries represented in this research. As shown, organizations in India, Arabian Region and US had the largest average number of records lost or stolen. South Africa had the smallest average number of records lost or stolen. In this report, we also show the relationship between the number of records lost or stolen and the cost of a data breach.

Figure 3. The average number of breached records by country
Global average = 23,834
(n=383)



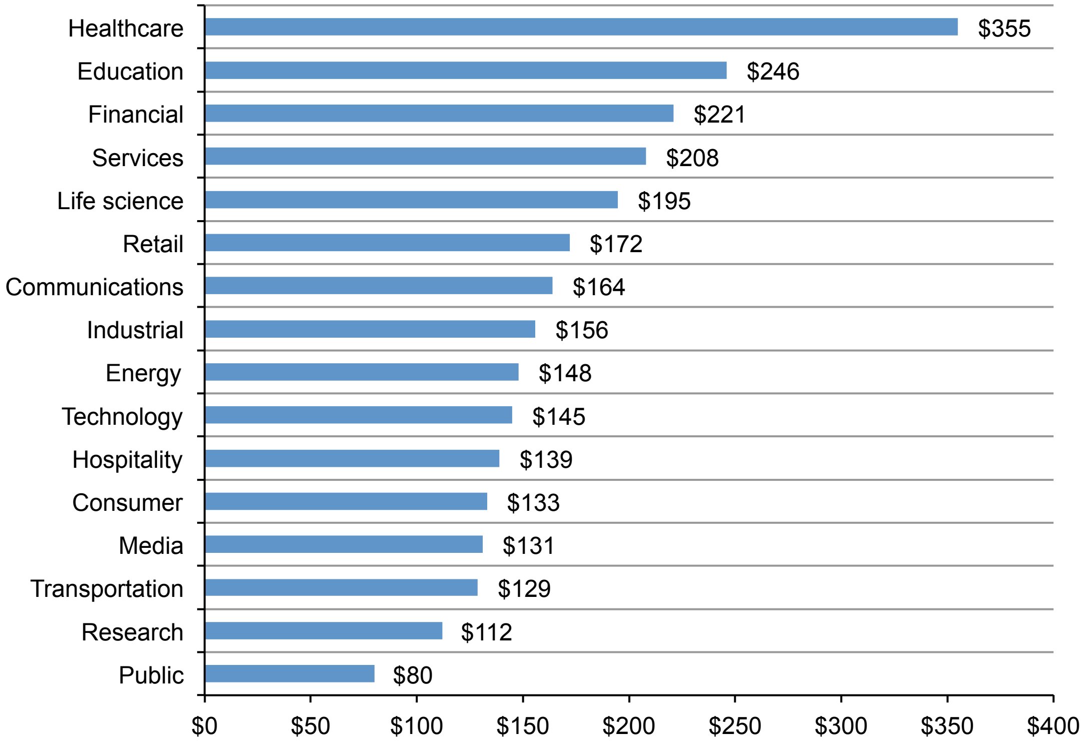
Measures reveal why the cost of data breach increased. Figure 3 presents four metrics that explain the increase in the cost of data breach. The average total cost of a data breach increased 5.4 percent and the per capita or record cost increased 2.9 percent. The average size of the data breach (number of records lost or stolen) increased 3.2 percent. Abnormal churn grew 2.9 percent. Abnormal churn is defined as the greater than expected loss of customers in the normal course of business.

Figure 3. Cost of data breach measures
Consolidated view (n=383)



Certain industries had higher data breach costs. Figure 4 reports the per capita costs for the consolidated sample by industry classification. Heavily regulated industries such as healthcare, education and financial organizations had a per capita data breach cost substantially above the overall mean of $158. Public sector, research and transportation organizations have a per capita cost well below the overall mean value.

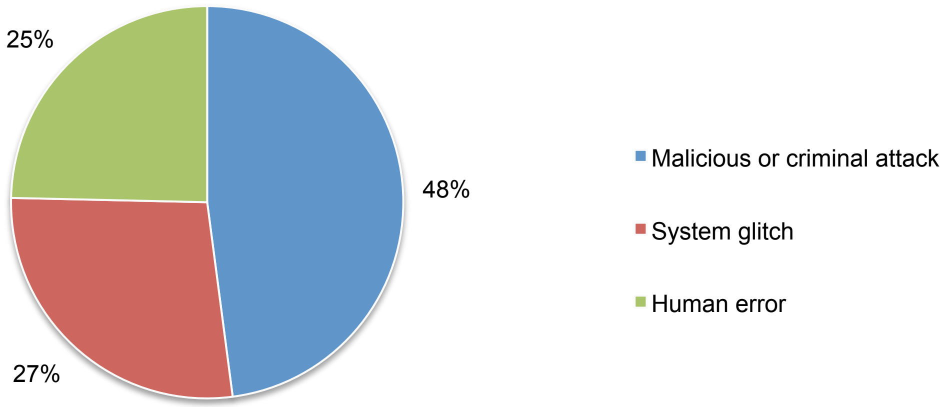
Figure 4. Per capita cost by industry classification
Consolidated view (n=383), measured in US$



The root causes of data breach

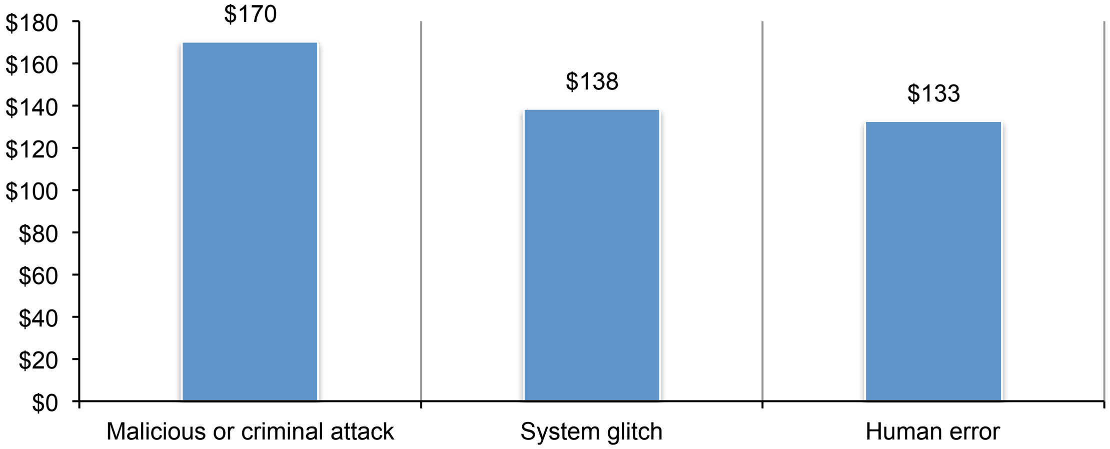
Most data breaches were caused by malicious or criminal attacks.[5] Pie Chart 2 provides a summary of the main root causes of a data breach on a consolidated basis for all 12 countries represented in the research. Forty-eight percent of incidents involved a malicious or criminal attack, 25 percent were caused by negligent employees or contractors (human factor) and 27 percent involve system glitches that includes both IT and business process failures.[6]

Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=383)



Malicious attacks are more costly globally. Figure 5 reports the per capita cost of data breach for three root causes of the breach incident. In 2016, the cost of data breaches due to malicious or criminal attacks was $170. This is significantly above the per capita cost for breaches caused by system glitch and human factors ($138 and $133, respectively).

