2018 Cost of a Data Breach Study: Global Overview

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

July 2018

→ Part 1/ Executive Summary 3

→ Part 2/ Our Methodology at a Glance 5

→ Part 3/ Key Findings 9

→ Part 4/ Full Detailed Findings 11

→ Part 5/ How We Calculate the Cost of a Data Breach 42

→ Part 6/ Organizational Characteristics and Benchmark Methods........ 44

→ Part 7/ Limitations 46

Part 1. Executive Summary

IBM Security and Ponemon Institute are pleased to release the *2018 Cost of a Data Breach Study: Global Overview*[1]. This year we conducted interviews with more than 2,200 IT, data protection, and compliance professionals from 477 companies that have experienced a data breach over the past 12 months. According to the findings, data breaches continue to be costlier and result in more consumer records being lost or stolen, year after year.

Global study at a glance

> Average total cost of a data breach: **$3.86 million**

> Average cost per lost or stolen record: **$148**

> Likelihood of a recurring material breach over the next two years: **27.9%**

> Average total one-year cost increase: **6.4%**

> One-year increase in per capita cost: **4.8%**

> Average cost savings with an Incident Response team: **$14 per record**

This year we found that the **average total cost** of a data breach, the average cost for each lost or stolen record (**per capita cost**), and the **average size** of data breaches have all increased beyond the 2017 report averages:

> The average total cost rose from $3.62 to $3.86 million[2], an increase of 6.4 percent

> The average cost for each lost record rose from $141 to $148, an increase of 4.8 percent

> The average size of the data breaches in this research increased by 2.2 percent

In addition to presenting trends in the various components of the cost of a data breach, the global study determines the **likelihood** that an organization will have one or more data breaches in the next two years. Two factors were used to determine the probability of a future data breach: the size of the data breach reported in this year's research and where the organization is located.

> The average global probability of a material breach[3] in the next 24 months is 27.9 percent, an increase over last year's 27.7 percent

> South Africa has the highest probability of experiencing a data breach at 43 percent

> Germany has the lowest probability of having a future data breach at 14.3 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 2017 calendar year.

[2] Local currencies were converted to U.S. dollars.

[3] A breach that involves a minimum of 1,000 lost or stolen records containing personal information.

As in past years, our study reports on the relationship between how quickly an organization can **identify and contain** data breach incidents and the financial consequences.

- The mean time to identify (MTTI) was 197 days
- The mean time to contain (MTTC) was 69 days
- Companies that contained a breach in less than 30 days saved over $1 million vs. those that took more than 30 days to resolve[4]

For the first time this year, we researched the influence of two new cost factors: **security automation** and the extensive use of **Internet of Things (IoT) devices**. Also for the first time we measure the cost of a data breach involving more than one million compromised records, or what we refer to as a **mega breach**.

- The average cost of a breach for organizations that fully deploy security automation is $2.88 million
- Without automation, estimated cost is $4.43 million, a $1.55 million net cost difference
- The extensive use of IoT devices increased cost by $5 per compromised record
- A mega breach of 1 million records yields an average total cost of $40 million
- A mega breach of 50 million records yields an average total cost of $350 million

Our research takes a variety of cost factors into account. By providing an overview of our methodology and by defining the factors and their weight and influence on our findings, we hope to help organizations make better decisions regarding resource allocation and to minimize financial consequences when the inevitable data breach strikes.

[4] $3.09 million vs $4.25 million

Part 2. Our Methodology at a Glance

For a more in depth explanation of the methodology used for this report, see How We Calculate the Cost of a Data Breach, Organizational Characteristics and Benchmark Methods, and Limitations.

In this section of the report, we discuss reasons for the fluctuation of data breach costs across countries, the use of activity-based costing to calculate the cost of a data breach, the factors that affect the cost, and frequently asked questions about the study.

Countries and regions surveyed

This year's study included the following 15 country or regional samples:

- ASEAN[5]
- Australia
- Brazil
- Canada
- France
- Germany
- India
- Italy
- Japan
- South Africa
- South Korea
- The Middle East[6]
- Turkey
- United Kingdom
- United States

What explains the increases in the cost of a data breach this year for most organizations? In contrast, why did organizations in some countries experience a reduction of the per capita and average total costs? Understanding how the cost of a data breach is calculated will explain the variance among the countries' results in this research.

How we gathered the data

For the *2018 Cost of a Data Breach Study: Global Overview,* we recruited 477 organizations and interviewed more than 2,200 individuals who are knowledgeable about the data breach incident in these organizations. The first data points we collected from these organizations were the number of customer records lost or stolen in the breach and what percentage of their customer base was lost following the data breach.

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. Other issues covered that may have an influence on the cost are the root causes of the data breach and the time to detect and contain the incident.

[5] ASEAN includes Singapore, Indonesia, Philippines and Malaysia.

[6] Middle East includes the United Arab Emirates and Saudi Arabia.

How the cost of a data breach is calculated

To calculate the cost of a data breach, we use an accounting methodology called activity-based costing (ABC). This methodology identifies activities and assigns a cost according to actual use. The ABC methodology is fully explained in Part 5 of this report.

Four process-related activities drive a range of expenditures associated with an organization's data breach detection, escalation, notification, and activities conducted following a data breach. The four cost centers are:

> Detection and escalation:

Activities that enable a company to detect and report the breach to appropriate personnel within a specified time period.

Examples:

- Forensic and investigative activities
- Assessment and audit services
- Crisis team management
- Communications to executive management and board of directors

> Post data breach response:

Processes set up to help individuals or customers affected by the breach to communicate with the company, as well as costs associated with redress activities and reparation with data subjects and regulators.

Examples:

- Help desk activities/inbound communications
- Credit report monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory interventions (fines)

> Notification costs:

Activities that enable the company to notify individuals who had data compromised in the breach (data subjects) as regulatory activities and communications.

Examples:

- Emails, letters, outbound telephone calls, or general notice that personal information was lost or stolen
- Communication with regulators; determination of all regulatory requirements, engagement of outside experts

> Lost business cost:

Activities associated with cost of lost business including customer churn, business disruption, and system downtime.

Examples:

- Cost of business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers
- Reputation losses and diminished goodwill

Factors found to affect the cost of a data breach

> **The unexpected loss of customers following a data breach**
Programs that preserve customer trust and loyalty in advance of a breach will help reduce the degree of abnormal churn. This year more organizations worldwide lost customers as a result of their data breaches. However, organizations with a senior-level leader, such as a chief privacy officer (CPO) or chief information security officer (CISO), directing initiatives to improve customer trust in the guardianship of their personal information reduces churn and, therefore, the cost of the breach. Organizations that offer data breach victims identity protection in the aftermath are also more successful in reducing churn.

"Each year we anticipate the latest cost of data breach study because it has truly helped to show our management the value of good data protection practices. We especially like the various factors that can increase or decrease costs and have used them to justify investments."

— CISO/US/Financial Services

> **The size of the breach or the number of records lost or stolen**
Of course, the more records lost, the higher the cost of a data breach. 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 to 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 experienced increases in both the time to identify and to contain a breach. We attribute increases in this years' time to identify and time to contain to the increasing severity of criminal and malicious attacks experienced by a majority of companies in our sample.

> **Effective management of detection and escalation costs**
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.

> **Effective management of post data breach costs**
These costs include help desk activities, inbound communications, issuing new accounts or credit cards, legal expenditures, product discounts, identity protection services, and regulatory interventions. As shown in this year's study, insurance protection and business continuity management (BCM) reduced the cost of a 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 to assist in the remediation of a data breach all increase post data breach costs. Expenditures to resolve lawsuits also increase post data breach costs.

