Ponemon INSTITUTE

2017 Cost of Data Breach Study

Global Overview

Benchmark research sponsored by IBM Security
Independently conducted by Ponemon Institute LLC
June 2017

Ponemon Institute©
Research Report

IBM Security

2017 Cost of Data Breach Study: Global Overview

Ponemon Institute, June 2017

Part 1. Introduction

IBM Security and Ponemon Institute are pleased to release the *2017 Cost of Data Breach Study: Global Overview*[1]. According to our research, the average total cost of data breach for the 419 companies participating in this research decreased from $4.00 to $3.62 million[2]. The average cost for each lost or stolen record containing sensitive and confidential information also significantly decreased from $158 in 2016 to $141 in this year's study. However, despite the decline in the overall cost, companies in this year's study are having larger breaches. The average size of the data breaches in this research increased 1.8 percent.

This year, a strong U.S. dollar significantly influenced the global cost analysis and contributed to the decline in the cost. As shown above, the cost of data breach declined $17 and approximately $8 (48 percent) of this decline can be attributed to currency rate fluctuation.[3] For purposes of consistency with prior years, we decided to continue to use the same accounting method rather than adjust the cost. It is important to note that this issue only affects the global analysis because all country-level results are shown in local currencies.

This year's study included the following 11 country and two regional samples:

- The United States
- The United Kingdom
- Germany
- Australia
- France
- Brazil
- Japan
- Italy
- India
- Canada
- South Africa
- The Middle East (including the United Arab Emirates and Saudi Arabia)
- ASEAN region (including Singapore, Indonesia, the Philippines and Malaysia)

Global study at a glance

- 419 companies in 13 country or regional samples
- $3.62 million is the average total cost of data breach
- 10% one-year decrease in average total cost
- $141 is the average cost per lost or stolen records
- 11.4% one-year decrease in the per capita cost
- 27.7% is the likelihood of a recurring material data breach over the next two years
- 2.1% increase in the likelihood of a recurring material data breach

All participating organizations experienced a data breach ranging from approximately 2,600 to slightly less than 100,000 compromised records. We define a compromised record as one that identifies the natural person whose information has been lost or stolen in a data breach. The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

In addition to presenting trends in the various components of the cost of data breach, the global study determines the likelihood that an organization will have one or more data breaches in the next 24 months. Two factors were used to determine the probability of a future data breach: the current data breach size and the organizations' location. Based on this year's research, we estimate an average probability of 27.7 percent that organizations in this study will have a material data breach in the next 24 months. Last year, the average probability was 25.6 percent.

[1]This report is dated in the year of publication rather than the year of fieldwork completion. Please note that the majority of data breach incidents studied in the current report happened in the 2016 calendar year.
[2]Local currencies were converted to U.S. dollars.
[3]The conversion from local currencies to the U.S. dollar deflated the per capita and average total cost estimates, especially for companies in the U.K., Germany, France and Italy (e.g., the Pound (£) and Euro (€)).

Organizations in South Africa, India and Brazil are those most likely to experience a material data breach involving 10,000 or more records over the next 24 months. At 41 percent, South Africa has the highest probability of experiencing a data breach in the next 24 months. At 14.5 percent, Canada has the lowest probability of having a future data breach.

A material data breach is one that involves a minimum of 1,000 lost or stolen records containing personal information about consumers or customers. This research does not include data breaches involving high-value information assets such as intellectual property, trade secrets and business confidential information.

Why the cost of data breach fluctuates across countries

What explains the significant increases in the cost of data breach this year for organizations in the Middle East, the United States and Japan? In contrast, how did organizations in Germany, France, Australia, and the United Kingdom succeed in reducing the costs to respond to and remediate the data breach? Understanding how the cost of data breach is calculated will explain the differences among the countries in this research.

For the *2017 Cost of Data Breach Study: Global Overview*, we recruited 419 organizations in 11 countries and two regions to participate in this year's study. More than 1,900 individuals who are knowledgeable about the data breach incident in these 419 organizations were interviewed. The first data points we collected from these organizations were: (1) how many customer records were lost in the breach (i.e. the size of the breach) and (2) what percentage of their customer base did they lose following the data breach (i.e. customer churn). This information explains why the costs increase or decrease from the past year.

In the course of our interviews, we also asked questions to determine what the organization spent on activities for the discovery of and the immediate response to the data breach, such as forensics and investigations, and those conducted in the aftermath of discovery, such as the notification of victims and legal fees. A list of these activities is shown in Part 3 of this report. Other issues covered that may have an influence on the cost are the root causes of the data breach (i.e. malicious or criminal attack, insider negligence or system glitch) and the time to detect and contain the incident.

It is important to note that only events directly relevant to the data breach experience of the 419 organizations represented in this research and discussed above are used to calculate the cost. For example, new regulations, such as the General Data Protection Regulation (GDPR), ransomware and cyber attacks, such as Shamoon, may encourage organizations to increase investments in their governance practices and security-enabling technologies but do not directly affect the cost of a data breach as presented in this research.

The calculation of the components of the cost of data breach that affect the cost

The following information presents the data that is used to calculate the cost and the factors that may increase or decrease these costs. We believe such information will help organizations make better decisions about how to allocate resources to minimize the financial consequences when the inevitable data breach strikes.

- **The unexpected and unplanned loss of customers following a data breach (churn rate)**

Programs that preserve customer trust and loyalty in advance of the breach will help reduce the number of lost business/customers. In this year's research, more organizations worldwide lost customers as a result of their data breaches. However, as shown, having a senior-level leader such as a chief privacy officer or chief information security officer who will be able to direct initiatives that improve customers' trust in how the organization safeguards their personal information will reduce churn and the cost of the breach. Organizations that offer data breach

victims breach identity protection in the aftermath of the breach are also more successful in reducing churn.

- **The size of the breach or the number of records lost or stolen**

It makes sense that the more records lost, the higher the cost of data breach. Therefore, data classification schema and retention programs are critical to having visibility into the sensitive and confidential information that is vulnerable to a breach and reducing the volume of such information.

- **The time it takes identify and contain a data breach**

The faster the data breach can be identified and contained, the lower the costs. In this year's study, organizations were able to reduce the days to identify the data breach from an average of approximately 201 in 2016 to 191 days and the average days to contain the data breach from 70 to 66 days. We attribute these improvements to investments in such enabling security technologies as security analytics, SIEM, enterprise wide encryption and threat intelligence sharing platforms.

In contrast, security complexity and the deployment of disruptive technologies can affect the time to detect and contain a data breach. Although some complexity in an IT security architecture is expected to deal with the many threats facing organizations, too much complexity can impact the ability to respond to data breaches. Disruptive technologies, access to cloud-based applications and data as well as the use of mobile devices (including BYOD and mobile apps) increase the complexity of dealing with IT security risks and data breaches. As shown in the research, cloud migration at the time of the data breach and mobile platforms were shown to increase the cost.

- **The detection and escalation of the data breach incident**

Detection and escalation costs include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. Investments in governance, risk management and compliance (GRC) programs that establish an internal framework for satisfying governance requirements, evaluating risk across the enterprise and tracking compliance with governance requirements can improve an organization's ability to detect and escalate a data breach.

- **Post data breach costs, including the cost to notify victims**

These costs include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. The United States had the highest notification costs.

The purchase of cyber and data breach insurance can help manage the financial consequences of the incident. As shown in this year's study, insurance protection and business continuity management reduced the cost of data breach following the discovery of the incident. In contrast, the rush to notify victims without understanding the scope of the breach, compliance failures and the engagement of consultants all increase post data breach costs. Expenditures to resolve lawsuits also increase post data breach costs.

- **An attack by a malicious insider or criminal is costlier than system glitches and negligence (human factor).**

Almost half of organizations represented in this research (47 percent) identified the root cause of the data breach as a malicious or criminal attack and the average cost was approximately $156. In contrast system glitches and human error or negligence averaged approximately $128 and $126, respectively. Factors that may decrease the cost are participation in threat sharing, use of security analytics and the recruitment and retention of knowledgeable personnel.

In conclusion, organizations in Australia, Germany, France and the United Kingdom were able to improve their ability to keep customers and, as a result, reduced the cost of data breach. Organizations in Australia, the United Kingdom and Germany also were able to limit the number of customer records lost or stolen and, as a result, had lower costs. Whereas, countries in the Middle East and the United States experienced a higher percentage of churn and had higher costs. Organizations in Brazil, India, the Middle East and South Africa had data breaches involving more lost or stolen records, which increased their costs. The individual country reports present in greater detail the cost components and factors that affected the cost.

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

The global cost of data breach decreases. The average cost of data breach decreased 10 percent and the per capita cost decreased 2.9 percent. However, the average size of a data breach (number of records lost or stolen) increased 1.8 percent. Over the past year, there was no change in the abnormal churn rate, which is defined as the greater than expected loss of customers. Last year the average total cost increased 5.4 percent, and the average size of a data breach increased 3.2 percent. Both abnormal churn and the per capita cost increased 2.9 percent.

Data breaches are most expensive in the United States and Canada and least expensive in Brazil and India. The average per capita cost of data breach was $225 in the United States and $190 in Canada. The lowest cost was Brazil ($79) and India ($64). The average total organizational cost in the United States was $7.35 million and $4.94 million in the Middle East. The lowest average total organizational cost was in Brazil ($1.52 million) and India ($1.68 million).

Trends in the cost of data breach vary among countries. The comparison of this year's cost of data breach to the four-year average reveals that the cost increased for organizations in five countries and decreased in seven countries. Germany had the biggest decrease in average total cost (-.91) followed by France (-.68), Australia (-.48) and the United Kingdom (-.45). The most significant increase in average total cost occurred in the Middle East (+.83), the United States (+.66) and Japan (+.52).

Certain industries have more costly data breaches. The average global cost of data breach per lost or stolen record was $141. However, health care organizations had an average cost of $380 and in financial services the average cost was $245. Media ($119), research ($101) and public sector ($71) had the lowest average cost per lost or stolen record.

Organizations in certain countries are more likely to have a data breach. Throughout the past four years, this research has studied the likelihood of one or more data breaches over a 24-month period. South Africa and India have the highest estimated probability of occurrence. Germany and Canada have the lowest probability of a data breach in the next 24 months.

Detection and escalation costs are highest in Canada and lowest in Brazil. Data breach costs to detect and escalate the incident 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 $1.46 million. In contrast, the average cost for detection and escalation for Brazil was $0.43 million.

Notification costs are the highest in the United States. These costs include the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication setups. Notification costs for organizations in the United States were the highest ($0.69 million), whereas India had the lowest ($0.02 million).

The United States and the Middle East spend the most on post data breach response. Post data breach response activities include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. In the United States, these costs were $1.56 million and $1.43 million in the Middle East.

Companies in the Middle East and Canada have the highest direct per capita costs and the United States has the highest per capita indirect costs. The Middle East and Canada had the highest direct per capita cost (both $81). These 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. The United States had the highest indirect per capita cost ($146).

Indirect costs include employees' time, effort and other organizational resources spent notifying victims and investigating the incident, as well as the loss of goodwill and customer churn.

The more records lost, the higher the cost of the data breach. Cost analysis reveals a relationship between the average total cost of data breach and the size of the incident. In this year's study, the average total cost ranged from $1.9 million for incidents with less than 10,000 compromised records to $6.3 million for incidents with more than 50,000 compromised records. Last year 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 records.

The faster the data breach can be identified and contained, the lower the costs. For the third year, our study reports the relationship between how quickly an organization can identify and contain data breach incidents and the financial consequences. For our consolidated sample of 419 companies, the mean time to identify (MTTI) was 191 days, with a range of 24 to 546 days. The mean time to contain (MTTC) was 66 days with a range of 10 to 164 days. Both the time to identify and the time to contain were highest for malicious and criminal attacks (214 and 77 days, respectively) and much lower for data breaches caused by human error (168 and 54 days, respectively).

Hackers and criminal insiders cause the most data breaches. Forty-seven 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 $156. In contrast, system glitches cost $128 per record and human error or negligence is $126 per record. Companies in the United States and Canada spent the most to resolve a malicious or criminal attack ($244 and $201 per record, respectively). India spent far less ($78 per record).