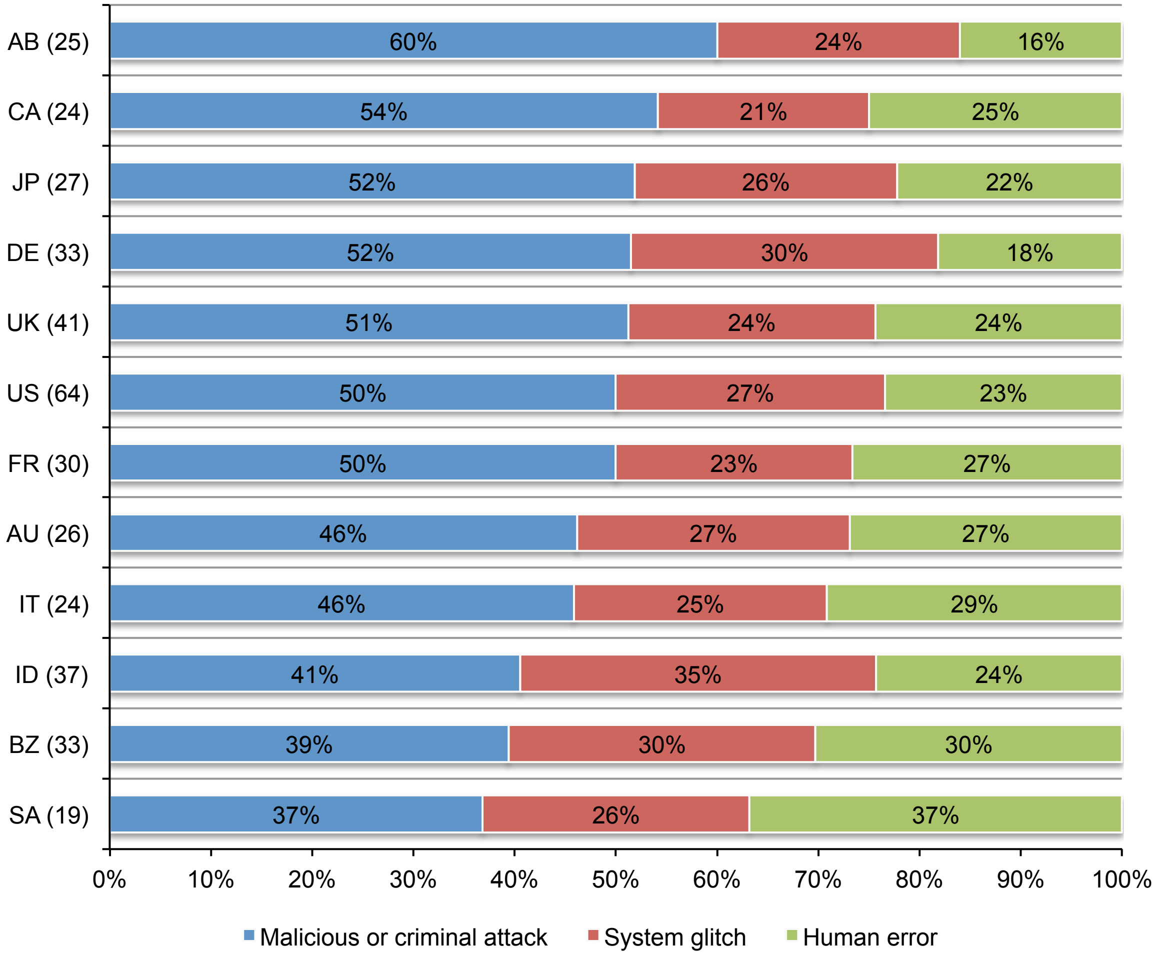
Figure 5. Per capita cost for three root causes of the data breach
Consolidated view (n=383), measured in US$



[5] 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).
[6] The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

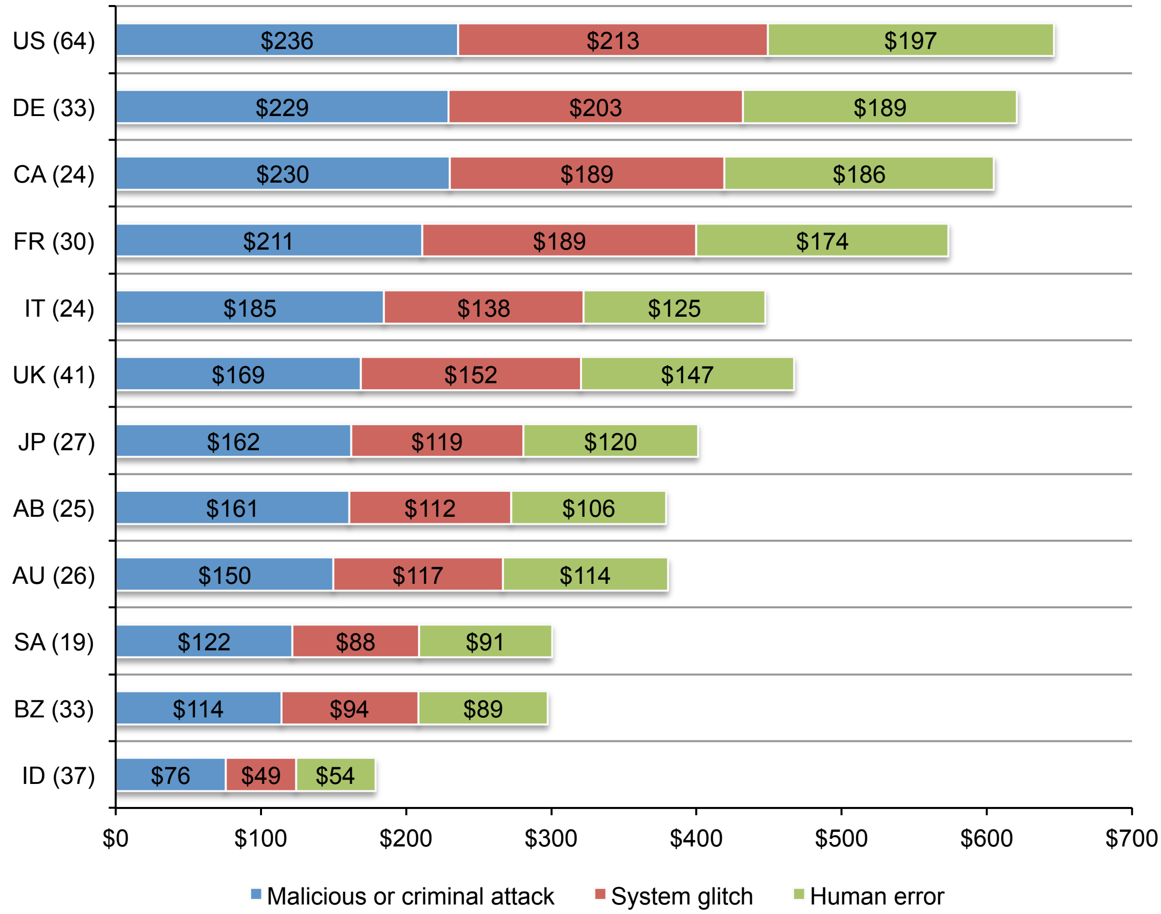
The country differences in data breach root causes. Figure 6 presents the main root causes of data breach for 12 country samples. At 60 percent, organizations in the Arabian region were most likely to experience a malicious or criminal attack. In contrast, South African and Brazilian companies were least likely to experience such data breaches. Instead, South African companies had the highest percentage of human error data breaches and Indian organizations are 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
(n=383)



The per capita cost for three root causes differs among countries. Figure 7 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 $236 per compromised record. In India, this per capita cost was $76.

Figure 7. Per capita cost for three root
(n=383)