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 $148.

How do you collect the data? Our researchers collected in-depth qualitative data through more than 2,500 separate interviews conducted over a 10-month period within 477 companies. Recruiting organizations began in February 2017 and interviews were completed in April 2018. In each of the 477 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. Only events directly relevant to the data breach experience are represented in this research. For example, new regulations such as the General Data Protection Regulation (GDPR), ransomware and other cyber attacks may encourage organizations to increase investments in their cybersecurity governance technologies, but do not directly affect the cost of a data breach as presented in this research.

How do you calculate the cost? To calculate the average cost of a 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. For purposes of consistency with prior years, we use the same currency translation method rather than adjust accounting costs. This approach only affects the global analysis because all country-level results are shown in local currencies.

How does benchmark research differ from survey research? The unit of analysis in the *Cost of a Data Breach Study* is the organization. In survey research, the unit of analysis is the individual. We recruited 477 organizations to participate in this study. Data breaches range from a low of 2,500 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 a data breach in our research does not apply to catastrophic or mega data breaches, such as Equifax or Facebook. These are not typical of the breaches many organizations experience. Hence, to draw useful conclusions in understanding data breach cost behaviors, we target data breach incidents that do not exceed 100,000 records. However, this year's study presents an alternative framework for measuring the cost impact involving one million or more records.

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 2,909 organizations.

Why are we using simulation methods to estimate the cost of a mega data breach? The sample size of 11 companies experiencing a mega breach is too small to perform a statistically significant analysis using activity-based cost methods. To remedy this issue, we deploy Monte Carlo simulation. This analytic approach allows us to estimate a range of possible (random) outcomes through repeated trials. In total, we performed more than 150,000 trials. The grand mean of all sample means provides a most likely outcome at each size of data breach — ranging from 1 million to 50 million compromised records.

Part 3. Key Findings

In this section of the report we provide a brief summary of the most salient findings from the research and how costs have changed over the past year.

The global cost of data breach increased.
The average total cost of data breach increased by 6.4 percent and the per capita cost increased by 4.8 percent. The average size of a data breach (number of records lost or stolen) also increased by 2.2 percent.

Data breaches are the most costly in the United States and the Middle East and least costly in Brazil and India.
The average total cost in the United States was $7.91 million and $5.31 million in the Middle East. The lowest average total cost was $1.24 million in Brazil and $1.77 million in India. The highest average per capita costs were $233 in the United States and $202 in Canada.

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 at $740,00 whereas India had the lowest at $20,000.

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 $1.76 million and $1.47 million in the Middle East.

Canada has the highest direct costs and the United States has the highest indirect costs.
Canada had the highest direct cost at $81 per compromised record. Direct costs refer to the 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 at $152. 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 faster a data breach can be identified and contained, the lower the costs.
For the fourth year, our study reports on the relationship between how quickly an organization can identify and contain data breach incidents and the financial consequences. For our consolidated sample of 477 companies, the mean time to identify (MTTI) was 197 days, and the mean time to contain (MTTC) was 69 days. Both the time to identify and the time to contain were highest for malicious and criminal attacks and much lower for data breaches caused by human error. Companies that identified a breach in less than 100 days saved more than $1 million as compared to those that took more than 100 days. Similarly, companies that contained a breach in less than 30 days saved over $1 million as compared to those that took more than 30 days to resolve.

Hackers and criminal insiders cause 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 $157. In contrast, system glitches cost $131 per record and human error or negligence is $128 per record. Companies in the United States and Canada spent the most to resolve a malicious or criminal attack ($258 and $213 per record, respectively). Brazil and India spent far less ($73 and $76 per record, 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 $14 per compromised record. Hence, companies with a strong IR capability could anticipate an adjusted cost of $134, down from $148 per record. Similarly, the extensive use of encryption reduced cost by $13 per capita, for an adjusted average cost of $135, down from $148 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 caused the data breach, the cost increased by more than $13 per compromised record for an adjusted average cost of $161, up from $148 per record. Organizations undergoing a major cloud migration at the time of the breach saw the cost increase to per capita cost by $12, for an adjusted average cost of $160, up from $148 per record.

The loss of customer trust has serious financial consequences.
Organizations that lost less than one percent of their customers due to a data breach resulted in an average total cost of $2.8 million. If four percent or more was lost, the average total cost was $6 million, a difference of $3.2 million.

Part 4. Full Detailed Findings

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

→ Global and industry cost differences 12

→ Root causes 19

→ Factors that influence the cost of a data breach 22

→ Trends in the frequency of compromised records and customer turnover 23

→ Trends in the cost components of a data breach 26

→ Direct and indirect costs 30

→ The likelihood an organization will have another data breach 31

→ The time to identify and contain data breaches impacts costs 33

→ Days to identify and contain the data breach by industry sector 35

→ Security automation impacts costs 37

→ The cost of a mega breach 39

Global and industry cost differences

This year's annual study was conducted in 15 countries or regional samples: the United States (US), United Kingdom (UK), Germany (DE), Canada (CA), France (FR), Italy (IT), Japan (JP), Australia (AU), the Middle East (ME), Brazil (BZ), India (IN), South Africa (SA), ASEAN (AS), and, for the first time, Turkey (TY) and South Korea (SK). In summary, a total of 477 organizations participated. Country or regional findings are presented in separate Power-Point-style reports.

Figure 1 provides a guide to the abbreviation, sample size and currency for each country represented in this global study, in addition to the number of years the country has been a part of our research.

> "We understand why our costs continue to increase. It is part of our culture to have the ability to protect the data of our customers so we invest ample resources in order to resolve our data breaches quickly."
>
> — Compliance Manager/Germany /Consumer Products

Figure 1. Global guide

Legend	Countries	Sample	Pct%	Currency	Years of study
US	United States	65	14%	US Dollar	13
ID	India	43	9%	Rupee	7
UK	United Kingdom	42	9%	GBP	11
BZ	Brazil	37	8%	Real	6
DE	Germany	35	7%	Euro	10
JP	Japan	32	7%	Yen	7
FR	France	31	6%	Euro	9
CA	Canada	28	6%	CA Dollar	4
ME	Middle East*	28	6%	AED/SAR	5
IT	Italy	26	5%	Euro	7
SK	South Korea	25	5%	Won	1
AU	Australia	24	5%	AU Dollar	9
TY	Turkey	21	4%	TRY	1
AS	ASEAN#	20	4%	SGD	2
SA	South Africa	20	4%	ZAR	3
	Total	**477**	**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.

Figure 2 presents the average per capita cost of a data breach in U.S. dollars by country or region. As shown in the figure, there was significant variation among countries. The consolidated average per capita cost for all samples was $148 compared to an average of $141 last year. The United States, Canada and Germany continue to have the highest per capita costs at $233, $202 and $188, respectively. Turkey, India and Brazil have much lower per capita costs at $105, $68 and $67, respectively.