Malicious or criminal attacks target Middle East and U.S. organizations. Fifty-nine percent of breaches in the Middle East and 52 percent of breaches in the United States were due to hackers and criminal insiders. Only 40 percent of data breaches in Italy and South Africa were due to malicious attacks. Italian and ASEAN organizations have the highest percentage of human error at 36 percent and 35 percent, respectively. German and Indian organizations were most likely to experience a data breach caused by a system glitch or business process failure (34 percent and 33 percent, respectively).

Incident response teams and the extensive use of encryption reduce costs. In this year's research, an incident response (IR) team reduced the cost by as much as $19 per compromised record. Hence, companies with a strong IR capability would anticipate an adjusted cost of $122 ($141-$19 per record). Similarly, the extensive use of encryption reduced cost by $16 per capita, with an adjusted average cost of $125 ($141-$16) per record.

Third party involvement in a breach and extensive cloud migration at the time of the breach increases the cost. If a third party was involved in the data breach, the cost of data breach increased by as much as $17 per compromised record with an adjusted average cost of $158 per record ($141+$17). Organizations undergoing a major cloud migration at the time of the breach saw this increase to per capita cost by $14, with an adjusted average cost of $155 ($141+$14) per record.

Four new factors are included in this year's cost analysis. The following factors influence data breach costs: (1) compliance failures, (2) the extensive use of mobile platforms, (3) CPO appointment and (4) the use of security analytics. The appointment of a CPO reduced the cost by $3. The deployment of security analytics saved $7 per compromised record. However, the extensive use of mobile platforms and compliance failures increased the cost per compromised record by $9 and $11 per compromised record, respectively.

The inability to retain customers has serious financial consequences. It pays to keep customers**.** Organizations that lost less than one percent of their customer base had an average

total cost of $2.6 million. If four percent or more was lost, the average cost was $5.1 million. Organizations in Japan, Italy and France lost the most customers. South Africa, Brazil and the ASEAN cluster were better able to keep customers. Industries with the highest churn were financial, health and services. Organizations in the United States paid the highest price for losing customers ($4.13 million).

Cost of Data Breach FAQs

What is a data breach? A breach is defined as an event in which an individual's name and 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 identified three main causes of a data breach: malicious or criminal attack, system glitch or human error. The costs of data breach 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. One example is a retail company's database with an individual's name associated with credit card information and other personally identifiable information. Another is a health insurer's record of the policyholder with physician and payment information. In this year's study, the average cost to the organization per compromised record was $141.

How do you collect the data? Our researchers collected in-depth qualitative data through more than 1,900 separate interviews conducted over a 10-month period in the 419 companies. Recruiting organizations began in February 2016 and interviews were completed March 2017. In each of the 419 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 did not collect organization-specific information.

How do you calculate the cost? To calculate the average cost of data breach, we collected 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 419 organizations to participate in this study. Data breaches range from a low of 2,600 compromised records to slightly more than 100,000.

Can the average cost of data breach be used to calculate the financial consequences of a mega breach such as one involving millions of lost or stolen records? The average cost of data breach in our research does not apply to catastrophic or mega data breaches, such as that of Sony, because these are not typical of the breaches most organizations experience. To be representative of global organizations and draw conclusions from the research that are useful in understanding costs when protected information is lost or stolen, we did not include data breaches of more than approximately 100,000 compromised records in our analysis.

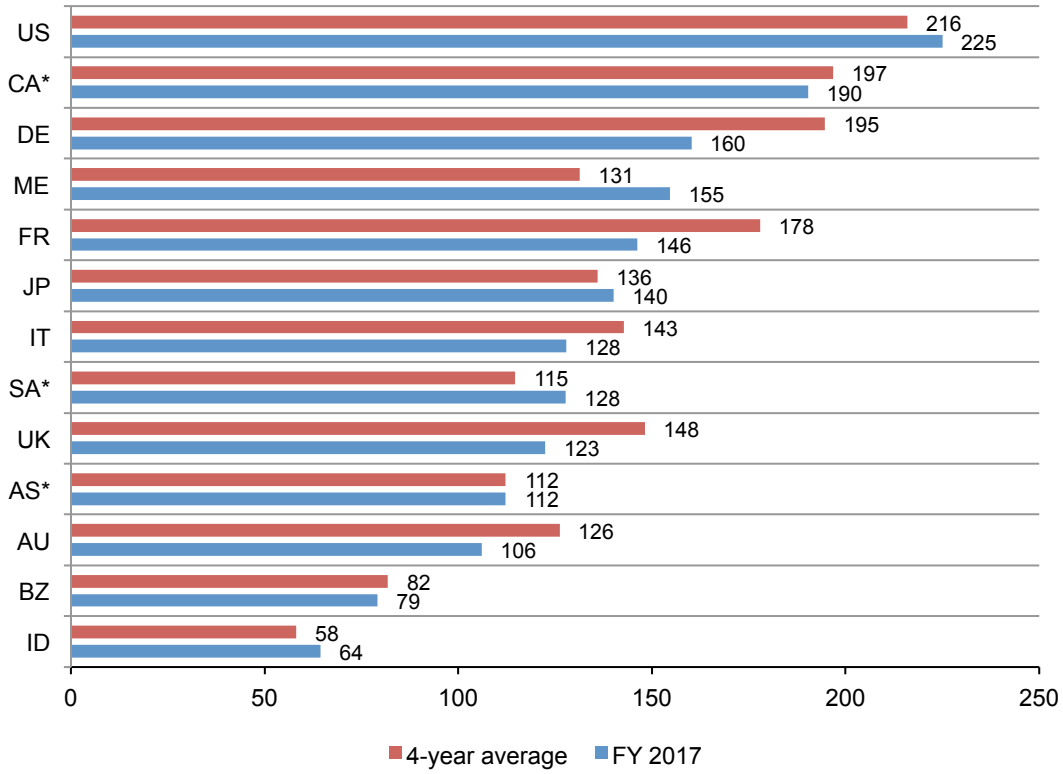
Are you tracking the same organizations each year? Each annual study involves a different sample of companies. In other words, we do not track the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach. Since starting this research in 2005, we have studied the data breach experiences of 2,432 organizations.

Global at a glance

This year's annual study was conducted in 11 countries and two regions: the United States, Germany, Canada, France, the United Kingdom, Italy, Japan, Australia, the Middle East, Brazil, India, South Africa and, for the first time, ASEAN (Association of Southeast Asian Nations**).** A total of 419 organizations participated. Country-specific results are presented in 13 separate reports.

Figure 1 presents the average per capita cost of data breach over four years expressed in U.S. dollars for country or regional studies. As shown in the figure, there was significant variation among countries.[4] The consolidated average per capita cost for all countries was $141 compared to an average of $158 average last year (excluding the ASEAN sample). The United States, Canada and Germany continue to have the highest per capita costs at $225, $190 and $160, respectively. India, Brazil and Australia have much lower per capita costs at $64, $79 and $106, respectively.

Figure 1. The 2017 per capita cost of data breach compared to the four-year average
Grand averages for FY2017=$141, FY2016=$158, FY2015=$154, FY2014=$145
*Historical data are not available for all years
Measured in US$



[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 data breach costs
- 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
- The mean time to identify and contain a data breach

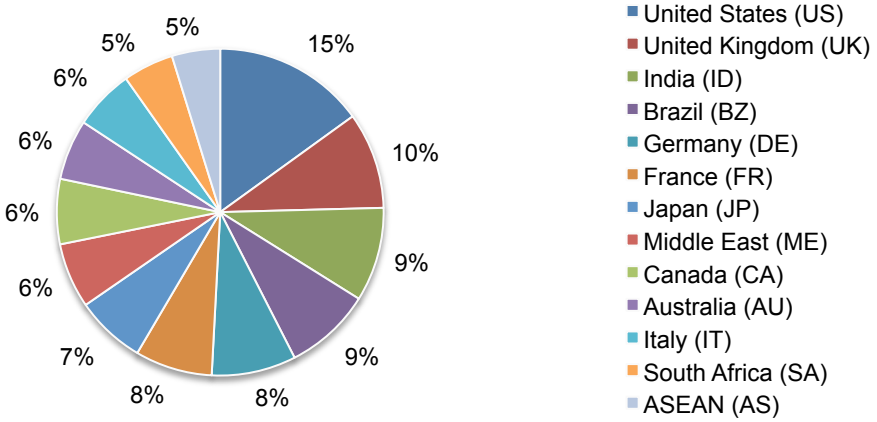
The following table lists countries, legend, sample sizes and currencies used in this global study. It also shows the number of years of annual reporting for each country ranging from one year for ASEAN to 12 years for the United States.

Table 1. Global study at a glance

Legend	Countries	Sample	Pct%	Currency	Years of study
US	United States	63	15%	US Dollar	12
UK	United Kingdom	40	10%	GBP	10
ID	India	39	9%	Rupee	6
BZ	Brazil	36	9%	Real	5
DE	Germany	35	8%	Euro	9
FR	France	32	8%	Euro	8
JP	Japan	29	7%	Yen	6
ME	Middle East*	27	6%	AED/SAR	4
CA	Canada	27	6%	CA Dollar	3
AU	Australia	25	6%	AU Dollar	8
IT	Italy	25	6%	Euro	6
SA	South Africa	21	5%	ZAR	2
AS	ASEAN#	20	5%	SGD	1
	Total	419	100%		

*ME is a cluster sample of companies located in Saudi Arabia and the United Arab Emirates
#ASEAN is a cluster sample of companies located in Singapore, Indonesia, the Philippines and Malaysia.

Pie Chart 1. Frequency of benchmark samples by country

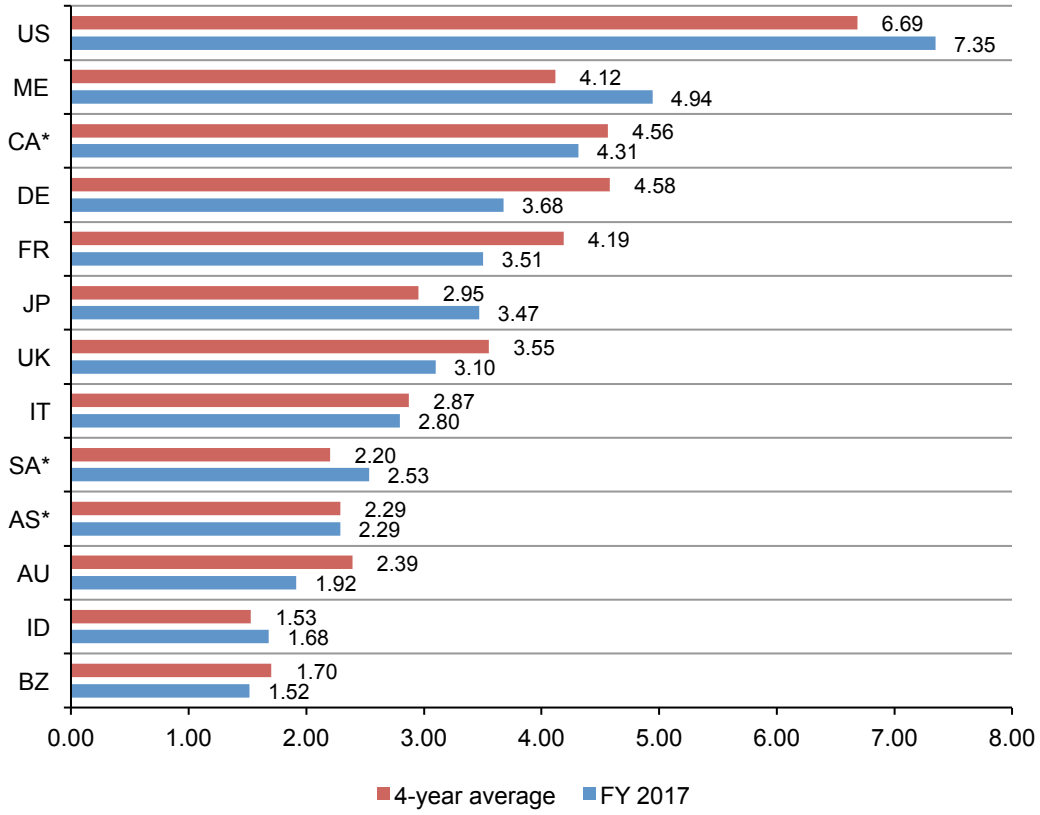


Global and industry differences in data breach costs

The average organizational cost of data breach varies by country. Figure 2 compares this year's total average cost of data breach to the four-year average. The most significant decrease in average total cost occurs in Germany (-.91), France (-.68), Australia (-.48) and the UK (-.45). In contrast, the biggest increases in average total cost are in the Middle East (+.83), United States (+.66) and Japan (+.52).