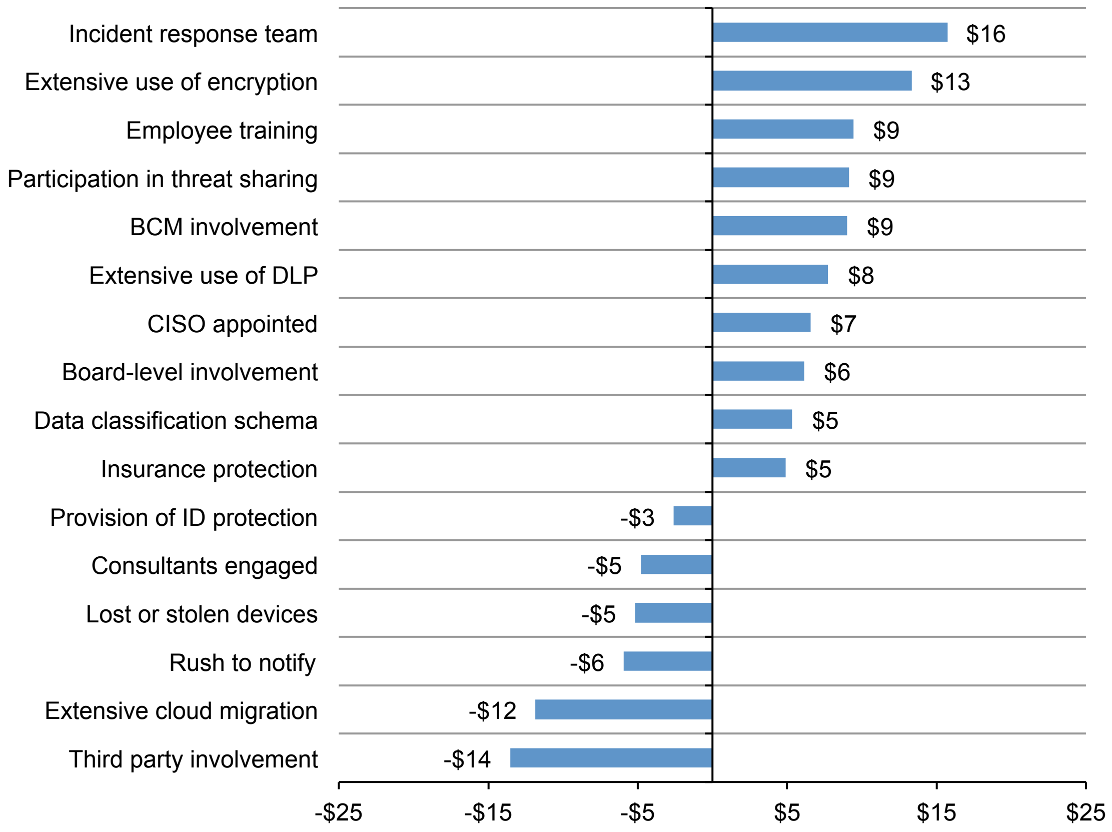


Factors that influence the cost of data breach

Certain factors decreased the cost of data breach. Figure 8 provides a list 16 factors that increased or decreased the per capita cost of data breach. As shown, an incident response team, extensive use of encryption, employee training, participation in threat sharing or business continuity management decreased the per capita cost of data breach.

Data breaches caused by third party involvement in the incident, extensive migration to cloud, rush to notify or lost or stolen devices increased the per capita cost of data breach (shown as negative numbers). For example, an incident response team reduced the cost of data breach by $16, from $158 to $142. In contrast, third party involvement in the cause of the data breach results in an increase of $14, from $158 to $172.

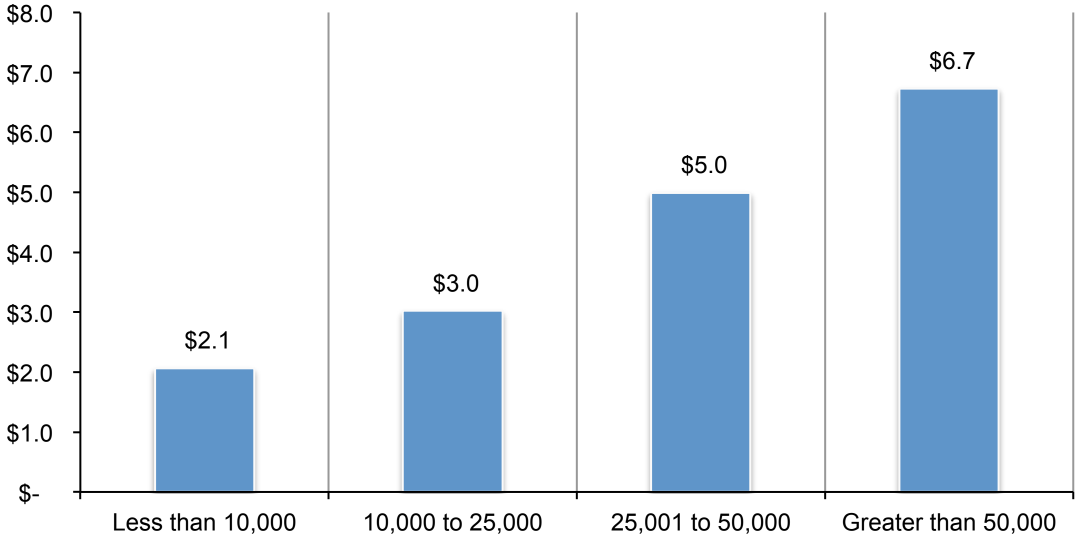
Figure 8. Impact of 16 factors on the per capita cost of data breach
Consolidated view (n=383), measured in US$



Trends in frequency of compromised records and customer turnover

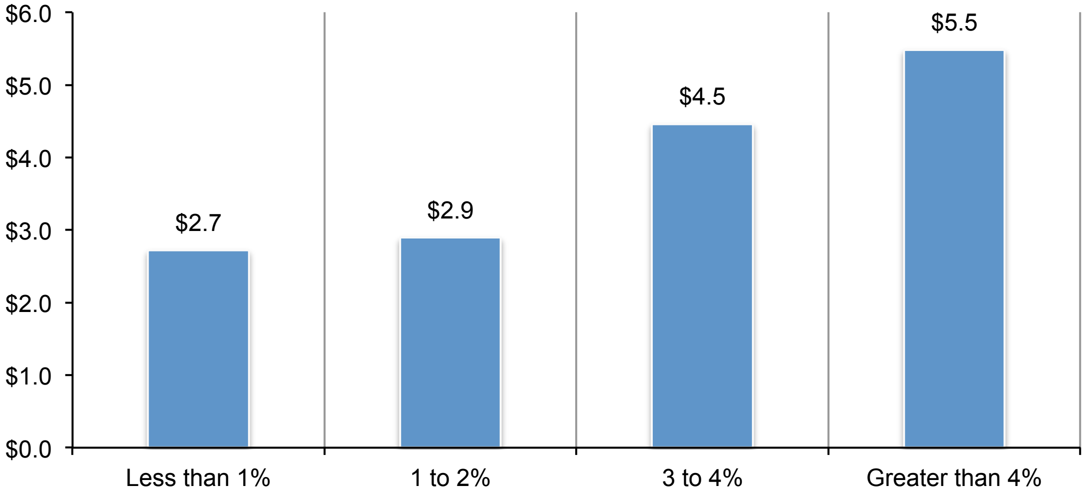
The more records lost, the higher the cost of the data breach. Figure 9 shows the relationship between the total cost of data breach and the size of the incident for 383 organizations in ascending order by the size of the breach incident. In this year's study, the cost ranged from $2.1 million to $6.7.

Figure 9. Total cost by size of the data breach
Consolidated view (n=383), measured in US$ million



The more churn, the higher the per capita cost of data breach. Figure 10 reports the distribution of per capita data breach costs in ascending rate of abnormal churn for 383 organizations. Companies that experienced less than a 1 percent loss of existing customers had an average data breach cost of $2.7 million or if the loss of existing customers exceeded 4 percent the cost averaged $5.5 million.