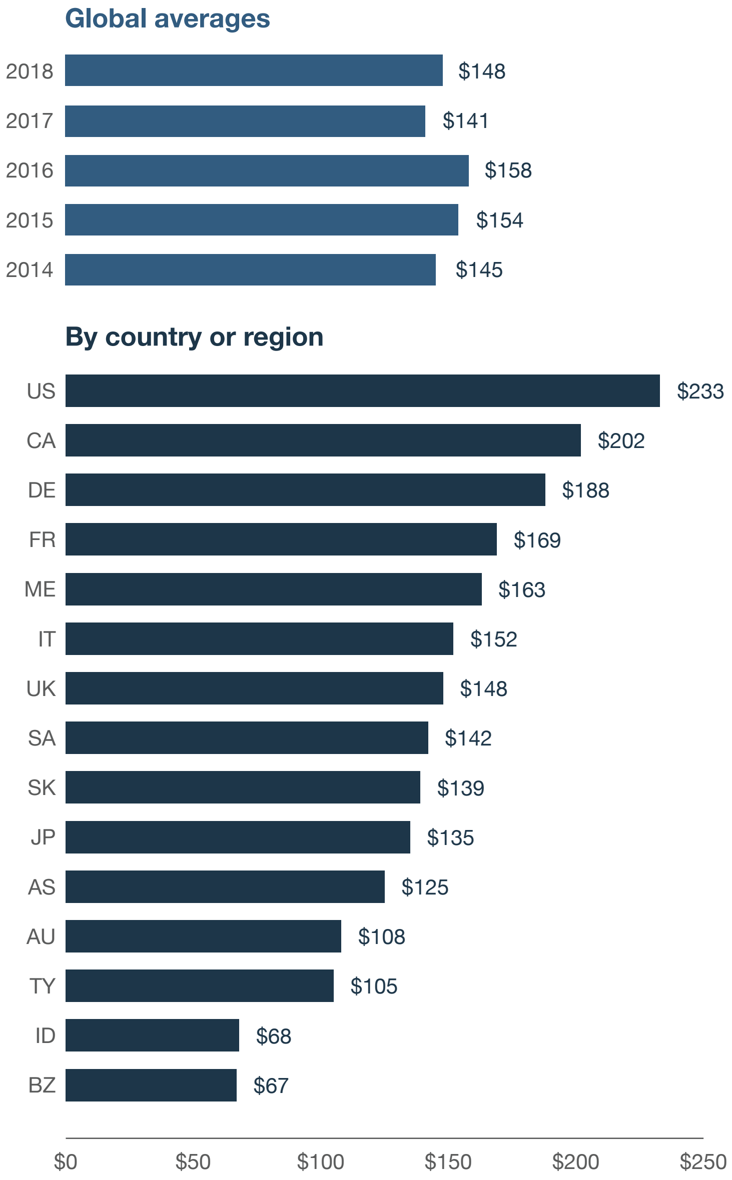
Figure 2. The 2018 per capita cost of data breach by country or region

Measured in US$

The consolidated average per capita cost for all samples was $148 compared to an average of $141 last year.

The United States, Canada, and Germany continue to have the highest per capita costs at $233, $202, and $188, respectively.

Turkey, India, and Brazil have much lower per capita costs at $105, $68, and $67, respectively.

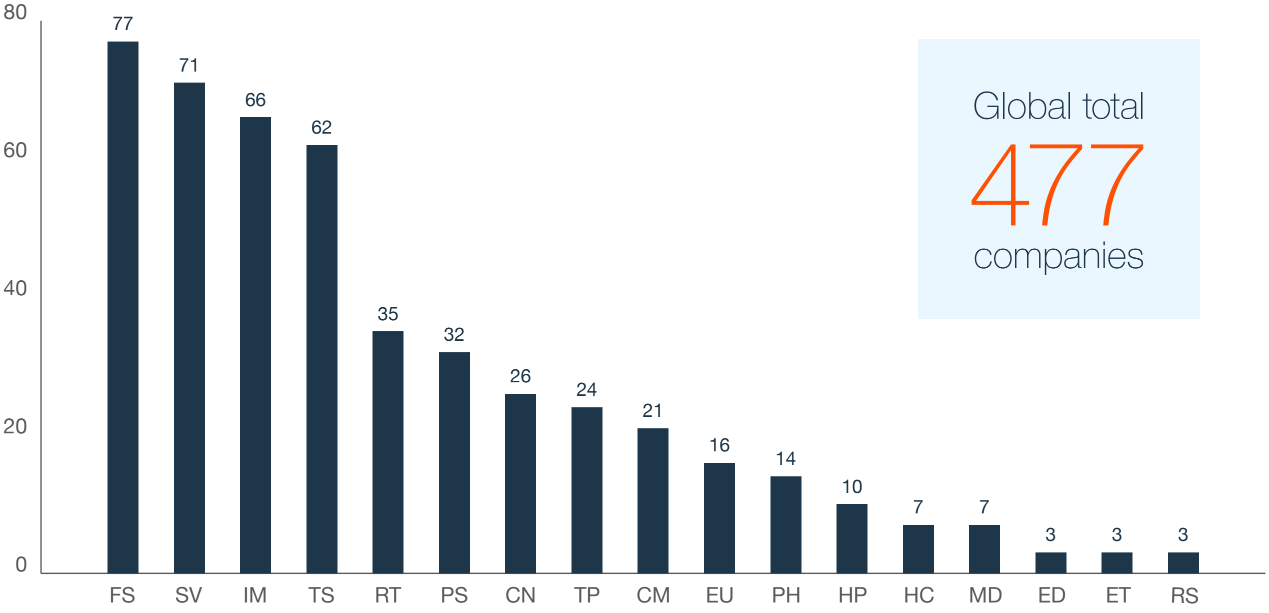


[7] Per capita cost is defined as the total cost of data breach divided by the size of the data breach (i.e., the number of lost or stolen records).

Figure 3 presents the frequency of data breaches by industry. Industries represented include:

- > FS — Financial Services
- > SV — Services
- > IM — Industrial Manufacturing
- > TS — Technology
- > RT — Retail
- > PS — Public Sector
- > CN — Consumer
- > TP — Transportation
- > CM — Communications
- > EU — Energy
- > PH — Pharmaceuticals
- > HP — Hospitality
- > HC — Healthcare
- > MD — Media
- > ED — Education
- > ET — Entertainment
- > RS — Research

Figure 3. Frequency of benchmark samples by industry



The average organizational cost of a data breach varies by country. Figure 4 shows this year's average total cost of a data breach by country. Organizations in the United States had the highest total average cost at $7.91 million, followed by the Middle East at $5.31 million. In contrast, Indian and Brazilian organizations had the lowest total average cost at $1.77 million and $1.24 million, respectively.