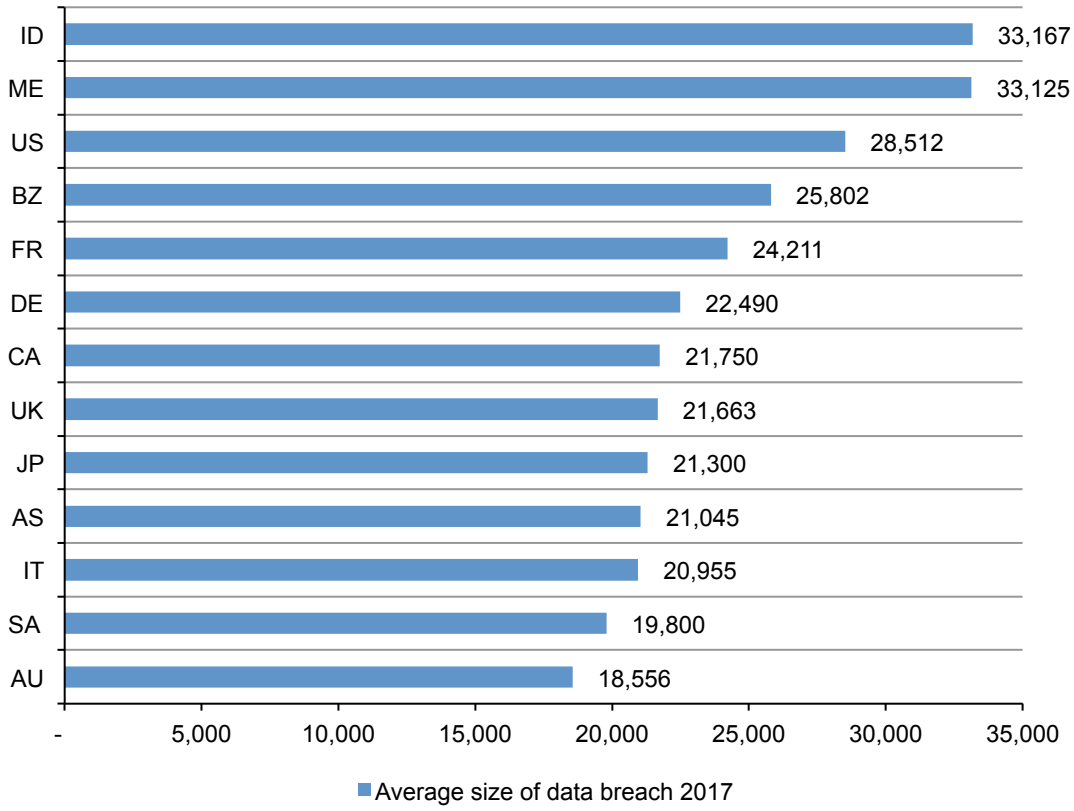
In the FY 2017 study, organizations in the United States had the highest total average cost at $7.35 million, followed by the Middle East at $4.94 million. In contrast, Brazilian and Indian organizations had the lowest total average cost at $1.52 million and $1.68 million, respectively.

Figure 2. The average total cost of a data breach compared to the four-year average
Grand average for FY2017=$3.62, FY2016=$4.00, FY2015=$3.79, FY2014=$3.50
*Historical data are not available for all years
Measured in US$ (millions)



Number of exposed or compromised records by country or region. Figure 3 reports the average size of data breaches for organizations in the countries and regions represented in this research. On average, organizations in India, the Middle East and the United States had the largest average number of breached records. Australia, South Africa and Italy had the smallest average number of breached records. Later in this report, we show the relationship between the number of records lost or stolen and the cost of data breach.

Figure 3. The average number of breached records by country or region
Global average = 24,089



Country differences in the percentage net change in cost of data breach measures[5]. Figure 4 presents four metrics that show the percentage change in data breach measures over the past year.[6] These are: (1) abnormal churn (the greater than expected loss of customers since the breach occurred), (2) size of data breach (the number of records lost or stolen), (3) average total cost of data breach and (4) the per capita cost. Following are the increases and decreases in these metrics for each country.

Percentage net change increase over one year

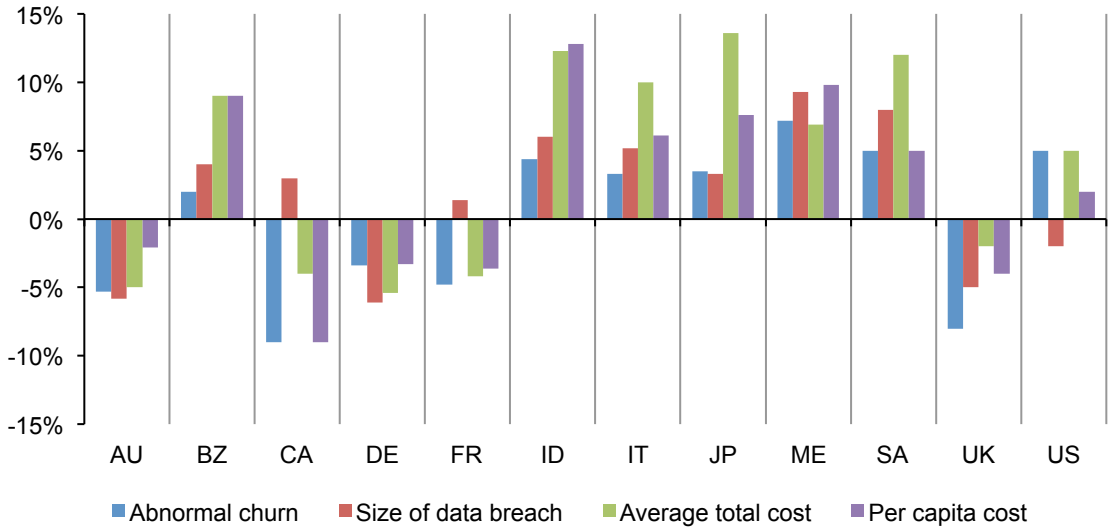
- Abnormal churn: Brazil, India, Italy, Japan, Middle East, South Africa and the U.S.
- Size of breach: Brazil, Canada, France, India, Italy, Japan, Middle East and South Africa
- Average total cost: Brazil, India, Italy, Japan, Middle East, South Africa and the U.S.
- Per capita cost: Brazil, India, Italy, Japan, Middle East and the U.S.

Percentage net change decrease over one year

- Abnormal churn: Australia, Canada, Germany, France, and the UK
- Size of breach: Australia, Germany, the UK and the U.S.
- Average total cost: Australia, Canada, Germany, France and the UK
- Per capita cost: Australia, Canada, Germany, France and the UK

As shown in Figure 4, more countries (Brazil, India, Italy, Japan, the Middle East and South Africa) experienced percentage net increases in all four cost measures. Only three countries (Australia, Germany and the UK) were able to improve all four cost measures and show percentage net change decrease.

Figure 4. Percentage change in data breach measures over the past year
Net change defined as the difference between the 2017 and 2016 results

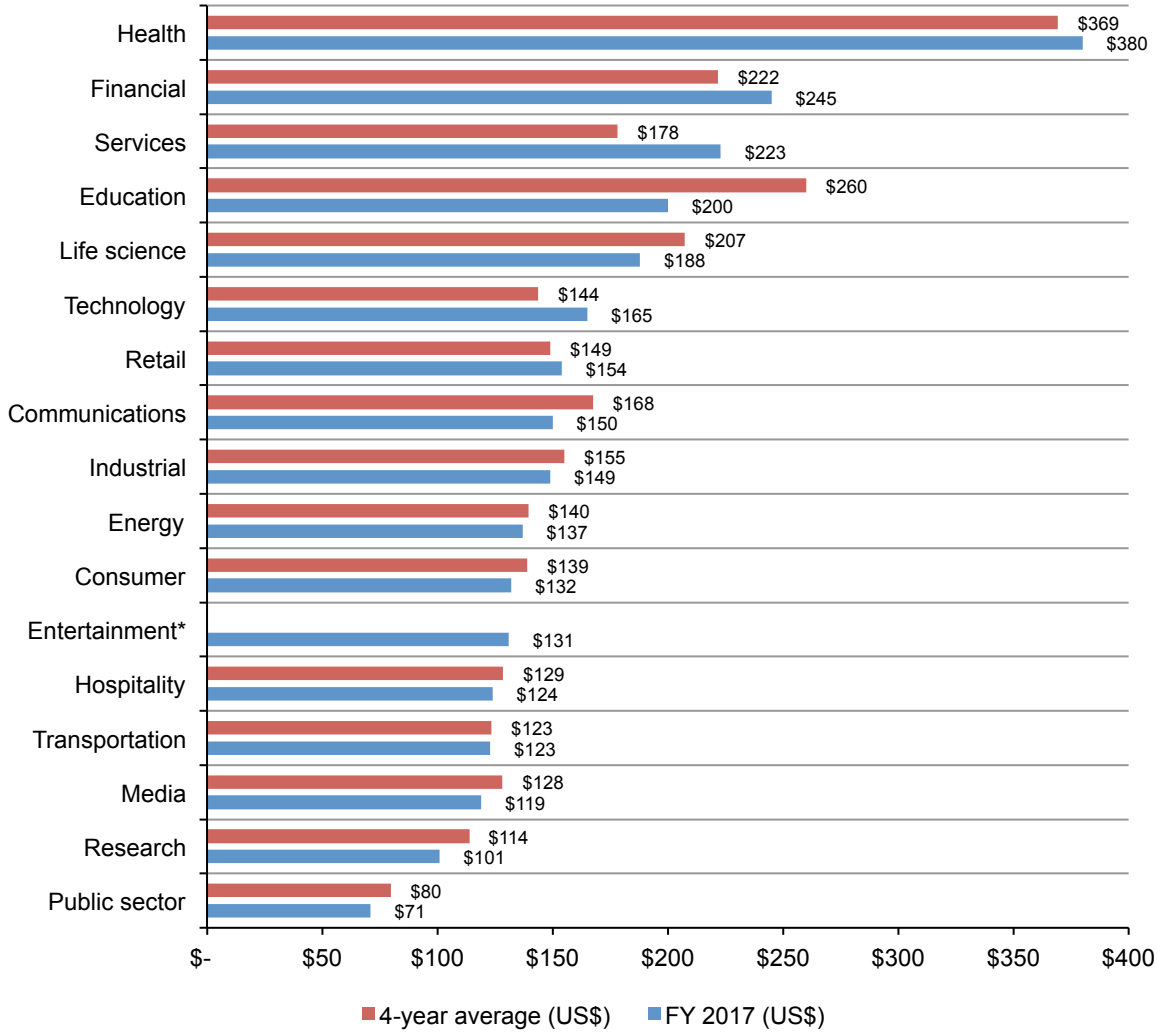


[5]ASEAN is not included in this analysis because this is the first year these countries are included in this research.
[6]The percentage change shown in Figure 4 is calculated from cost figures in local currencies rather than the U.S. dollar. Hence, this analysis is not influenced by currency gains or losses.

Certain industries have higher data breach costs. Figure 5 compares this year's per capita costs for the consolidated sample by industry classification to the four-year average. Heavily regulated industries such as healthcare, education and financial organizations have a per capita data breach cost substantially higher than the overall mean of $141. Public sector, research, media and transportation organizations have a per capita cost well under the overall mean value.

The most significant increases in per capita cost compared to the four-year average were services (+$45), financial (+$23), technology (+$21) and health (+$11). The most significant decreases were education (-$60), life science (-$19) and communications (-$18).