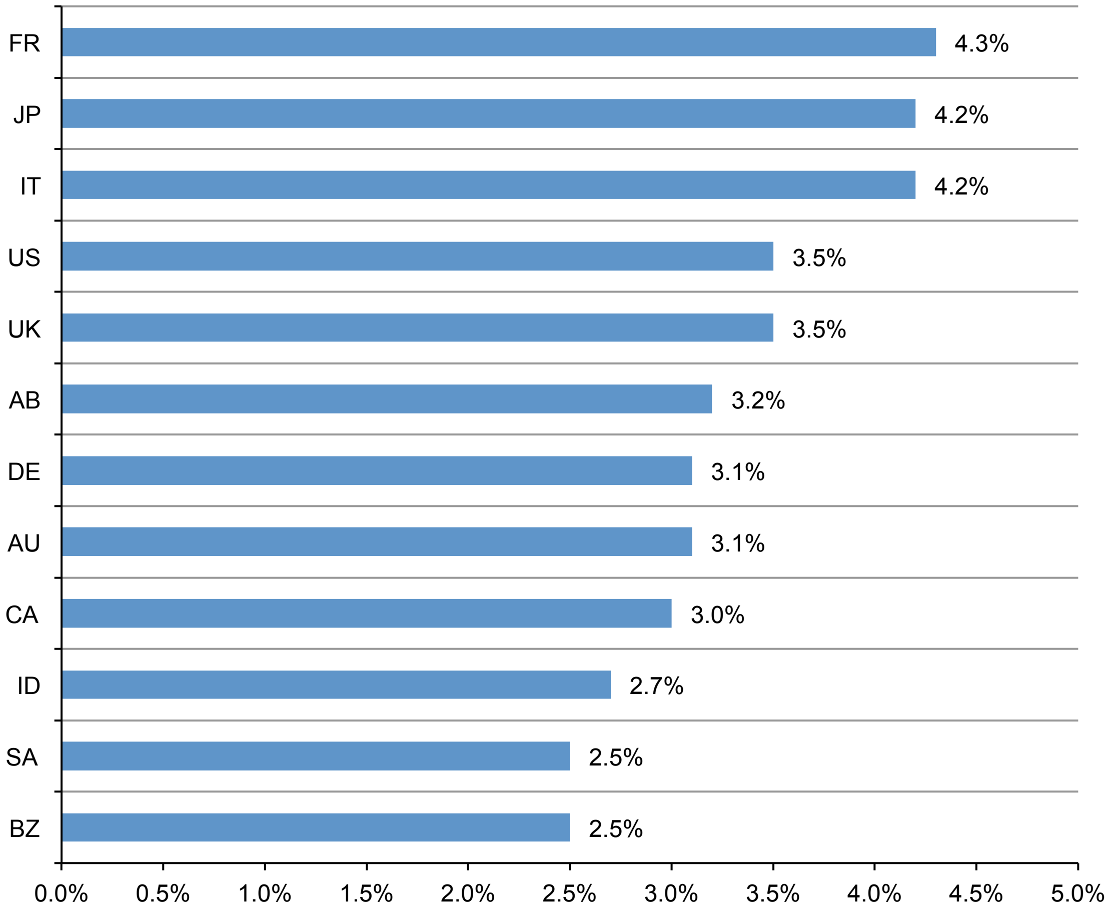
Figure 10. Total cost of data breach by abnormal churn rate
Consolidated view (n=383), measured in US$ millions



Certain countries are more vulnerable to churn. Figure 11 reports the average abnormal churn rates for the 12 countries represented in this research. Results show marked differences among countries. France continued to experience the highest rate of churn followed by Japan. Public and retail experienced the lowest abnormal churn or turnover.

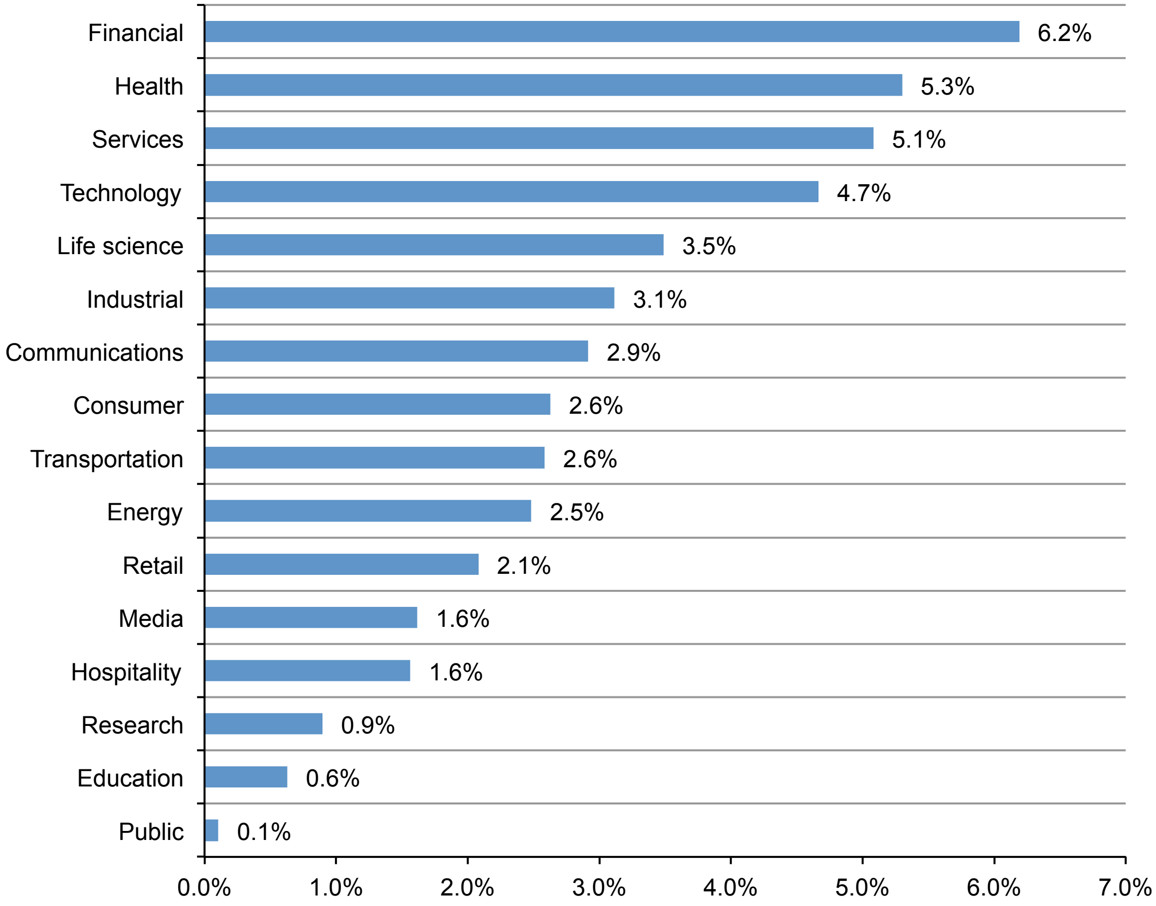
The implication of this finding is that organizations in countries with high churn rates could significantly reduce the costs of data breach by putting an emphasis on customer retention activities to preserve reputation and brand value.

Figure 11. Abnormal churn rates over three years by country sample
(n = 383)



Certain industries are more vulnerable to churn. Figure 12 reports the abnormal churn rate of benchmarked organizations for the 2016 study. While a small sample size prevents us from generalizing the affect of industry on customer churn rates, financial, health and service organizations experienced relatively high abnormal churn and public sector and education organizations experienced a relatively low abnormal churn.[7]

Figure 12. Abnormal churn rates by industry classification of benchmarked companies
(n = 383)

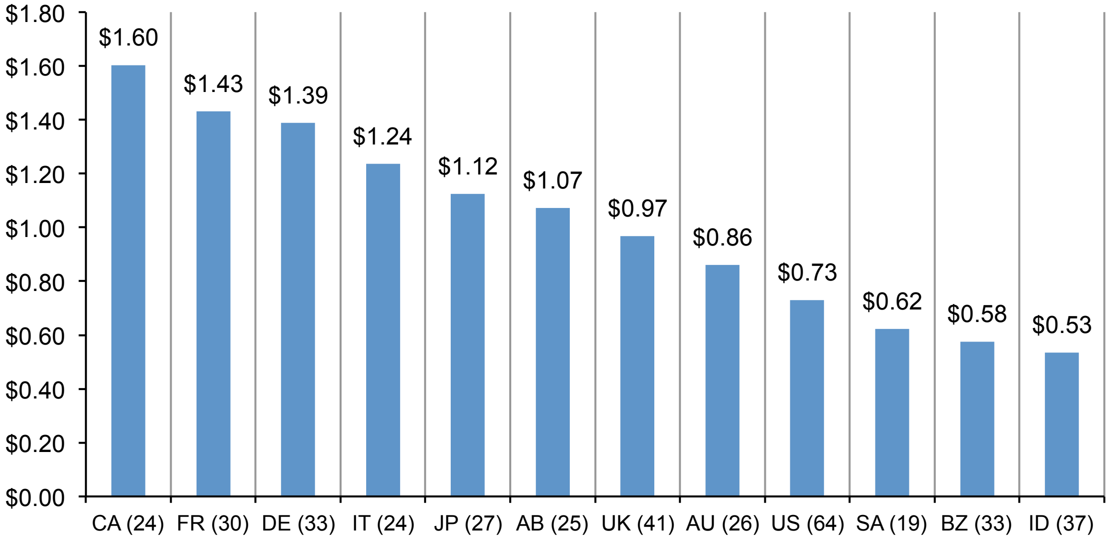


[7] Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have an alternative choice.