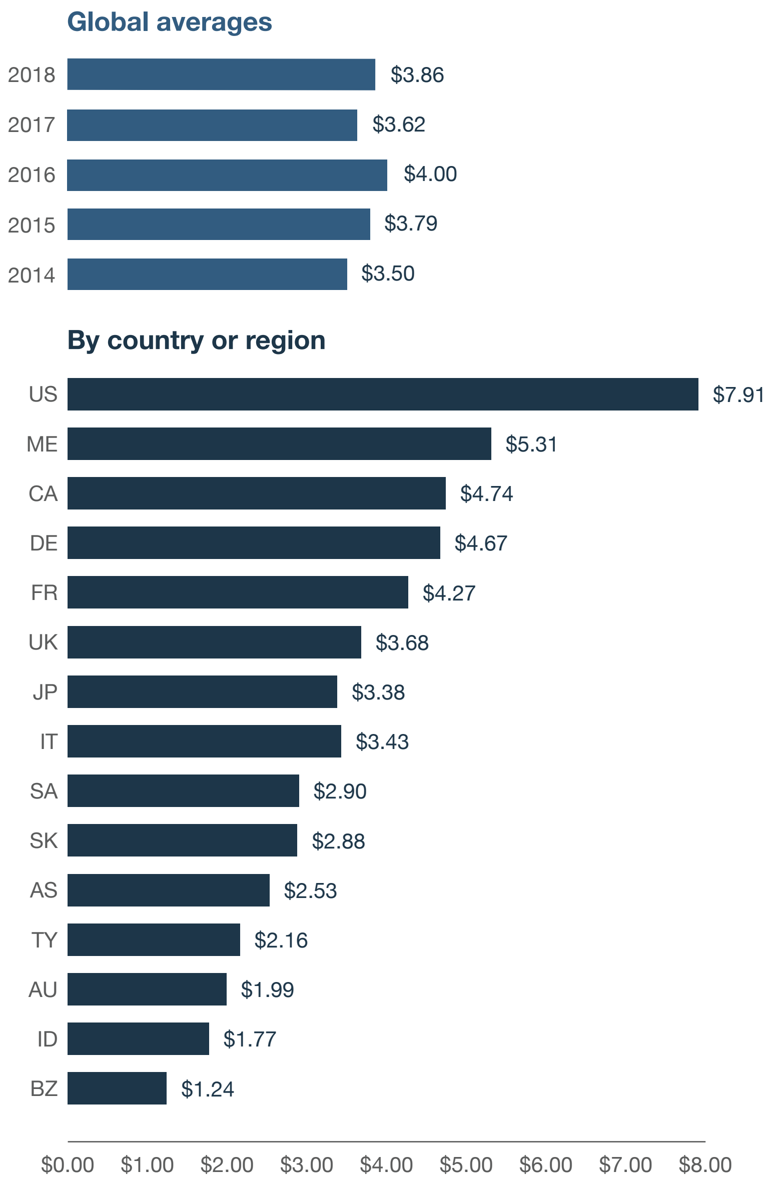
Figure 4. The average total cost of a data breach by country or region

Measured in US$ millions

The average total cost for all samples was $3.86 million compared to an average of $3.62 million last year.

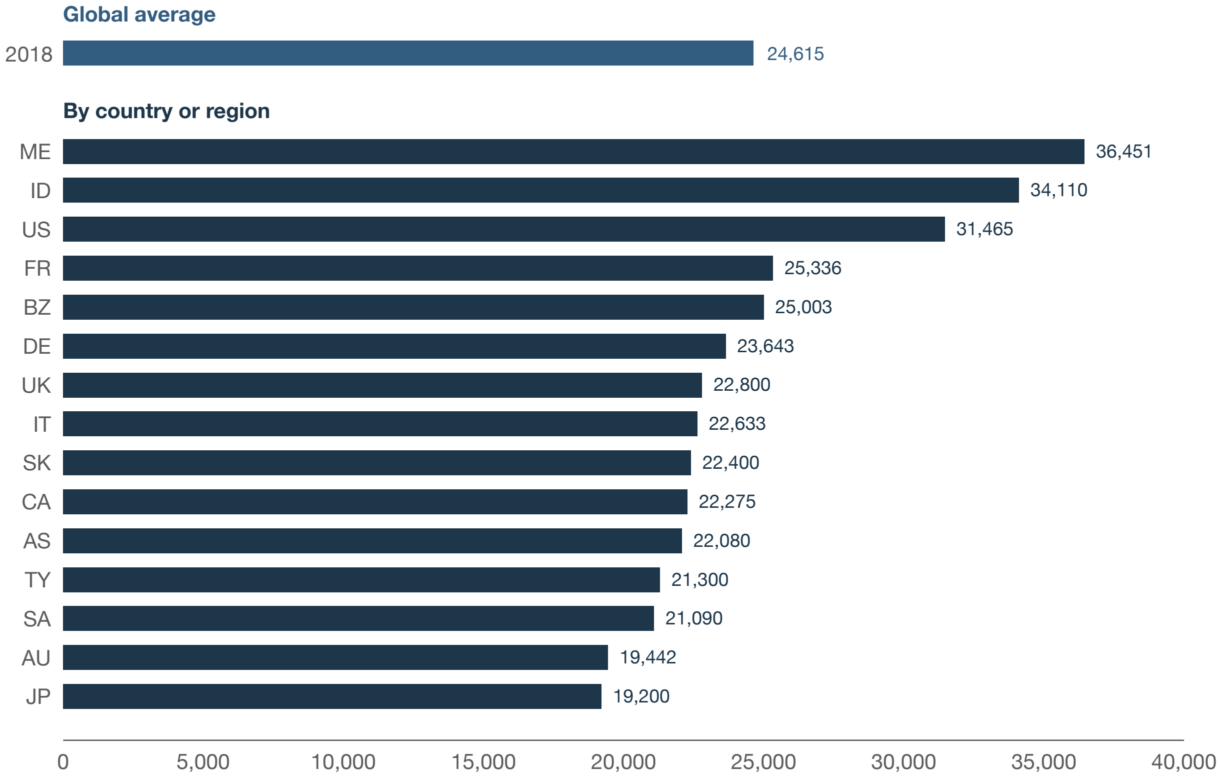
Organizations in the United States had the highest total average cost at $7.91 million, followed by the Middle East at $5.31 million.

Indian and Brazilian organizations had the lowest total average cost at $1.77 million and $1.24 million, respectively.



Number of exposed or compromised records by country or region. Figure 5 reports the average size of data breaches for organizations in the countries and regions represented in this research. The average size of a data breach increased by 2.2 percent. Organizations in the Middle East, India, and the United States had the largest average number of breached records. Japan, Australia, and South Africa had the smallest average number of breached records.

Figure 5. The average number of breached records by country or region



Net change in the cost of a data breach for each country[8]**.** Figure 6 presents the percentage change in four metrics over the past year[9]. These metrics are:

> **abnormal churn**
(the greater than expected loss of customers since the breach occurred),

> **size of data breach**
(the number of records lost or stolen),

> **average total cost of a data breach** and

> **the per capita cost.**

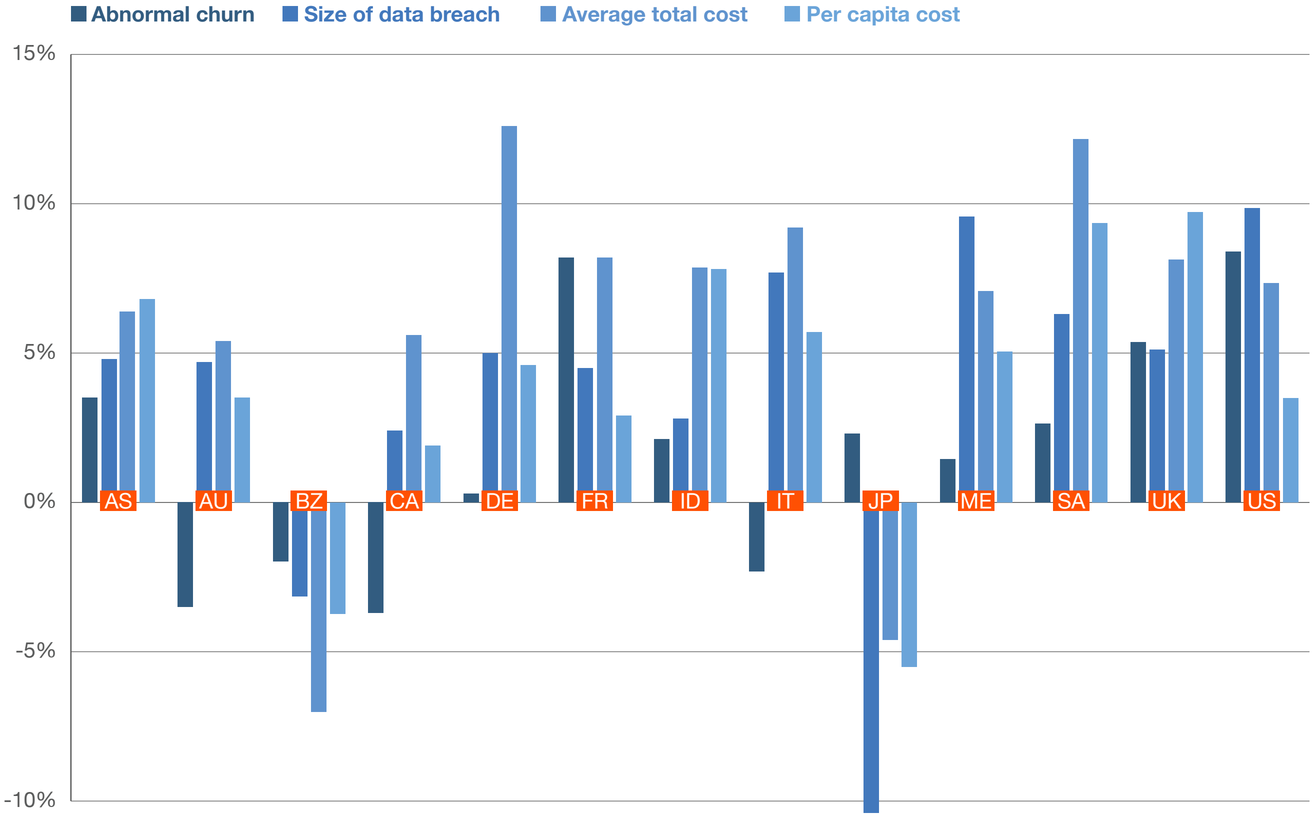
> "Our average total cost has increased but we don't look at these increases as necessarily bad. We are investing in the protection of data for the long term because we know data breaches are not going away."
>
> — IT Supervisor/South Africa/Industrial