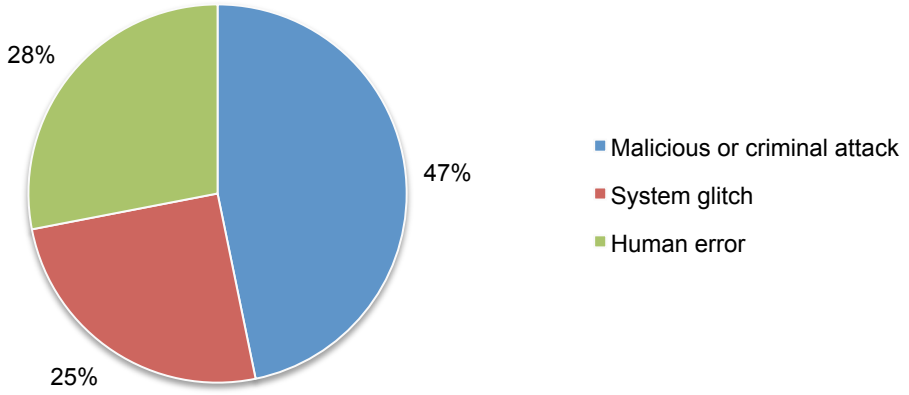
Figure 5. Per capita cost by industry classification
*Historical data are not available for all years
Measured in US$



The root causes of a data breach

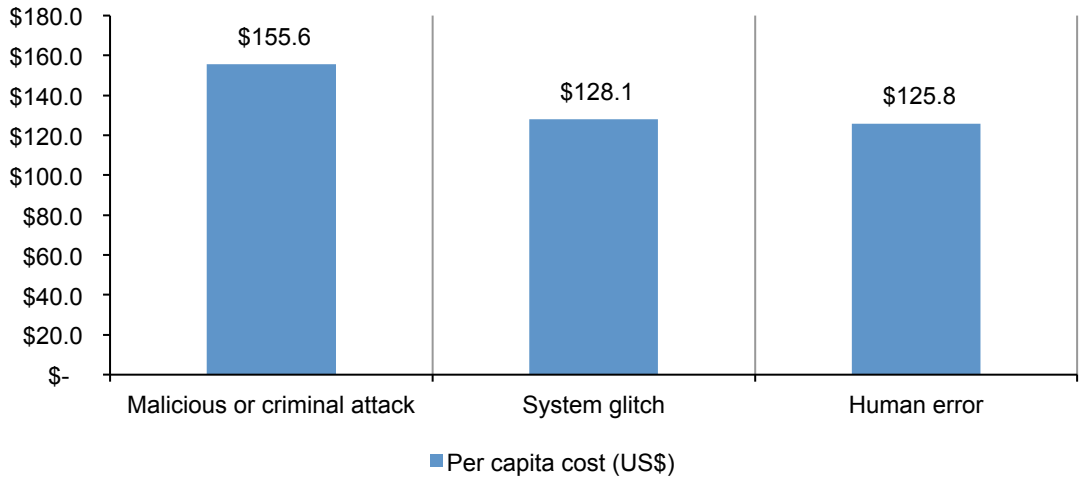
Malicious or criminal attacks cause the most data breaches.[7] Pie Chart 2 provides a summary of the main root causes of data breaches on a consolidated basis for organizations in all countries. Forty-seven percent of incidents involved a malicious or criminal attack, 25 percent were due to negligent employees or contractors (human factor) and 28 percent involved system glitches, including both IT and business process failures.[8]

Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach



Malicious attacks are costlier. Figure 6 reports the per capita cost of data breach for three root causes of the breach incident. In 2017, the cost of data breaches due to malicious or criminal attacks was $156. This is significantly higher than the per capita cost for breaches caused by system glitches and human factors ($128 and $126, respectively).

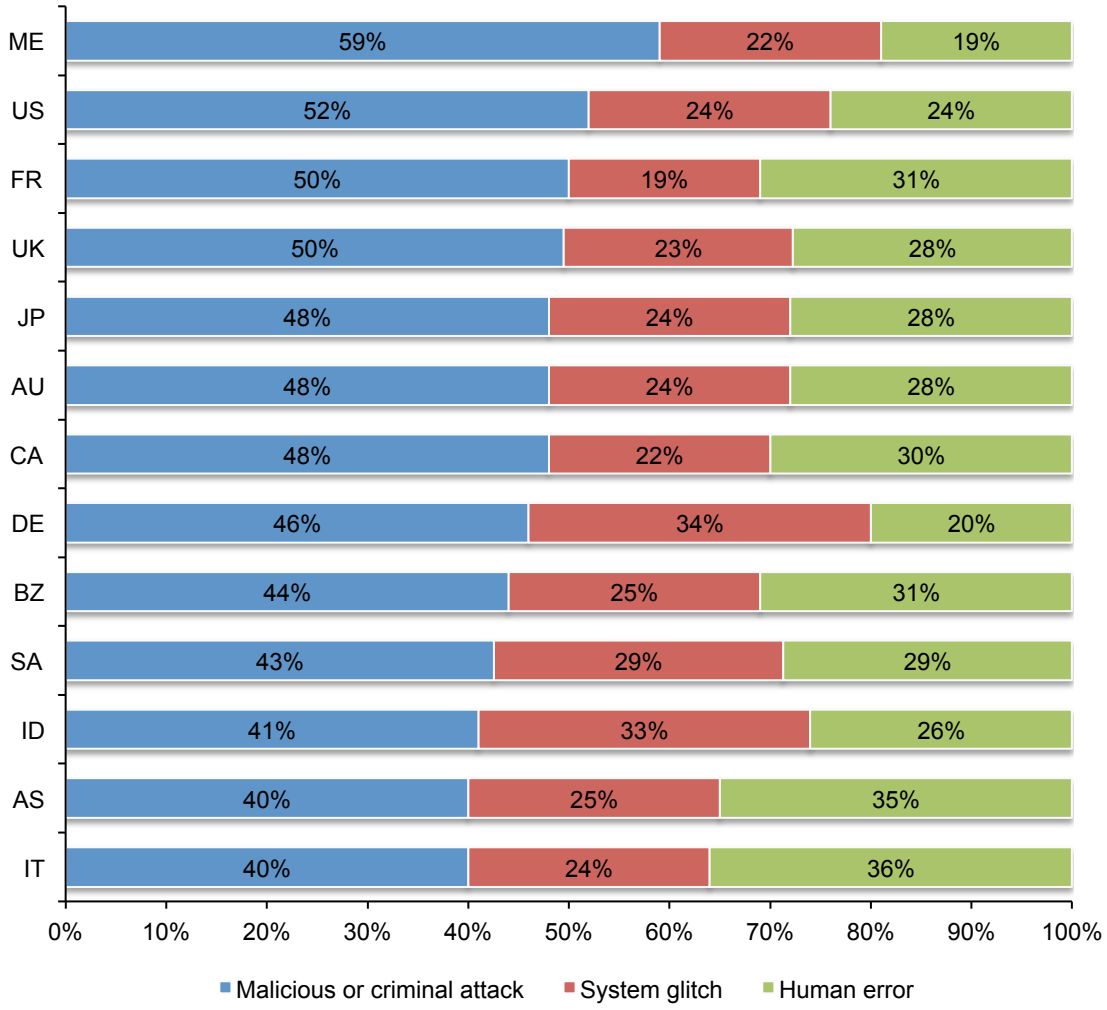
Figure 6. Per capita cost for three root causes of the data breach
Measured in US$



[7]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).
[8]The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

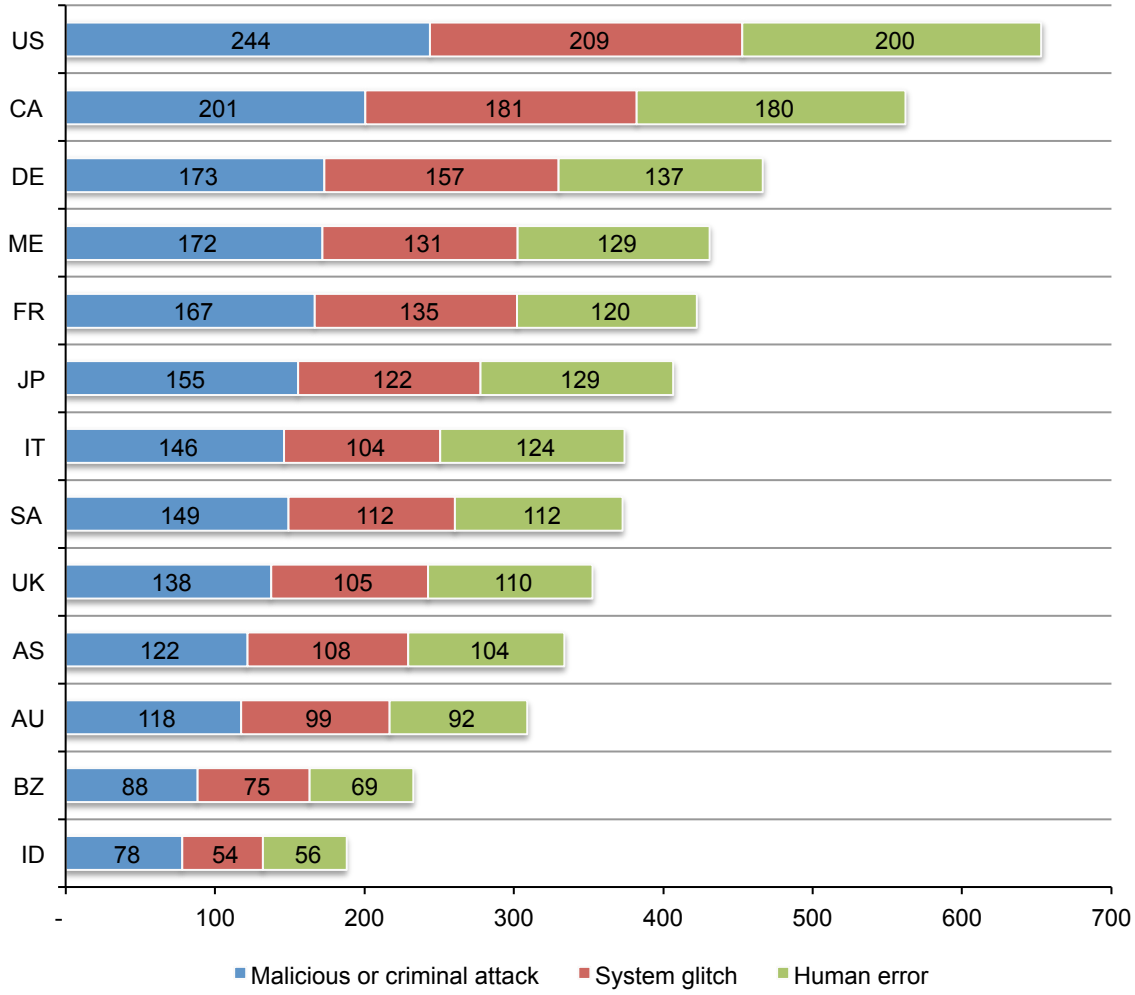
Percentage differences in data breach root causes by country and region. Figure 7 presents the main root causes of data breach for 11 countries and two regions. Organizations in the Middle East region are most likely to experience a malicious or criminal attack (59 percent). In contrast, organizations in Italy, ASEAN and India, were the least likely to experience criminally motivated data breaches. Italian and ASEAN companies had the highest percentage of human error (non-criminal) data breaches and German and Indian organizations were the most likely to experience a data breach due to a system glitch or business process failure.

Figure 7. Percentage of data breach root causes per country and region



The per capita cost for root causes. Figure 8 reports the per capita cost of data breach for three root causes. These results clearly show data breach costs resulting from malicious or criminal attacks were consistently higher than costs resulting from system glitches or human error. There was also wide variation among the countries. In the United States, the cost of a malicious or criminal data breach incident was $244 per compromised record, whereas, in India the per capita cost of a criminally motivated data breach was only $78.