Trends in the cost components of a data breach

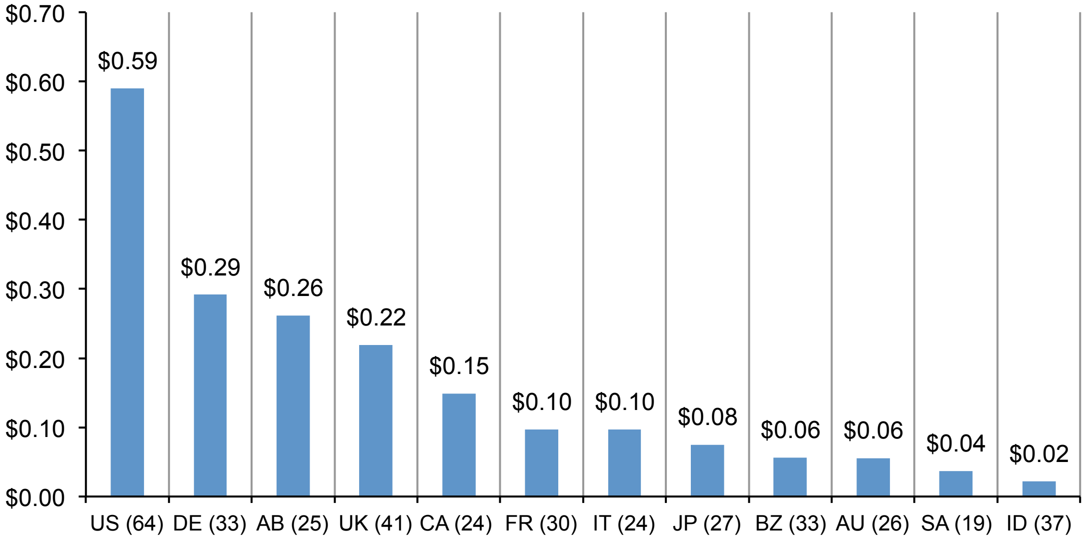
Detection and escalation costs were the highest in Canada and lowest in India. Data breach costs associated with detection and escalation are forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. As shown in Figure 13, the average detection and escalation costs for Canada were $1.60. In contrast, the average costs for India were $0.53.

Figure 13. Detection and escalation costs
(n = 383), Measured in US$ (millions)



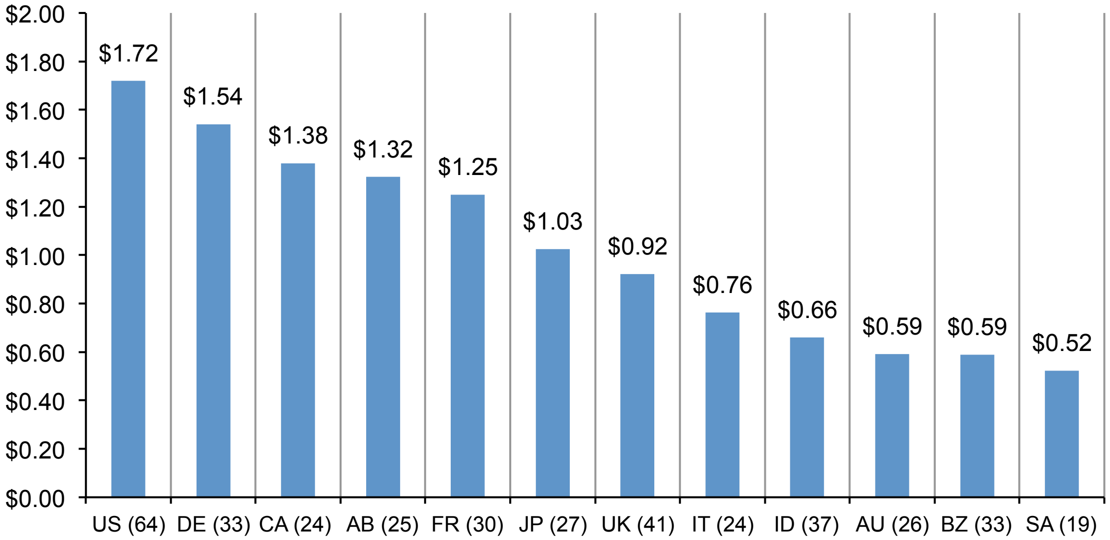
Notification costs were the highest in US. Notification-related include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication set-up. By far, notification costs for US organizations were the highest ($0.59), as shown in Figure 14.

Figure 14. Notification costs
(n = 383), Measured in US$ (millions)



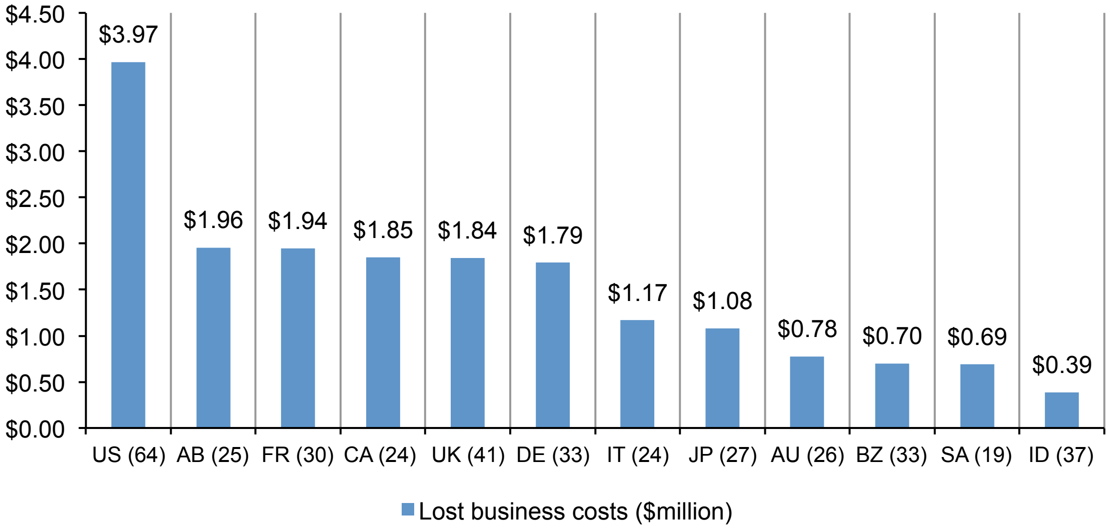
Post data breach response costs were highest in US and Germany. The costs associated with ex-post response and detection in the US was $1.72 and $1.54 in Germany as shown in Figure 15. Ex-post costs include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions.

Figure 15. Ex-post response costs
(n = 383), Measured in US$ (millions)



US organizations paid the highest price for losing customers after a data breach. According to Figure 16, the cost of lost business was particularly high for US organizations ($3.97). This cost component includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.

Figure 16. Lost business costs
(n = 383), Measured in US$ (millions)