Following are the increases and decreases in these metrics for each country.

As shown, only three countries experienced a net decrease in this year's study. Specifically, Japanese companies experienced a decrease in per capita cost, average total cost and size of the data breach. Brazil realized a decrease in all four metrics, and Australia experienced a decrease in churn rate.

Figure 6. Percentage change in data breach measures over the past year

Net change defined as the difference between the 2018 and 2017 results



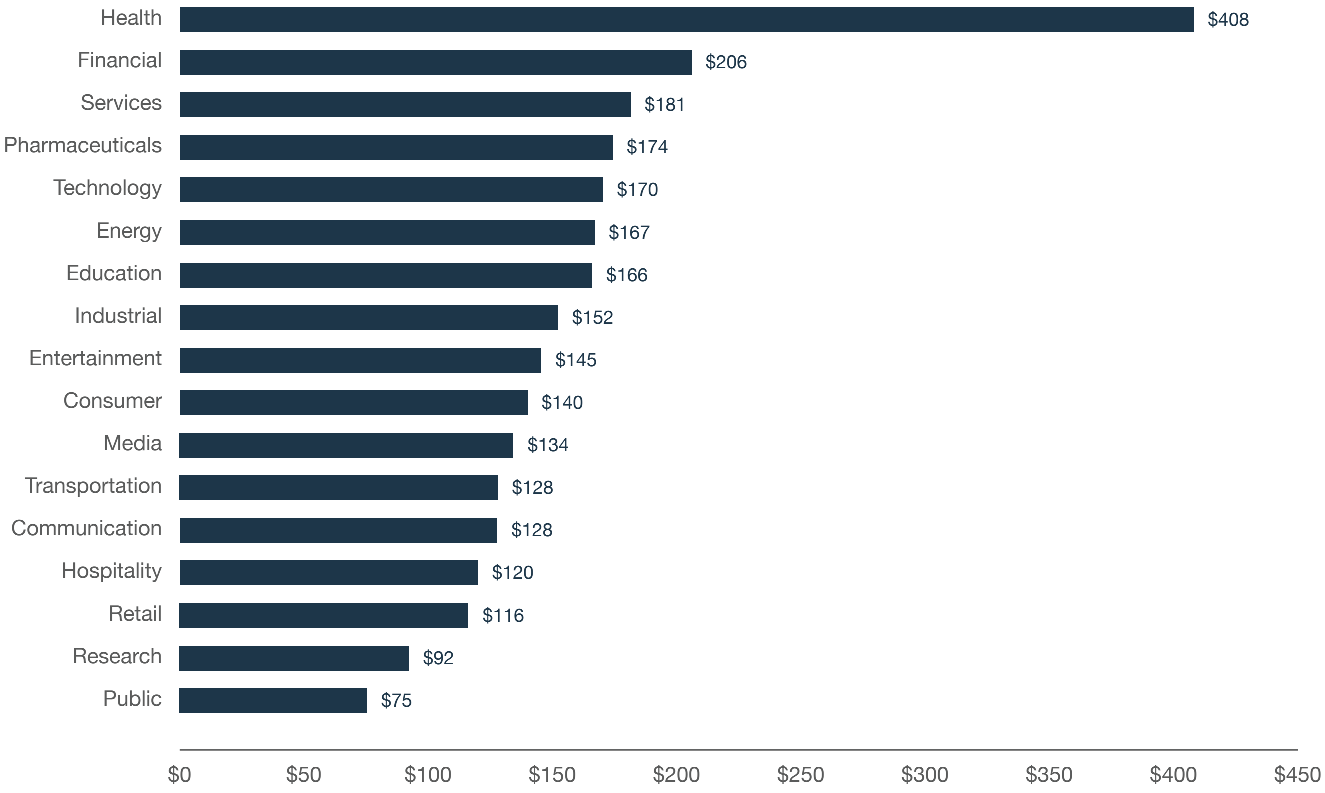
[8] Turkey and South Korea are not included in this analysis because this is the first year these countries are included.

[9] The percentage change shown in Figure 5 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 7 compares this year's per capita costs for the consolidated sample by industry classification. As can be seen, heavily regulated industries such as healthcare and financial organizations have a per capita data breach cost substantially higher than the overall mean. Public sector, research, media and transportation organizations have a per capita cost well under the overall mean value.

Figure 7. Per capita cost by industry sector

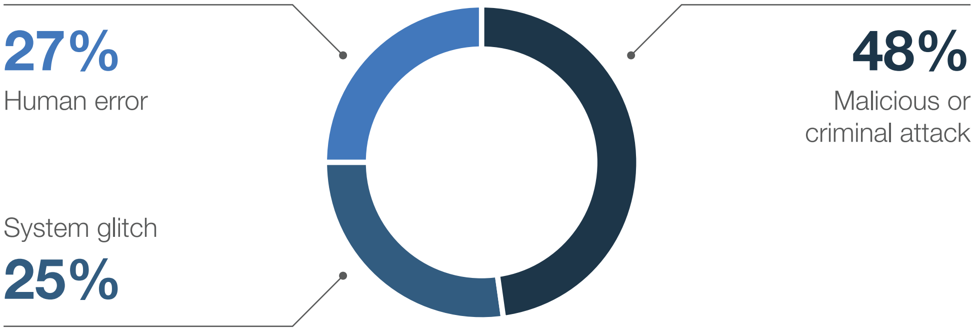
Measured in US$



Root causes

Malicious or criminal attacks cause the most data breaches[10]. Figure 8 provides a summary of the main root causes of data breaches on a consolidated basis for organizations in all countries. 48 percent of incidents involved a malicious or criminal attack, 27 percent were due to negligent employees or contractors (human factor) and 25 percent involved system glitches, including both IT and business process failures[11].