Figure 8. Per capita cost for three root causes of data breach by country and region
Measured in US$



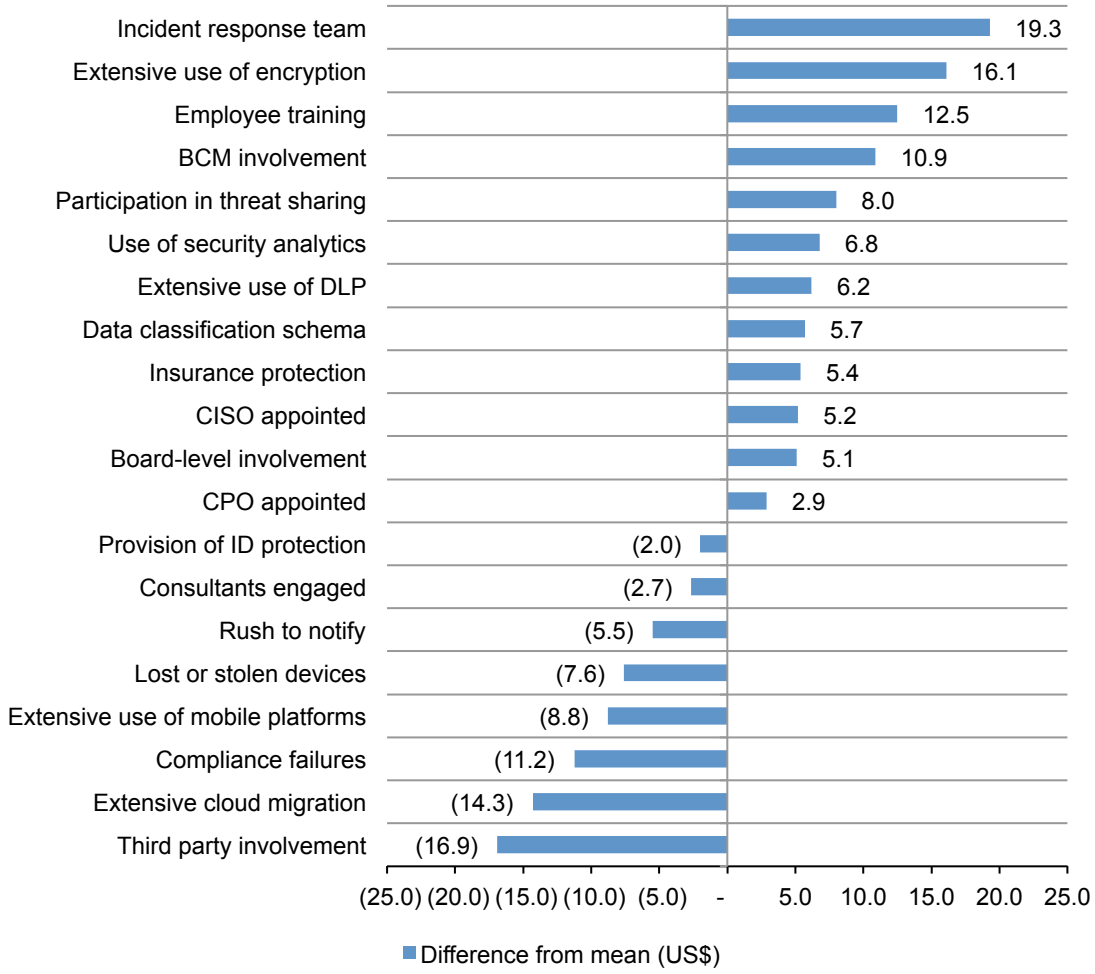
Factors that influence the cost of data breach

Certain factors decrease or increase the cost of data breach. Figure 9 provides a list 20 factors that increase or decrease the per capita cost of data breach. As shown, an incident response team, extensive use of encryption, employee training, BCM involvement, participation in threat sharing, and use of security analytics decreased the per capita cost of data breach by seven or more dollars per compromised record.

Data breaches caused by third party involvement, extensive migration to the cloud, compliance failures, extensive use of mobile platforms, lost or stolen devices or rush to notify increased the per capita cost of data breach (as shown by negative numbers) by five or more dollars.

To illustrate how these factors may affect the cost of data breach, a fully functional incident response team reduced the cost of data breach by $19 from $141 (average) to $122. In contrast, third party involvement in the cause of the data breach resulted in an increase of $17, from $141 to $158.

Figure 9. Impact of 20 factors on the per capita cost of data breach
Measured in US$



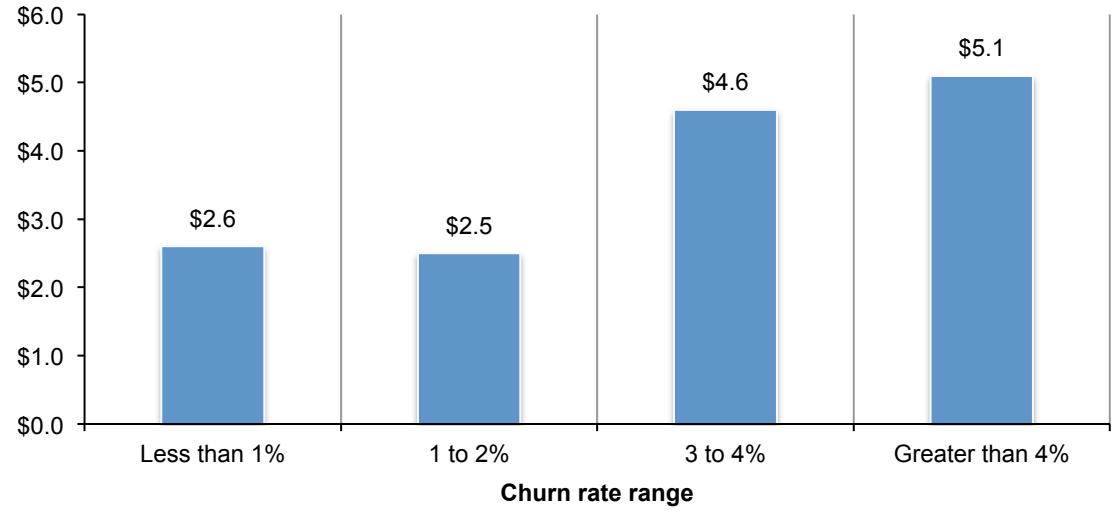
Trends in the frequency of compromised records and customer turnover

The more records lost, the higher the cost of the data breach. Figure 10 shows the relationship between the average total cost of data breach and incident size for 419 organizations in ascending order relative to the size of the data breach incident. In this year's study, the cost ranged from $1.9 million for incidents with less than 10,000 compromised records to $6.3 million for incidents with more than 50,000 compromised records.

Figure 10. Average total cost by size of the data breach
Measured in US$ (millions)

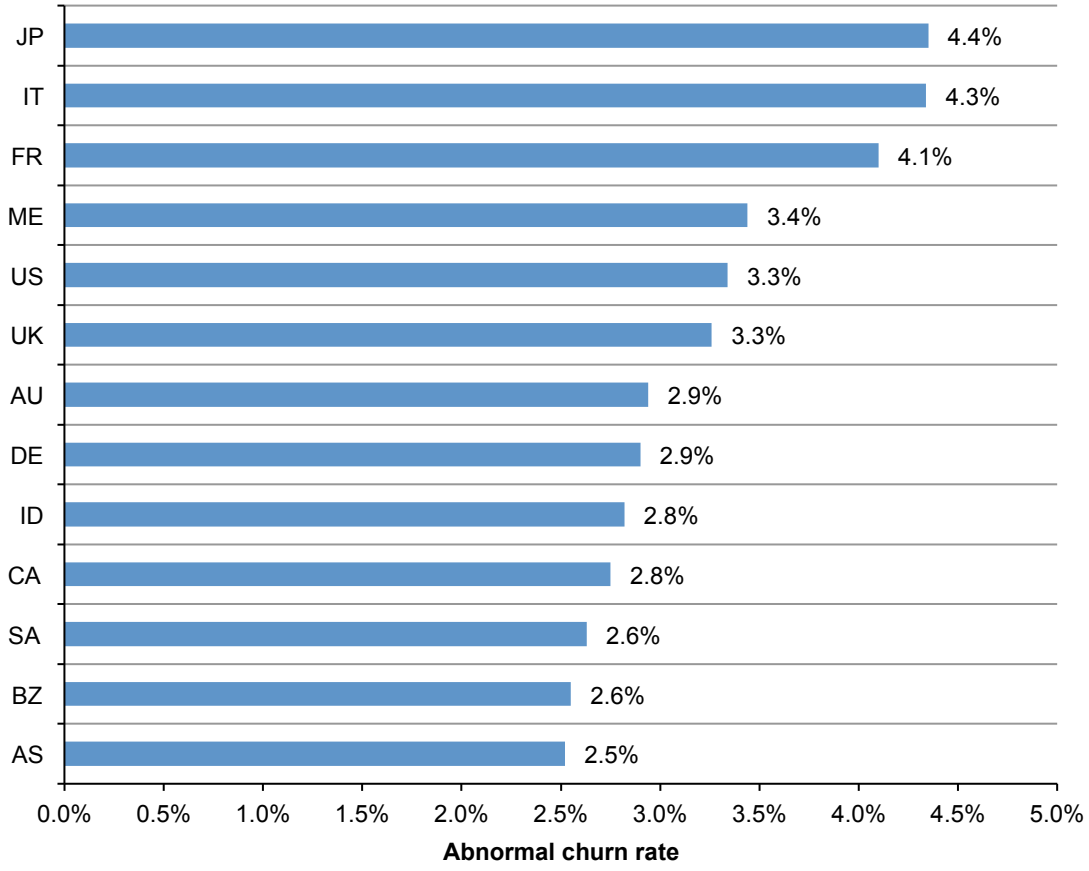
The more churn, the higher the average total cost of data breach. Figure 11 reports the average total cost of data breach for four abnormal churn rates from less than one percent to more than four percent for 419 organizations. Companies that experienced less than a one percent loss of existing customers under one percent had an average total cost of $2.6 million. We estimate an average cost of $5.1 million for companies experiencing a churn rate greater than four percent.

Figure 11. Average total cost by abnormal churn rate
Measured in US$ (millions)



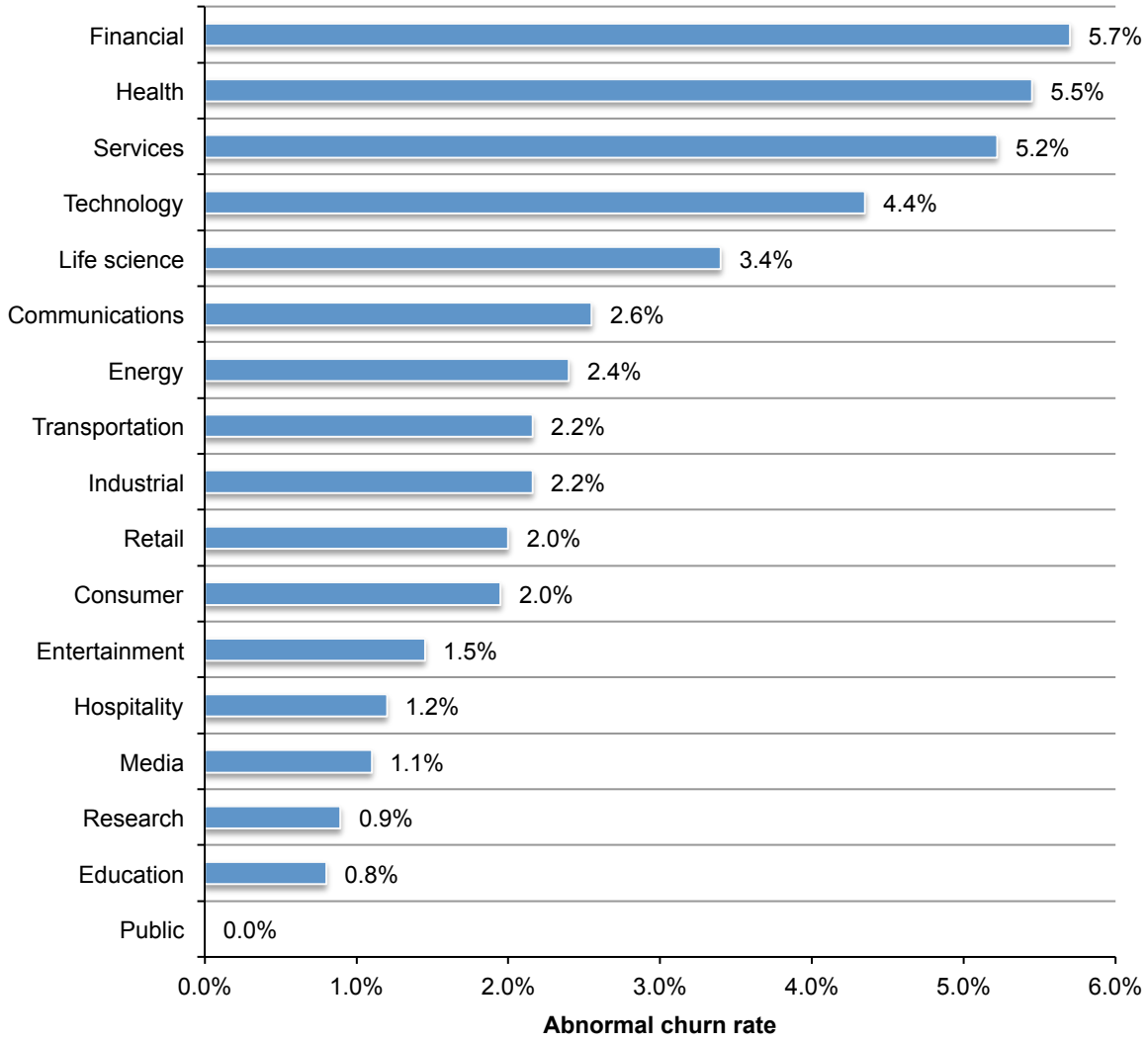
Certain countries are more vulnerable to churn. Figure 12 reports the average abnormal churn rates for all country or regional samples represented in this research. Results show marked differences among countries. Japan, Italy and France experienced the highest abnormal churn rate, whereas, ASEAN, Brazil and South Africa had the lowest abnormal churn rate. The grand average churn rate for our combined sample of 419 companies was 3.24 percent. Last year's average churn rate was 2.90 percent. Thus, organizations in countries with high churn rates can significantly reduce the costs of data breach by emphasizing customer retention activities to preserve reputation and brand value.