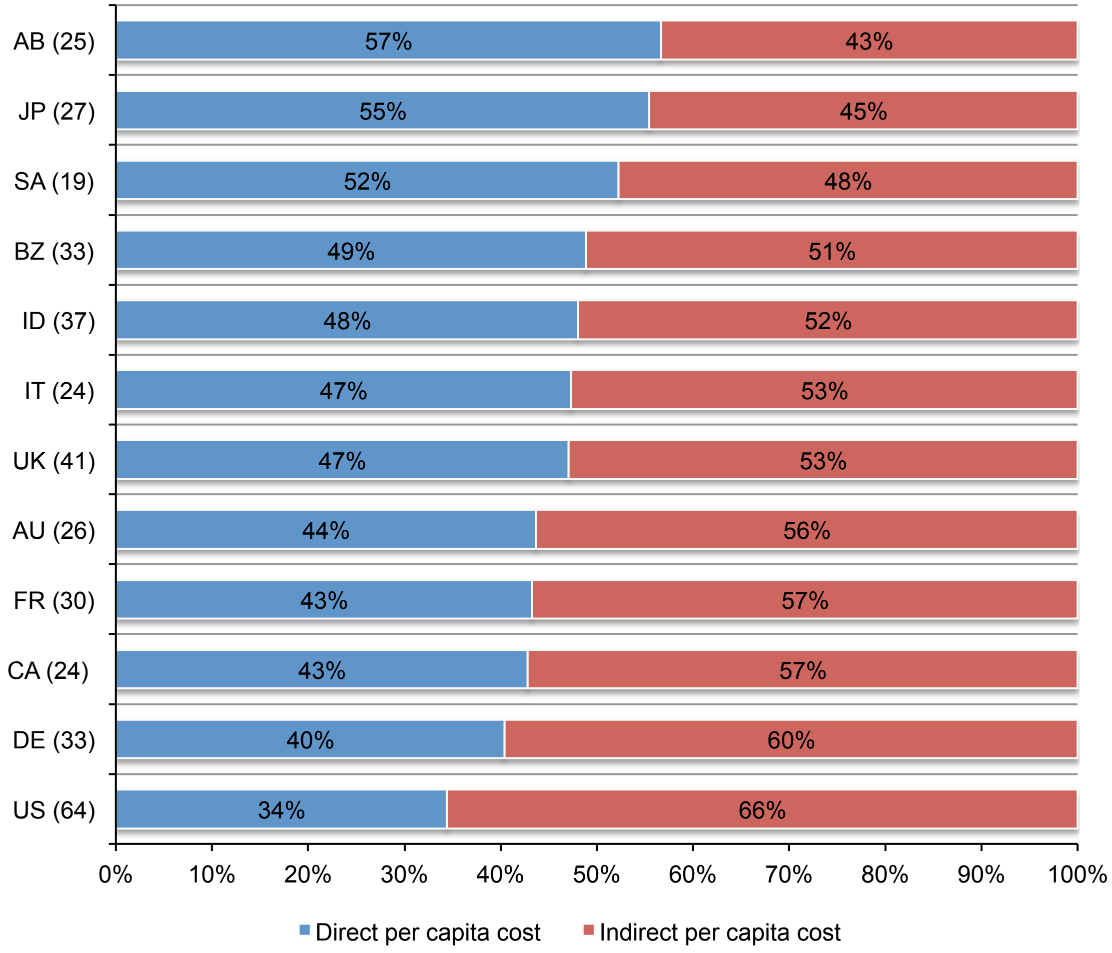


The proportion of direct and indirect costs of data breach varies by country

The Arabian Region had the highest direct costs and the US has the highest indirect costs. 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 17 reports the percentage direct and indirect per capita data breach costs for all 12 countries. The Arabian Region had the highest percentage (57 percent) of direct costs and the US had the highest percentage (66 percent) of indirect costs.

Figure 17. Percentage direct and indirect per capita data breach costs
Consolidated view (n=383)

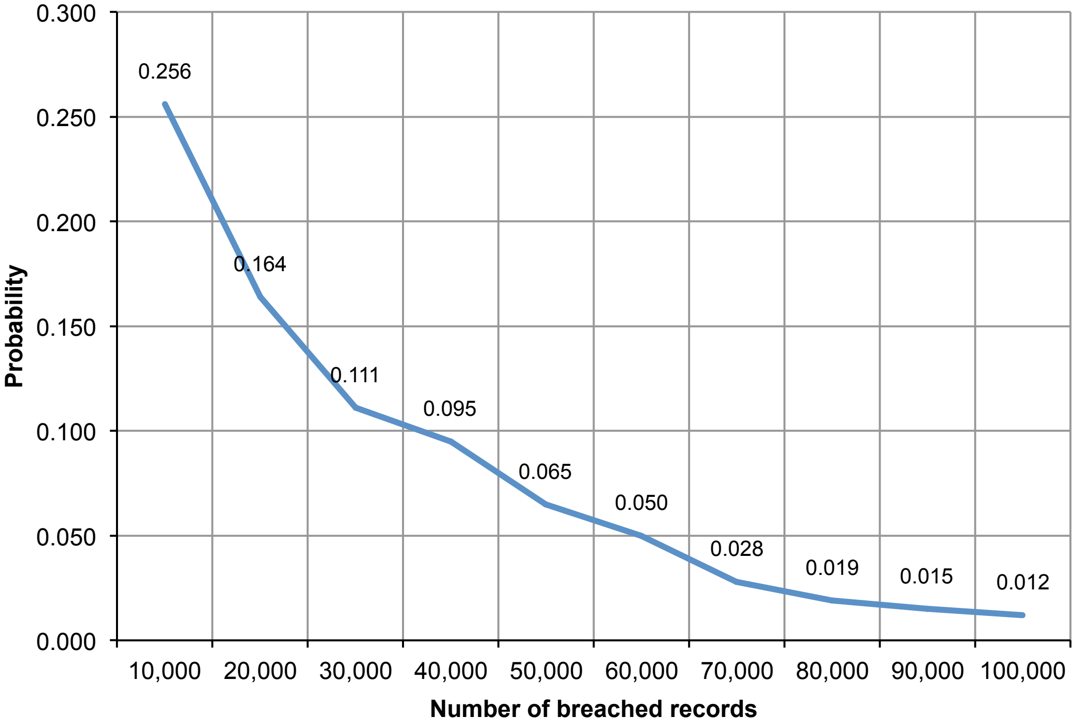


The likelihood that an organization will have a data breach

Our research provides an analysis of the likelihood of one or more data breach occurrences in the next 24 months. Based on the experiences of organizations in our research, we believe we can predict the probability of a data breach based on two factors: how many records are lost or stolen and the company's industry.

Figure 18 shows the subjective probabilities of breach incidents involving a minimum of 10,000 to 100,000 compromised records.[8] As can be seen, the likelihood of a data breach steadily decreases as the size increases. While the likelihood of a data breach involving a minimum of 10,000 records is estimated at approximately 26 percent over a 24-month period, the chances of a data breach involving a 100,000 records is less than 1 percent.

Figure 18. Probability of a data breach involving a minimum of 10,000 to 100,000 records
Consolidated view (n=383)