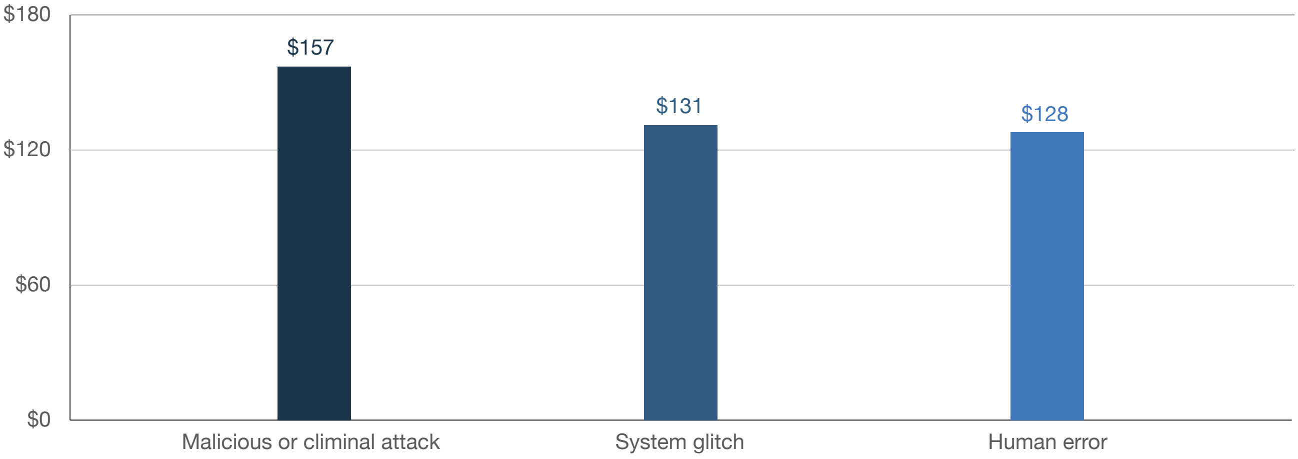
Figure 8. Distribution of the benchmark sample by root cause of the data breach



Malicious or criminal attacks are the costliest. Figure 9 reports the per capita cost of a data breach for three root causes. In 2018, the cost of data breaches due to malicious or criminal attacks was $157. This is significantly higher than the per capita cost for breaches caused by system glitches and human factors, which were $131 and $128, respectively.

Figure 9. Per capita cost for three root causes of the data breach

Measured in US$



[10] 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).

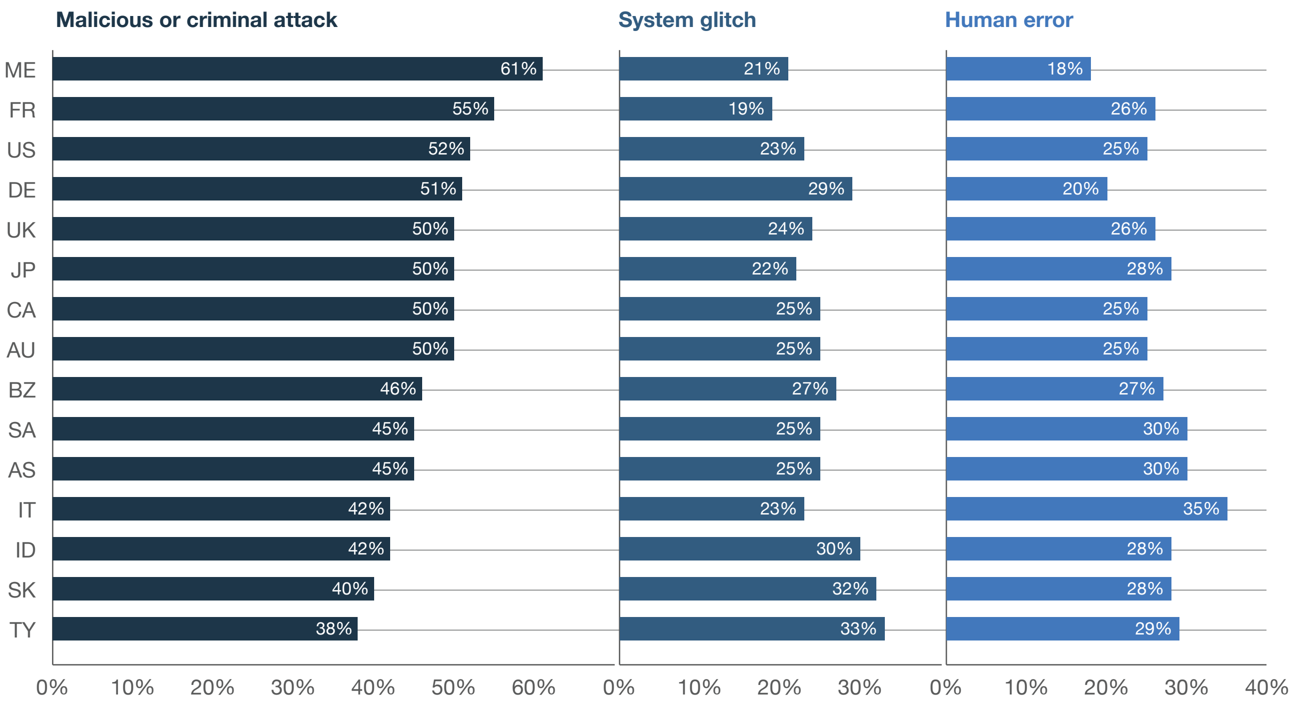
[11] The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Root cause by country or region. Figure 10 presents the main root causes of a data breach for all country or regional samples. Organizations in the Middle East region are most likely to experience a malicious or criminal attack (61 percent). Companies operating in this part of the world have fewer regulations, which may influence their security posture. In addition, criminals perceive these companies to have high-value information assets and IT infrastructures that are more vulnerable to attacks.

> "We are struggling to address global regulations and we are lagging in having the most current technology. It is very hard to get our managers to make investments we so badly need."
>
> — Data Security Analyst/Turkey/Services

In contrast, organizations in Turkey, South Korea and India were the least likely to experience criminally motivated data breaches. Italian companies had the highest percentage of human error (non-criminal) data breaches and Turkish organizations were the most likely to experience a data breach due to a system glitch or business process failure.