Figure 12. Abnormal churn rates by country sample
Grand average for FY 2017=3.24%



Certain industries are more vulnerable to churn. Figure 13 reports the abnormal churn rate of 17 industries. The small sample size in this research prevents us from generalizing the effect of industry on customer churn rates. However, financial, health and service organizations experienced relatively high abnormal churn and public sector and education organizations experienced a relatively low abnormal churn.[9]

Figure 13. Abnormal churn rates by industry
Grand average for FY 2017=3.24%

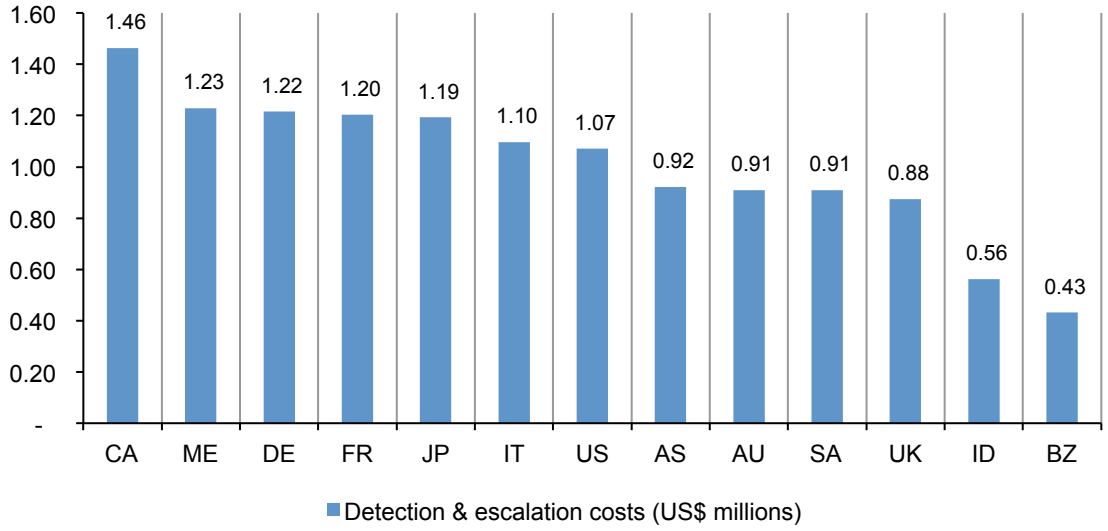


[9]Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have an alternative choice.

Trends in the cost components of a data breach

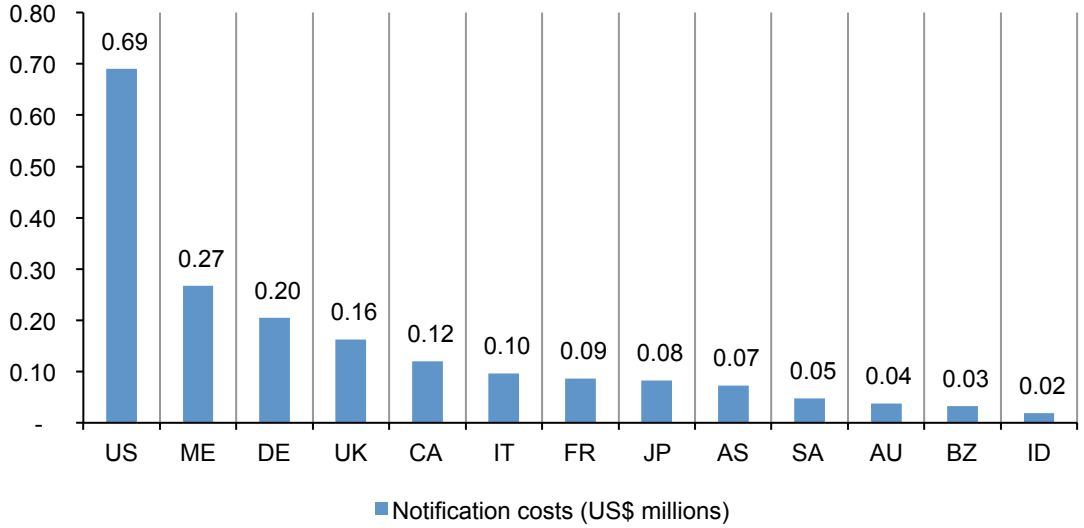
Detection and escalation costs are highest in Canada and lowest in Brazil. Detection and escalation costs include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. As shown in Figure 14, the average detection and escalation cost for Canada was $1.46 million. In contrast, the average cost for Brazil was only $0.43 million.

Figure 14. Detection and escalation costs
Measured in US$ (millions)



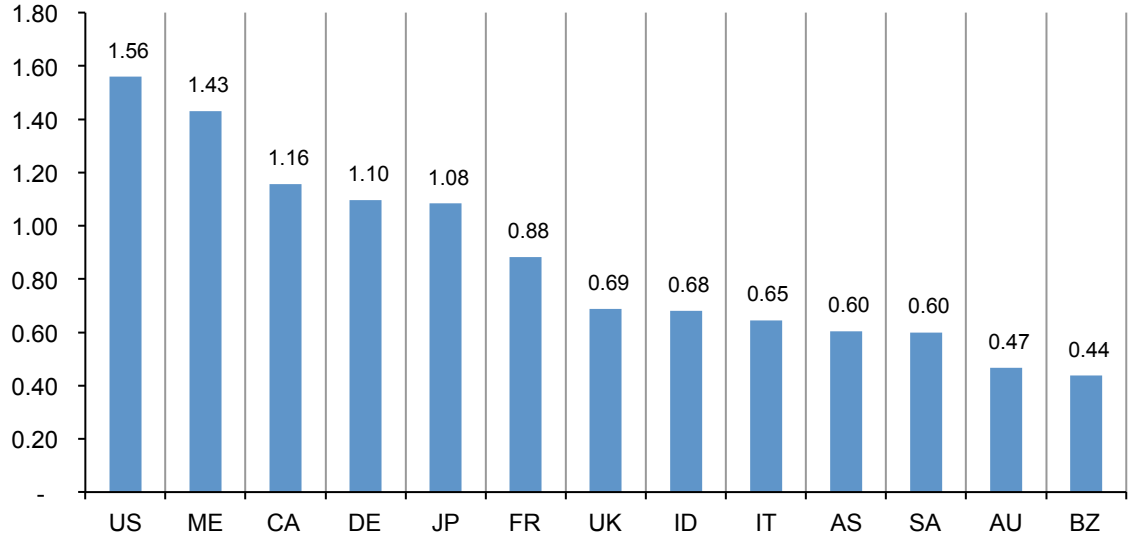
U.S. notification costs are highest. These costs include the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication set up. By far, notification costs for U.S. organizations were the highest ($0.69 million), whereas they were the lowest for India ($0.02), as shown in Figure 15.

Figure 15. Notification costs
Measured in US$ (millions)



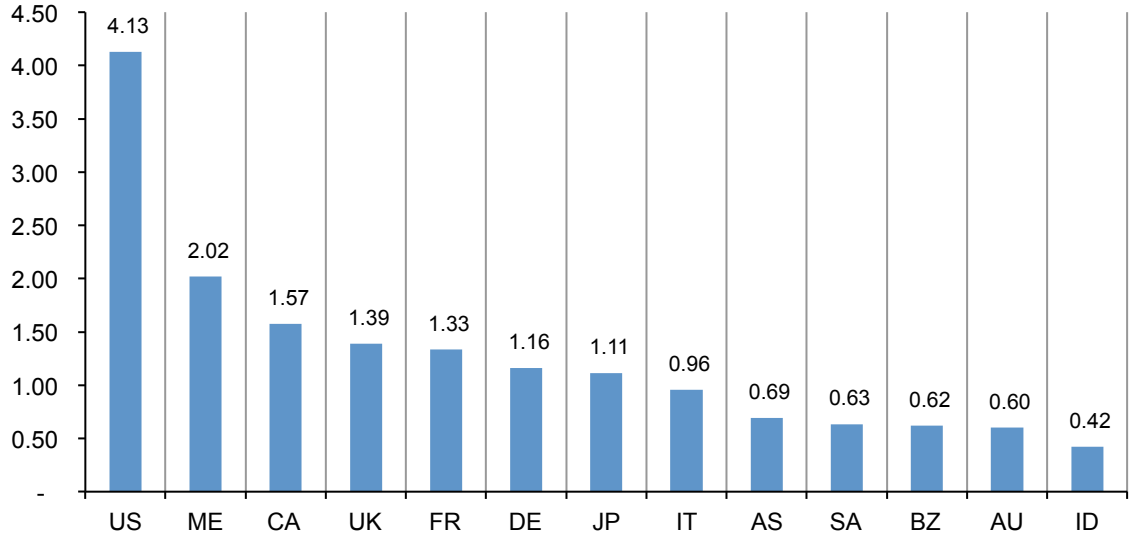
Post data breach response costs are highest in the United States and the Middle East. The costs associated with ex post response and detection in the United States were $1.56 million and $1.43 million in the Middle East, as shown in Figure 16. Ex post costs include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions.

Figure 16. Ex post response costs
Ex post response costs measured in US$ (millions)



U.S. organizations pay the highest price for losing customers after a data breach. According to Figure 17, the cost of lost business was particularly high for U.S. organizations ($4.13 million). This cost component includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.

Figure 17. Lost business costs
Lost business costs measured in US$ (millions)

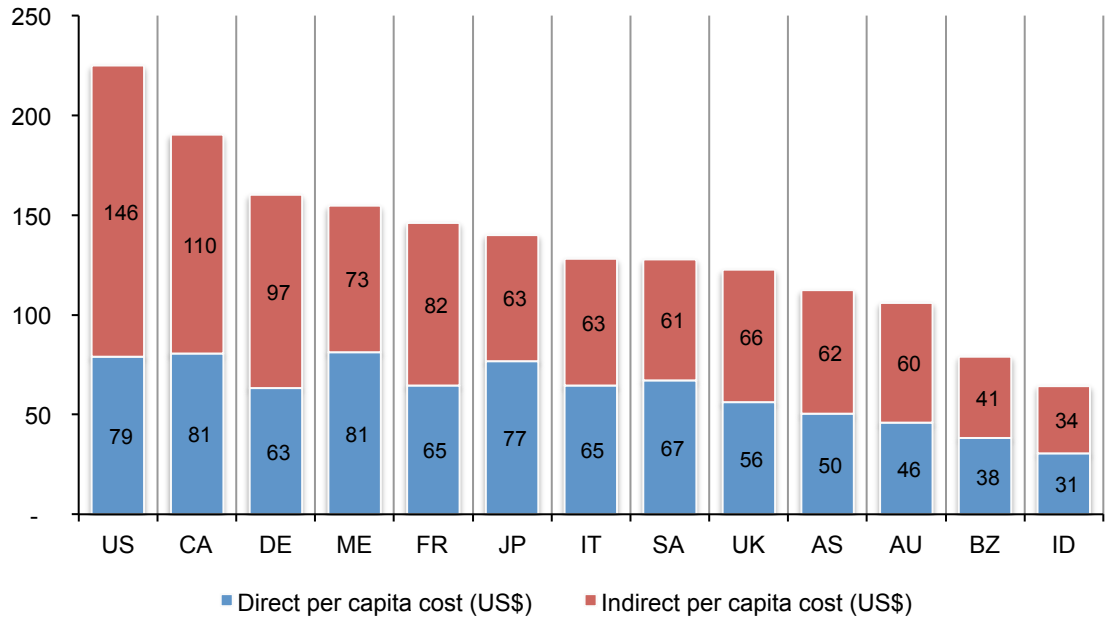


The proportion of direct and indirect costs varies by country

Organizations in the Middle East and Canada have the highest direct costs and U.S. organizations have the highest indirect costs. Direct costs involve funds spent to accomplish a given activity such as engaging forensic experts, hiring a law firm or offering victims identity protection services.