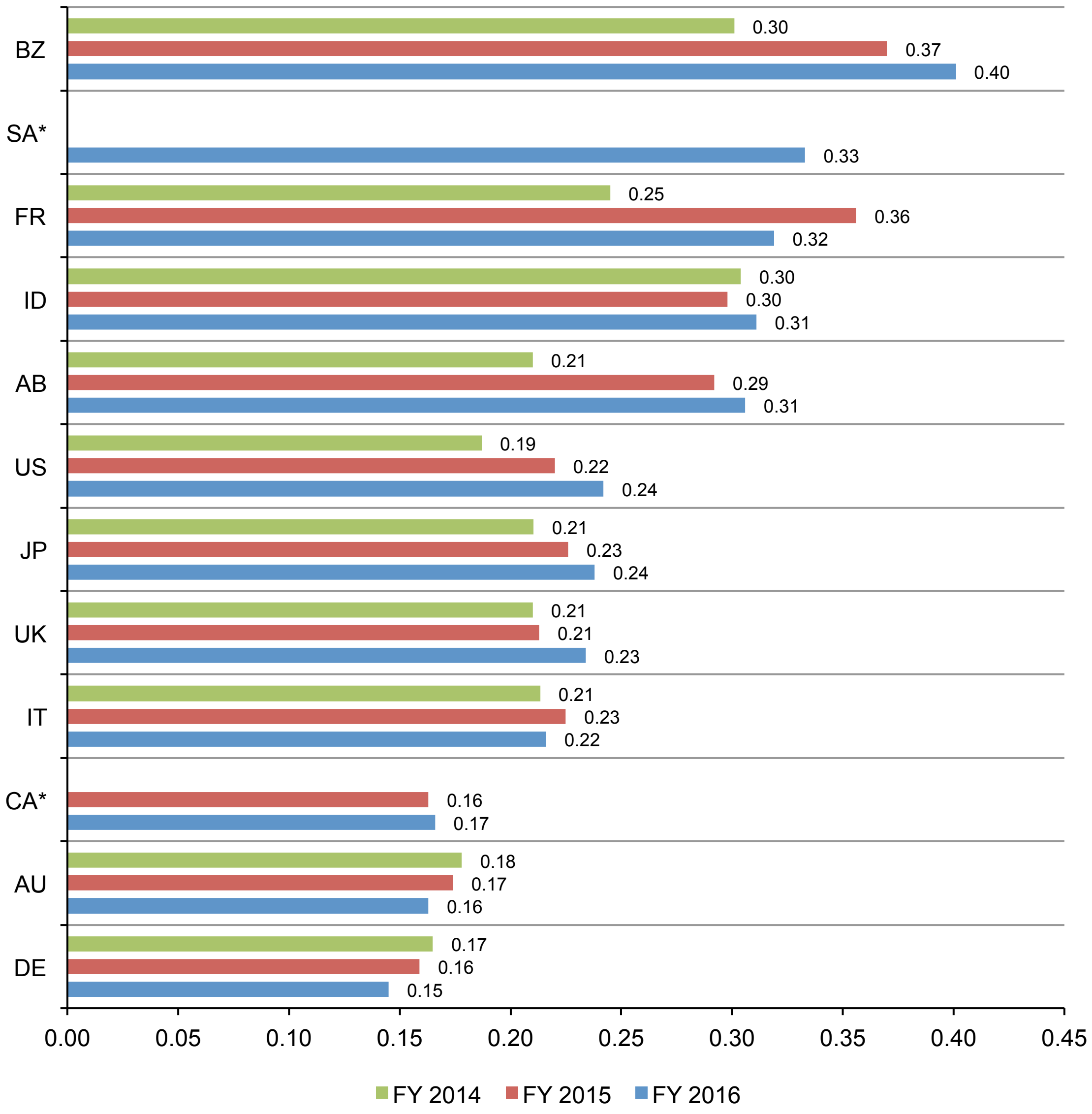


[8] Estimated probabilities were captured from sample respondents using a point estimation technique. Key individuals such as the CISO or CPO who participated in cost assessment interviews provided their estimate of data breach likelihood for 10 levels of data breach incidents (ranging from 10,000 to 100,000 lost or stolen records). The time scale used in this estimation task was the forthcoming 24-month period. An aggregated probability distribution was extrapolated for each one of the 383 participating companies.

Organizations in certain countries are more likely to have a data breach. Figure 19 summarizes the probability of a data breach involving a minimum of 10,000 records for the 12 countries in this research. While a small sample size prevents us from generalizing country differences, the estimated likelihood of a material data breach varies considerably across countries.

Brazil and South Africa appear to have the highest estimated probability of occurrence. Germany and Australia have the lowest probability of data breach.

Figure 19. Probability of a data breach involving a minimum of 10,000 records by country
Grand average = 25.6%
A minimum of 10,000 compromised records
*Historical data is not available in all years
Consolidated view (FY 2016=383, FY 2015=350, FY 2014=315)



Time to identify and contain data breaches impact cost

Mean Time to Identify (MTTI) and Mean Time to Contain (MTTC) metrics are used to determine the effectiveness of their organization's incident response and containment processes. The MTTI metric helps organizations to understand the time it takes to detect that an incident has occurred and the MTTC metric measures the time it takes for a responder to resolve a situation and ultimately restore service.

Figure 20 provides data on the mean time to identify (MTTI) and mean time to contain (MTTC) the data breach. For our consolidated sample of 383 companies, we estimate it took a mean time to identify of 201 days with a range of 20 to 569 days. The mean time to contain was 70 days with a range of 11 to 126 days.

Figure 20. Mean time to identify and contain data breach incidents (in days)
Consolidated view (n = 383)

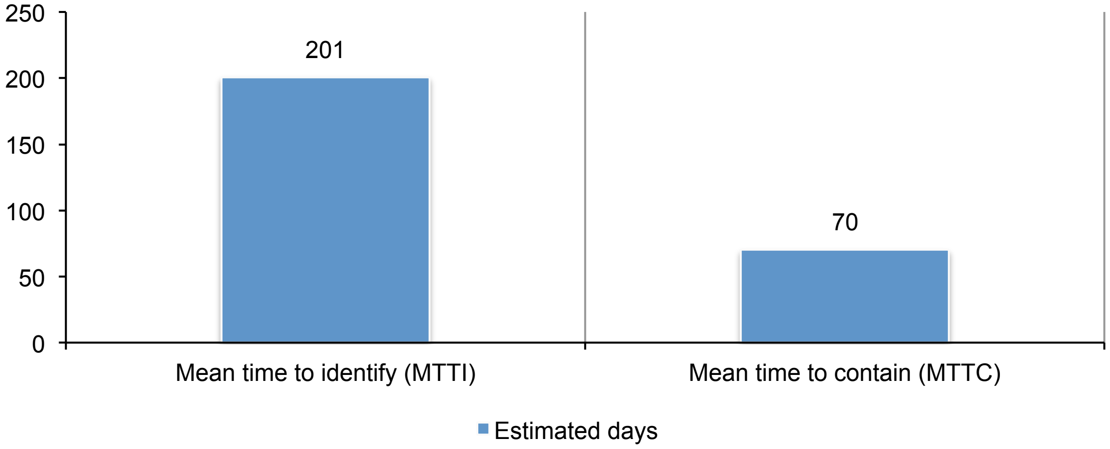


Figure 21 provides MTTI and MTTC by three root causes of the data breach incident. As shown, both the time to identify and time to contain was highest for malicious and criminal attacks (229 and 82 days, respectively) and much lower for data breaches caused by human error (162 and 59 days, respectively).

Figure 21. Mean time to identify and contain data breach incidents by root cause (in days)
Consolidated view (n = 383)

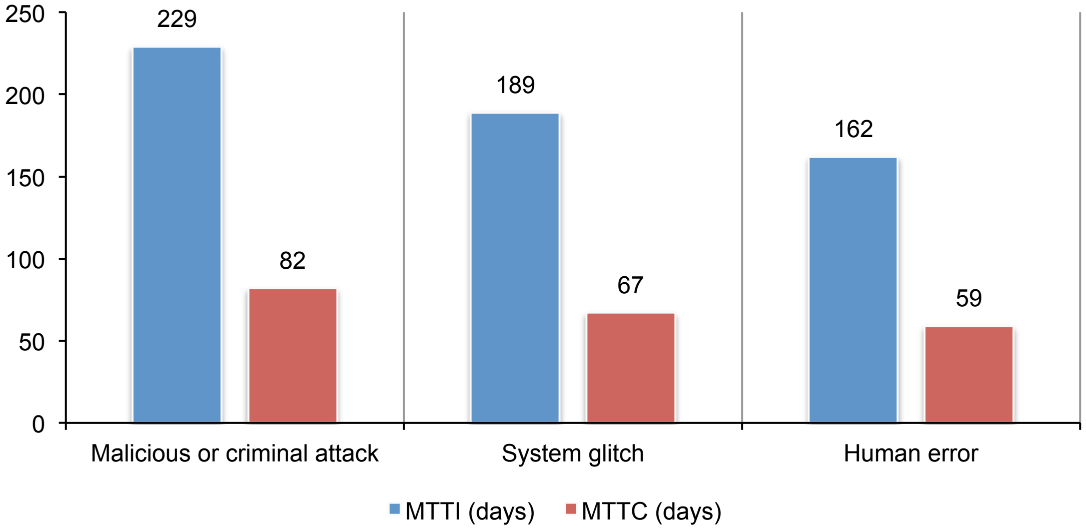


Figure 22 shows an upper-sloping linear relationship between total data breach cost and mean time for 383 companies in 12 countries. This significant relationship suggests the failure to quickly identify the data breach will lead to higher costs and the importance of having an incident response plan in place. If the MTTI was less than 100 days the average cost to identify the data breach was $3.23 million. If it took more than 100 days, the cost was $4.38 million.

Figure 22. Relationship between mean time to identify and total average cost
Consolidated view (n=383), measured in US$ (millions)