Figure 10. Percentage of data breach root causes per country or region

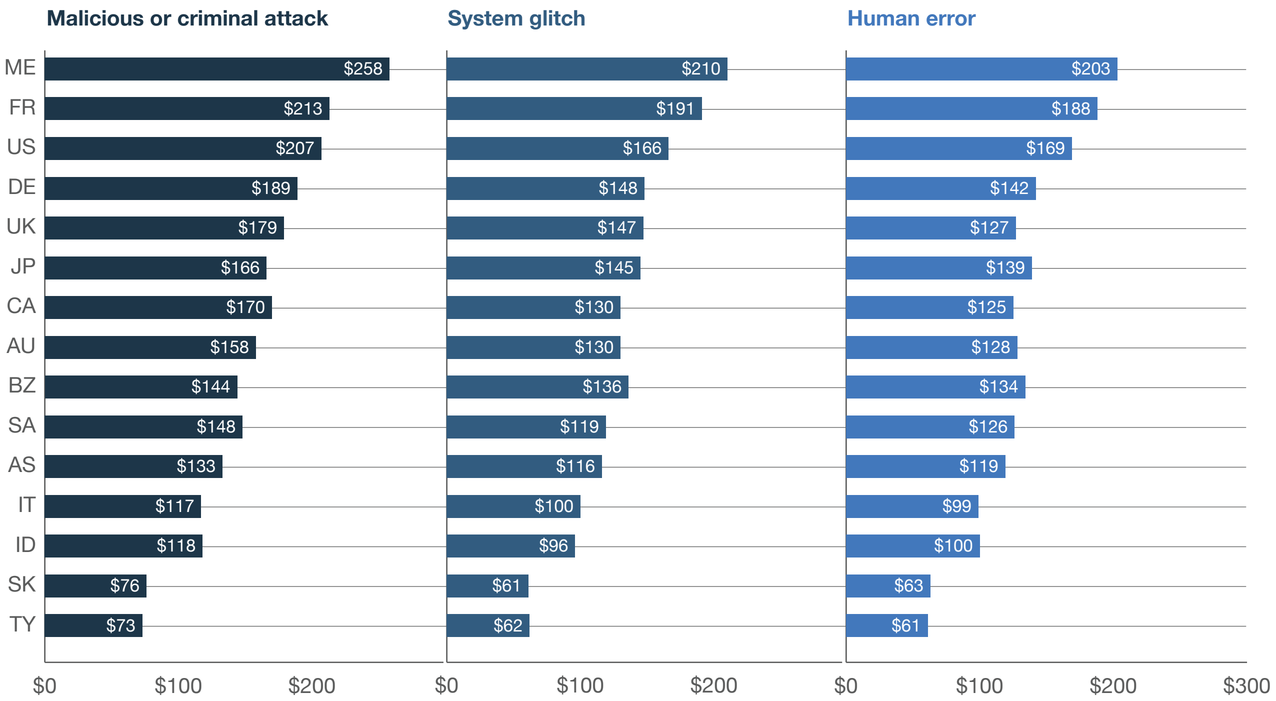


The per capita cost for root causes by country or region. Figure 11 reports the per capita cost of a data breach for three root causes. These results clearly show data breach costs resulting from malicious or criminal attacks were consistently higher than costs resulting from system glitches or human error. These attacks are harder to detect with precise knowledge than data breaches resulting from employee carelessness. Even after detection, findings show malicious or criminal attacks take longer to contain and remediate.

There was also wide variation among the countries. In the United States, the cost of a malicious or criminal data breach incident was $258 per compromised record, whereas, in Brazil the per capita cost of a criminally motivated data breach was only $73.

Figure 11. Per capita cost for three root causes of a data breach by country or region

Measured in US$

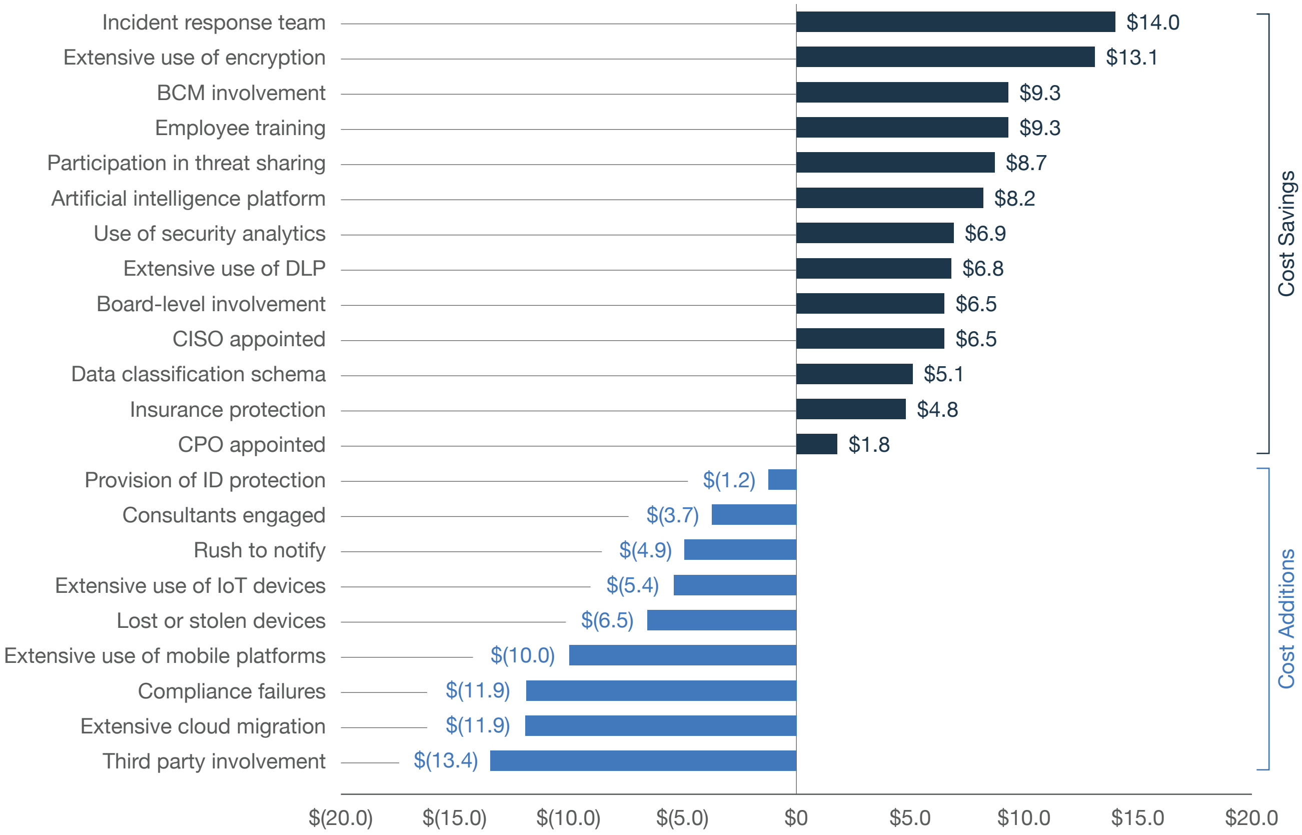


Factors that influence the cost of a data breach

Certain factors decrease or increase the cost of a data breach. Figure 12 provides a list of 22 factors that increase or decrease the per capita cost of a data breach.

Figure 12. Impact of 22 factors on the per capita cost of data breach

Measured in US$



Incident response teams and the extensive use of encryption result in the greatest decrease in the per capita cost. In this year's research, an incident response (IR) team reduced the cost by as much as $14 per compromised record. While the average cost per record is $148, companies with a strong IR team can anticipate an adjusted cost of $134 per record. Similarly, the extensive use of encryption reduced cost by $13 per capita, with an adjusted cost of $135.

Third party involvement in a breach and extensive cloud migration at the time of the breach increase the cost. If a third party caused the breach, the cost increased by more than $13 per compromised record with an adjusted average cost of $161 per record. Organizations undergoing a major cloud migration at the time of the breach saw this increase to per capita cost by $12, with an adjusted average cost of $160 per record. An extensive cloud migration is one that consumes a significant amount of corporate IT resources. It is also senior management's priority because of the expectation the cloud will reduce costs.