Indirect costs involve the allocation of resources, such as employees' time and effort to notify victims and investigate the breach. Indirect costs also include the loss of goodwill and customer churn. As shown in Figure 18, the Middle East and Canada had the highest direct per capita cost ($81). The United States had the highest indirect per capita cost ($146).

Figure 18. Direct and indirect per capita data breach costs
Measured in US$

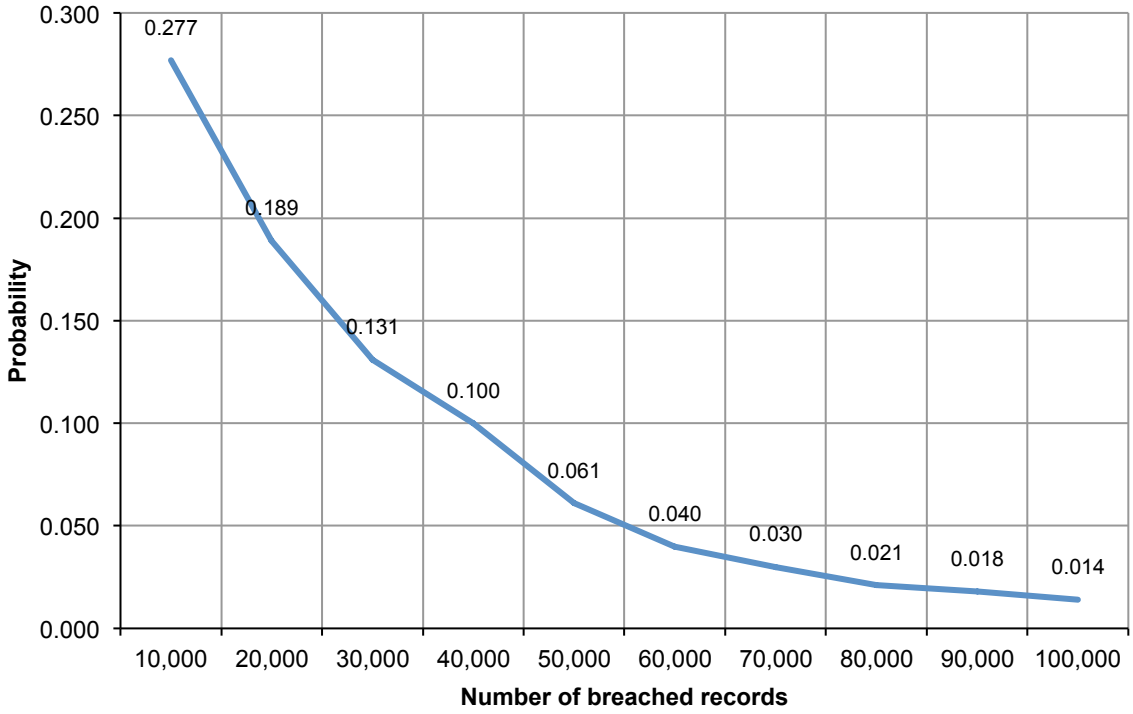


The likelihood an organization will have another data breach

The larger the data breach, the less likely the organization will have another breach in the next 24 months. Based on the experiences of organizations in our research, the probability of a data breach can be predicted based on two factors: how many records are lost or stolen and where the organization is located.

Figure 19 shows the subjective probability distribution of data breach incidents involving a minimum of 10,000 and a maximum of 100,000 compromised records over a 24-month time horizon.[10] As can be seen, the likelihood of data breach steadily decreases as the number of breached records increases. The likelihood of a data breach involving a minimum of 10,000 records is estimated at approximately 27.7 percent over a 24-month period. The chance of a data breach involving a minimum of 100,000 records is less than 1 percent.

Figure 19. Probability of a data breach involving a minimum of 10,000 and a maximum of 100,000 records



[10]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 419 participating companies.

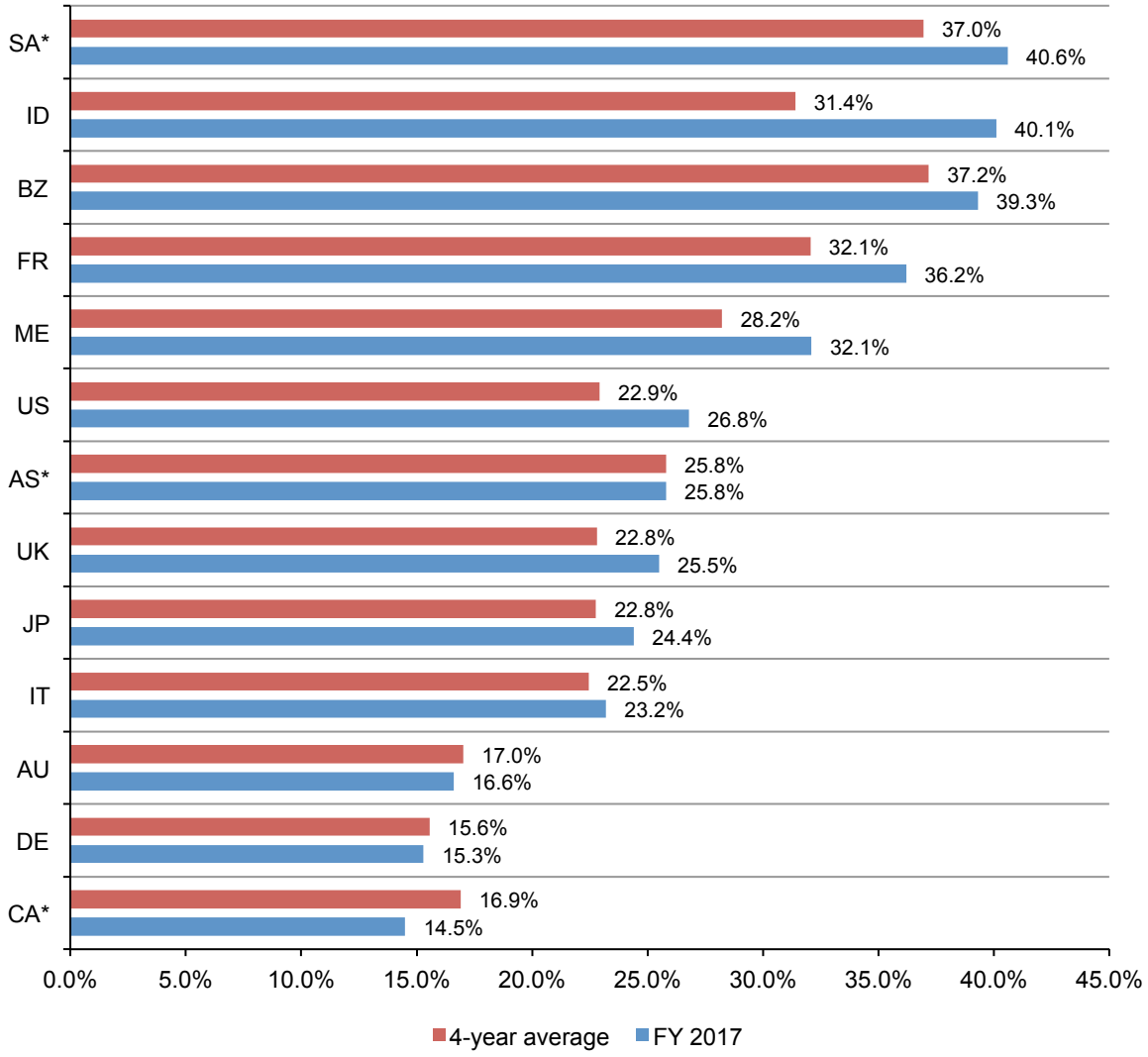
Organizations in South Africa, India and Brazil are more likely to have another data breach. Figure 20 summarizes the probability of a data breach involving a minimum of 10,000 records for country or region samples over a 24-month period. The figure compares the current year's results to a four-year average. While a small sample size prevents us from generalizing country differences, the estimated likelihood of a material data breach varies considerably.

South Africa, India and Brazil appear to have the highest estimated probabilities of a data breach at 40.6 percent, 40.1 percent, and 39.3 percent, respectively. Canada and Germany have the lowest probability of data breach at 14.5 percent and 15.3 percent, respectively.

It is interesting to note that nine of 13 countries showed an increase in the probability of data breach. India had the largest increase at 8.7 percent, followed by France at 4.2 percent. In contrast, Canada had the largest decrease at -2.4 percent.

Figure 20. The 2017 probabilities of a data breach involving a minimum of 10,000 records compared to four-year averages

Grand averages in FY2017=27.7%, FY2016=25.6%, FY2015=24.5%, FY2014=22.2%
A minimum of 10,000 compromised records
*Historical data are not available in all years

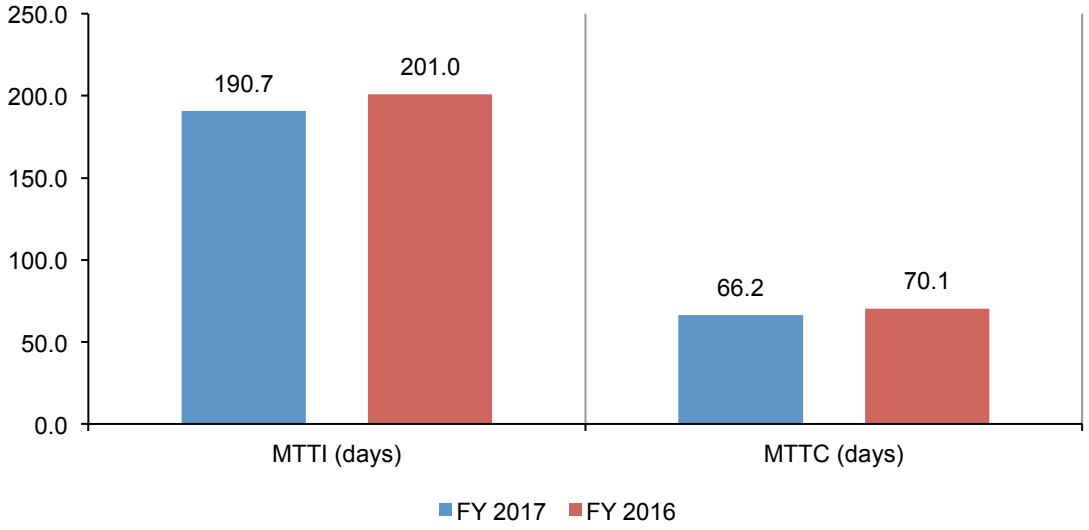


The time to identify and contain data breaches impact costs

The faster the data breach can be identified and contained, the lower the costs. MTTI and MTTC metrics are used to determine the effectiveness of an 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.