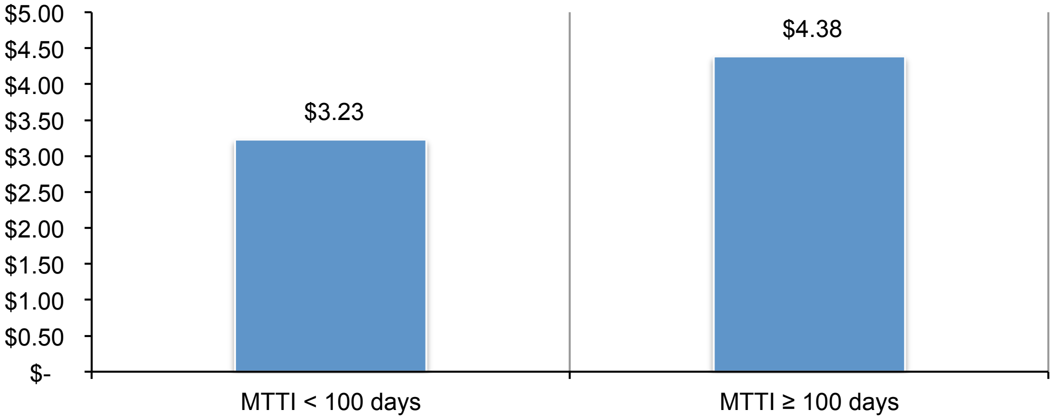
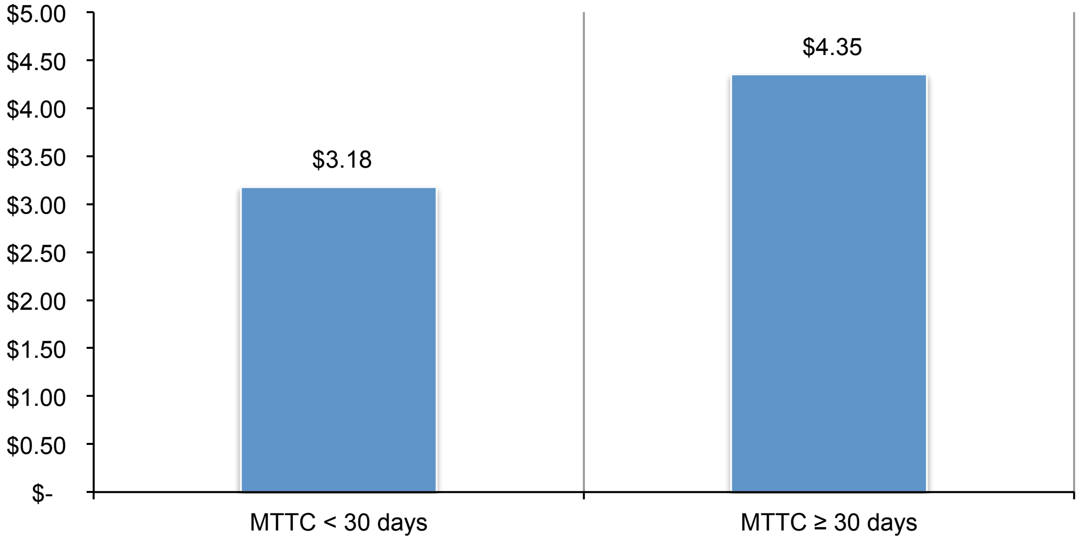


Figure 23 also shows an upper-sloping linear regression line between total data breach cost and MTTC. Similar to the above, this significant relationship suggests the failure to quickly contain the data breach will lead to higher costs. If the time to contain the breach took less than 30 days the cost to contain was $3.18 million. If it took more than 30 days, the cost was $4.35 million.

Figure 23. Relationship between mean time to contain and total average cost
Consolidated view (n=383), measured in US$ (millions)



Part 3. How we calculate the cost of data breach

To calculate the cost of data breach, we use a costing methodology called activity-based costing (ABC). This methodology identifies activities and assigns a cost according to actual use. Companies participating in this benchmark research are asked to estimate the cost for all the activities they engage in to resolve the data breach.

Typical activities for discovery and the immediate response to the data breach include the following:

- Conducting investigations and forensics to determine the root cause of the data breach
- Determining the probable victims of the data breach
- Organizing the incident response team
- Conducting communication and public relations outreach
- Preparing notice documents and other required disclosures to data breach victims and regulators
- Implementing call center procedures and specialized training

The following are typical activities conducted in the aftermath of discovering the data breach:

- Audit and consulting services
- Legal services for defense
- Legal services for compliance
- Free or discounted services to victims of the breach
- Identity protection services
- Lost customer business based on calculating customer churn or turnover
- Customer acquisition and loyalty program costs

Once the company estimates a cost range for these activities, we categorize the costs as direct, indirect and opportunity as defined below:

- *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).

Our study also looks at the core process-related activities that drive a range of expenditures associated with an organization's data breach detection, response, containment and remediation. The costs for each activity are presented in the Key Findings section (Part 2). 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.

- Post data breach: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimize potential harms. Post data breach activities also include 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).

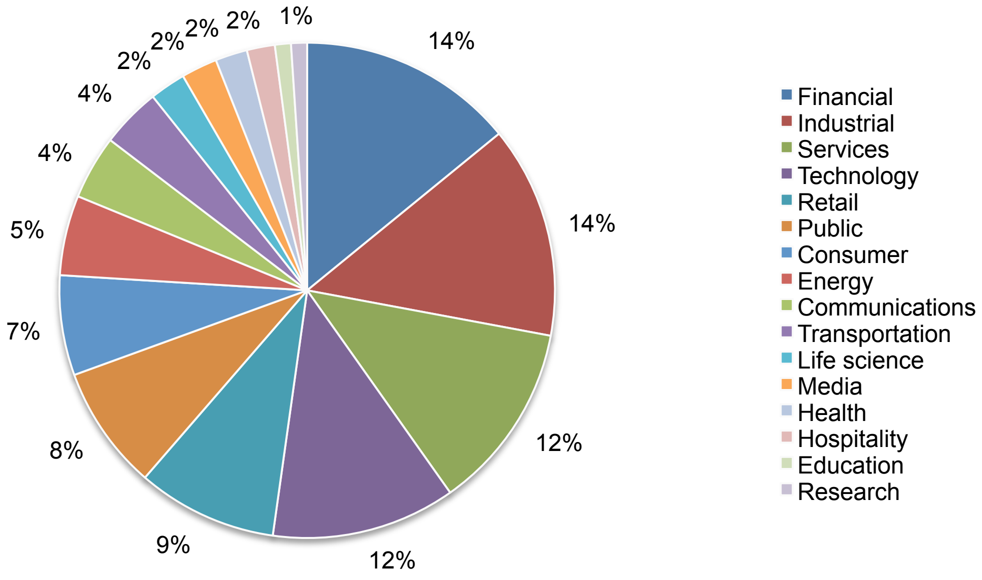
[9] In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organization, but the volume of customer activity actually declines. This partial decline is especially salient in certain industries – such as financial services or public sector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

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

Part 4. Organizational characteristics and benchmark methods

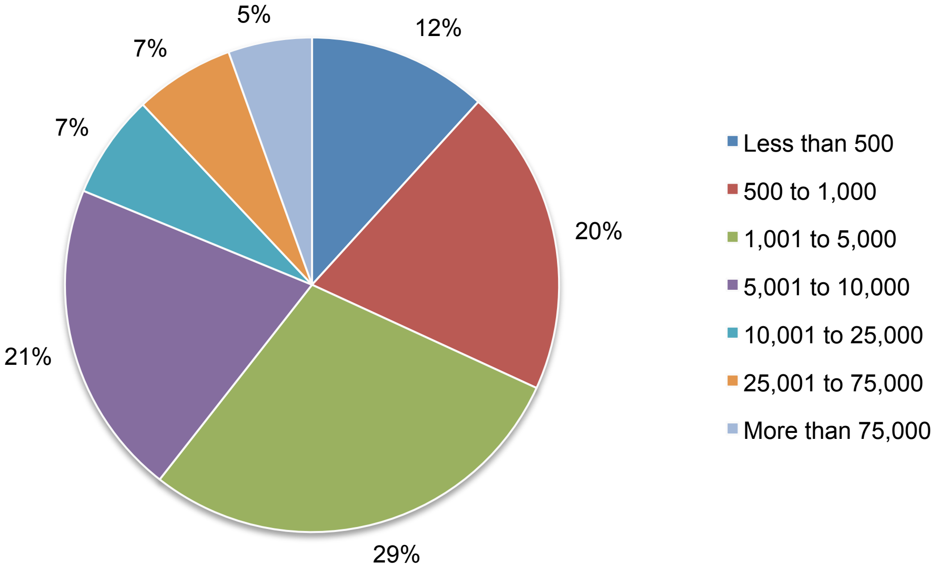
Pie Chart 3 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 16 industries are represented. The largest sector is financial services, which includes banks, insurance, investment management and payment processors.

Pie Chart 3. Distribution of the benchmark sample by industry segment
Consolidated view (n=383)



Pie Chart 4 shows the distribution of benchmark organizations by total headcount. The largest segments include companies with more than 1,000 employees.

Pie Chart 4. Global headcount of participating companies
Consolidated view (n=383)



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.

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.

For purposes of 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.

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.

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 global 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. In this global study, 383 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

Complete copies of all country reports are available at **www.ibm.com/security/data-breach**

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.