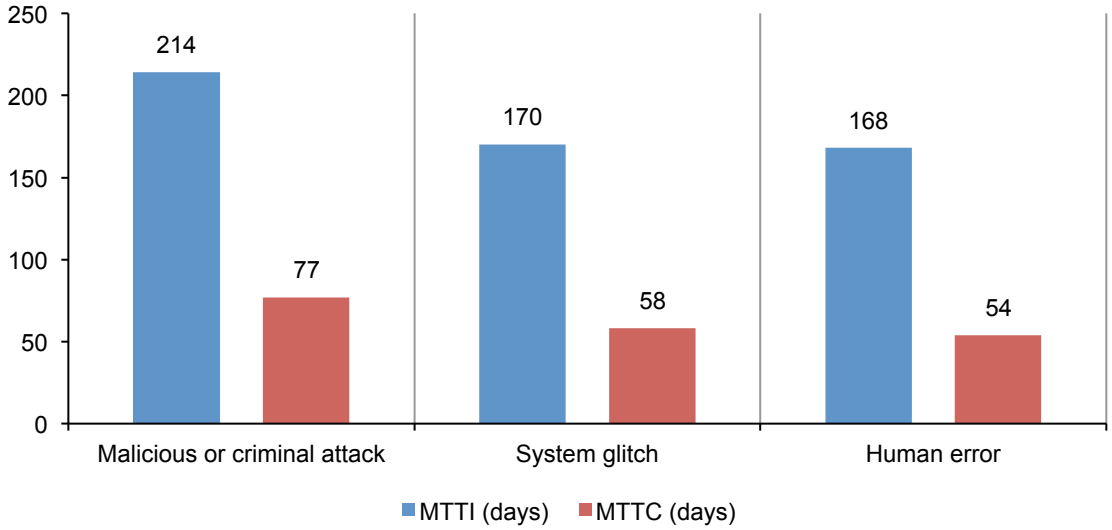
As shown in Figure 21, since last year, the MTTI and MTTC of a data breach decreased. In this year's study, for our consolidated sample of 419 companies, the MTTI was 191 days. The MTTC was 66 days with a range of 10 to 164 days. Last year's MTTI and MTTC were 201 and 70 days, respectively.

Figure 21. Days to identify and contain the data breach over the past year



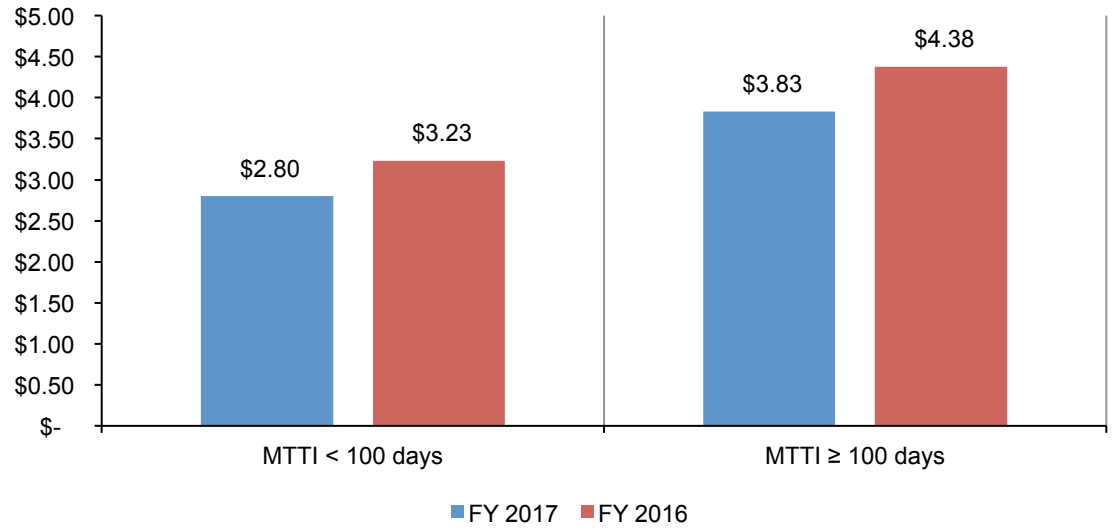
Malicious or criminal attacks take longer to identify and detect. Figure 22 provides the MTTI and MTTC for three root causes of the data breach incident. As shown, both the time to identify and time to contain is highest for malicious and criminal attacks (214 and 77 days, respectively). They are much lower for data breaches caused by human error (168 and 54 days, respectively).

Figure 22. Days to identify and contain data breach incidents by root cause



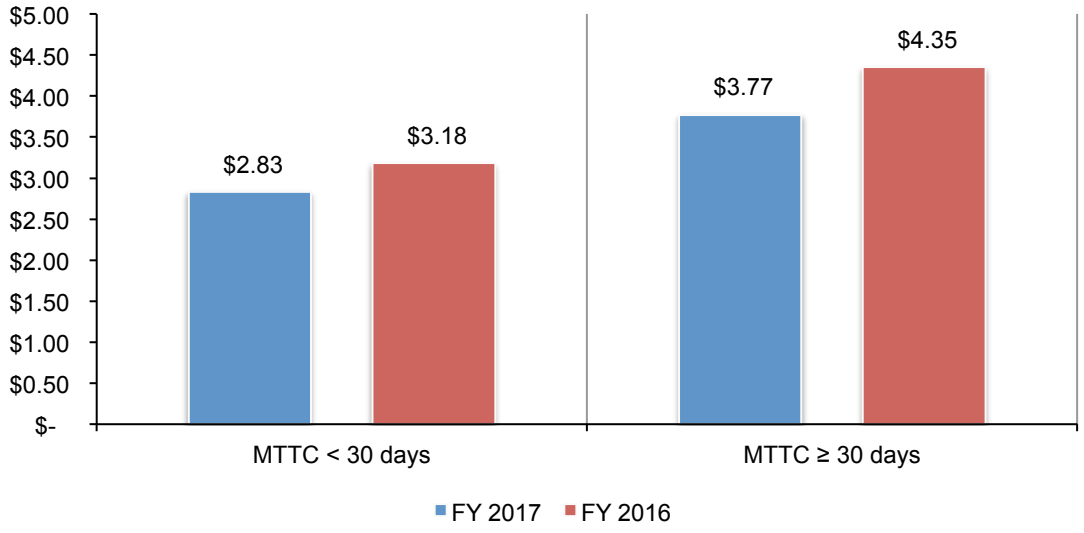
The failure to quickly identify the data breach increases costs. Figure 23 shows a relationship between total data breach costs and breach identification for 419 companies. We bifurcated the consolidated sample according to those with an MTTI below 100 days and those with an MTTI above 100 days. If the MTTI was under 100 days, the estimated average total cost of data breach was $2.80 million. If it was over 100 days, the estimated cost was $3.83 million. The significant cost difference between these two subsamples suggests that the failure to quickly identify the data breach leads to higher costs. Having tools that heighten detective or forensic capabilities can significantly reduce data breach cost. Last year's average total cost was $3.23 million (less than 100 days to identify) and $4.38 (100 days or greater to identify).

Figure 23. Relationships between mean time to identify and average total cost
Measured in US$ (millions)



The time to contain a data breach affects the cost. Figure 24 shows a relationship between total data breach cost and breach containment for 419 companies. We bifurcated the consolidated sample between those with an MTTC below and above 30 days. If the MTTC was less than 30 days, the estimated average total cost of data breach was $2.83 million. If it took more than 30 days to contain the breach, the estimated cost was $3.77 million. The significant cost difference between these two subsamples suggests the failure to quickly contain the data breach will lead to higher costs. Having tools and processes that heighten remediation capabilities, such as a fully functional incident response process can significantly reduce data breach cost. Last year's average total cost was $3.18 million (less than 30 days to contain) and $4.35 (30 days or greater to contain).

Figure 24. Relationships between mean time to contain and average total cost
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 in which they engage to resolve the data breach.

Typical activities for the discovery of 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 discovery:

- Audit and consulting services
- Legal services for defense
- Legal services for compliance
- Free or discounted services offered 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 allocated to data breach resolution, 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 is 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: Communication with victims of a breach to help them minimize potential harms and other assistance such as credit report monitoring or reestablishing a new account or credit card.

In addition to the above process-related activities, most companies experience opportunity costs associated with the breach incident. Such costs are the result of diminished trust or confidence by present and future customers. Accordingly, Ponemon Institute's research shows that the negative publicity associated with a data breach incident causes reputation effects that may lead to 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.[11]

- 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.

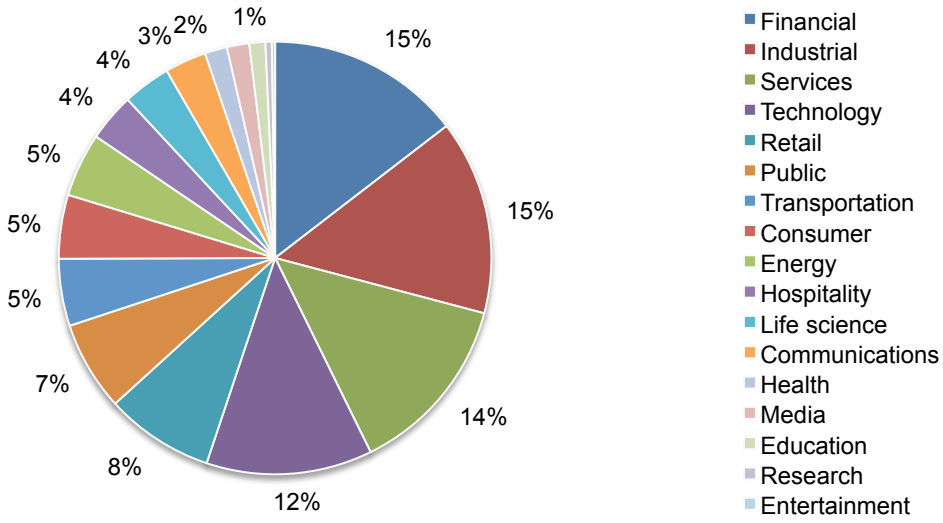
We acknowledge that the loss of non-customer data, such as employee records, may not impact an organization's churn or turnover.[12] In these cases, we would expect the business cost category to be lower when data breaches do not involve customer or consumer data (including payment transactional information).

[11] In several instances, turnover is partial, as in cases when breach victims 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.
[12] In this study, we consider citizen, patient and student information as customer data.

Part 4. Organizational Characteristics and Benchmark Methods

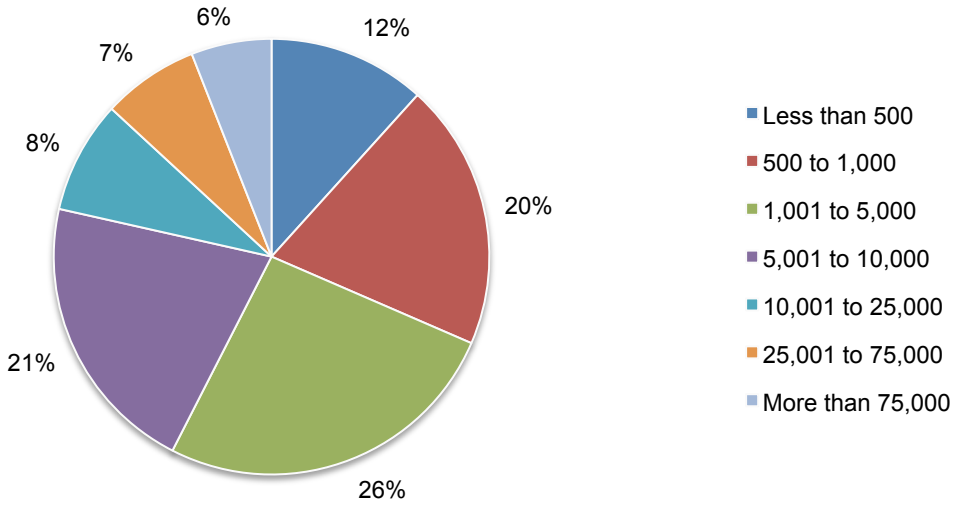
Pie Chart 3 shows the distribution of benchmark organizations by their primary industry classification. Seventeen (17) industries were represented in this year's study. The largest sectors were financial services and industrial companies. Financial service companies included banks, insurance, investment management and payment processors.

Pie Chart 3. Distribution of the benchmark sample by industry segment



Pie Chart 4 shows the distribution of benchmark organizations by total headcount. The largest segment included companies with 1,001 to 5,000 employees. The smallest segment included companies with more than 75,000 employees

Pie Chart 4. Global headcount of participating companies



Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant. 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 ensure a manageable size for the benchmarking process, 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 better quality 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, 419 companies completed the benchmark process. Non-response bias was not tested so it is possible that 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 omitted 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, it is always possible 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.

- Currency translation gains and losses: This year**,** a strong U.S. dollar significantly influenced the global cost analysis. The conversion from local currencies to the U.S. dollar deflated the per capita and average total cost estimates, especially for companies in the U.K., Germany, France and Italy (e.g., the Pound (£) and Euro (€)). For purposes of consistency with prior years, we decided to continue to use the same accounting method rather than adjust the cost. It is important to note, that this issue only affects the global analysis because all country-level results are shown in local currencies.

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.

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.