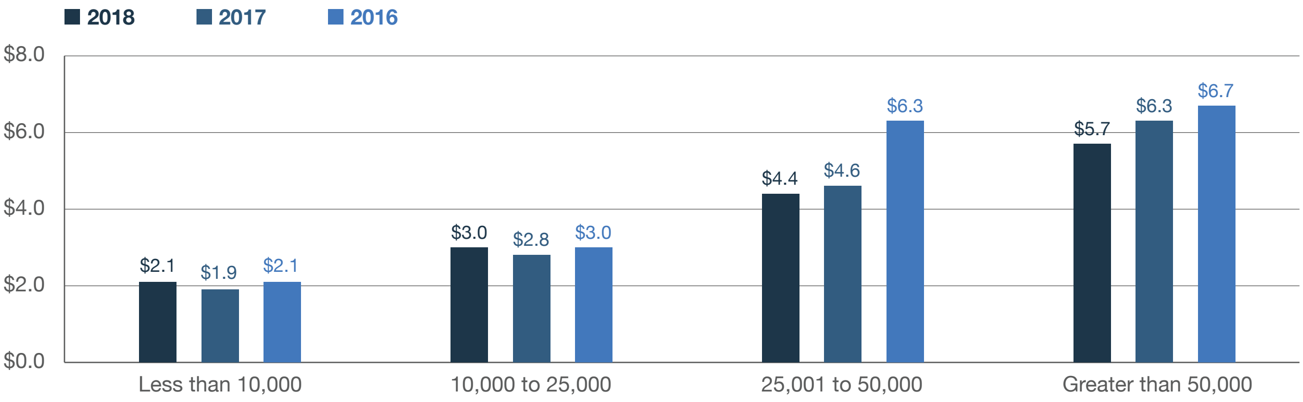
Two new factors are included in this year's cost analysis. The following factors influence data breach costs: (1) deployment of an artificial intelligence platform as part of a security automation solution and (2) the extensive use of Internet of Things (IoT) devices. The deployment of an AI platform saved $8 per compromised record, while the extensive use of IoT devices increased cost by $5 per compromised record.

Trends in the frequency of compromised records and customer turnover

The more records lost, the higher the cost of the data breach. Figure 13 shows the relationship between the average total cost of a data breach and incident size for 477 organizations according to the size of a data breach incident. In this year's study, the cost ranged from $2.1 million for incidents with less than 10,000 compromised records to $5.7 million for incidents with more than 50,000 compromised records. Each year, the findings show a consistent relationship between cost and size of the data breach.

Figure 13. Average total cost by size of the data breach

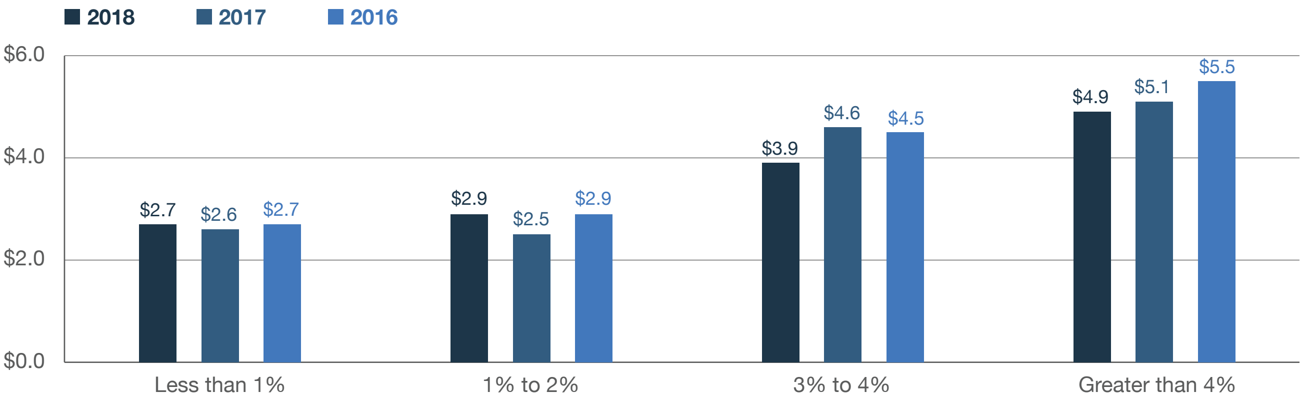
Measured in US$ millions



The more customers lost following the breach, the higher the average total cost of a data breach. Figure 14 reports the average total cost of a data breach for four abnormal churn rates from less than 1 percent to more than 4 percent. Companies that experienced less than a 1 percent loss of existing customers had an average total cost of $2.7 million. We estimate an average cost of $4.9 million for companies experiencing a churn rate greater than 4 percent.

Figure 14. Average total cost by abnormal churn rate

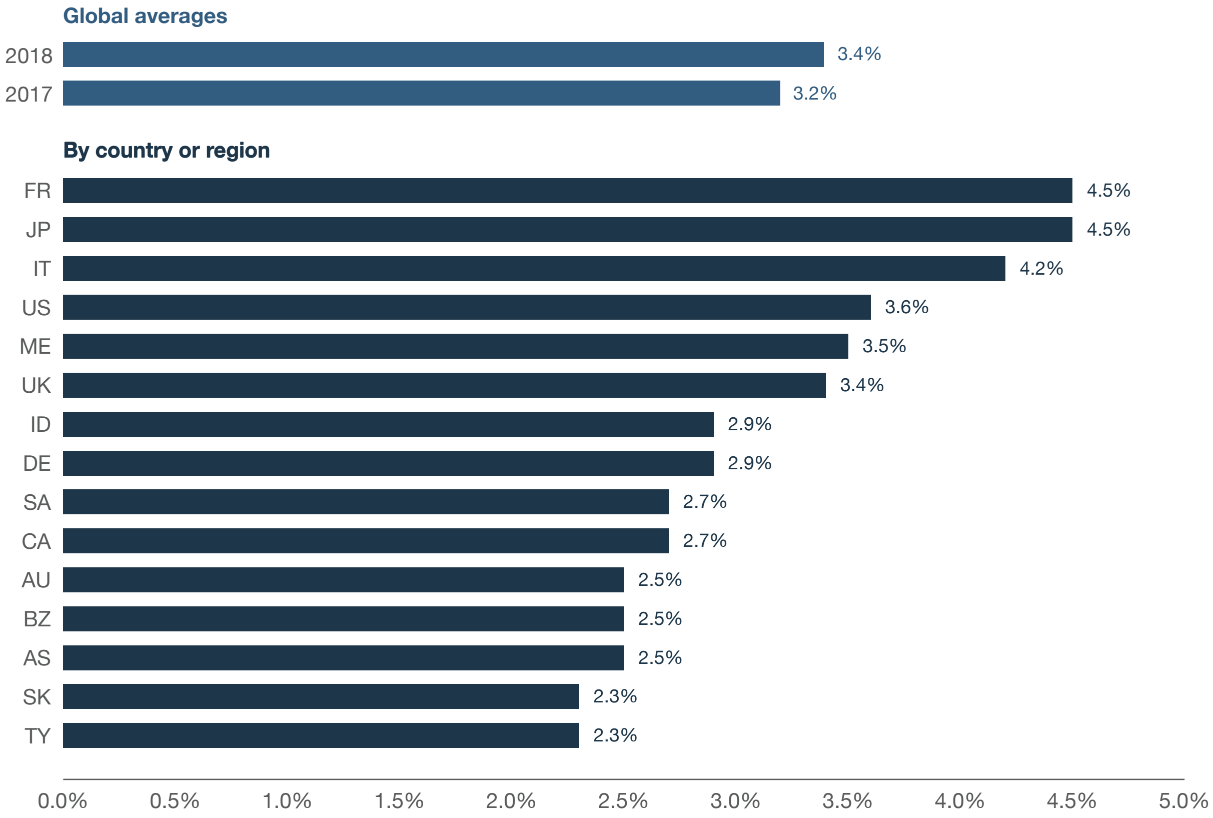
Measured in US$ millions



Certain countries are more vulnerable to churn. Figure 15 reports the average abnormal churn rates for all country or regional samples represented in this research. Results show marked differences among countries.

France, Japan, and Italy experienced the highest abnormal churn rate, whereas, Turkey, South Korea, and Australia had the lowest abnormal churn rates. The global average churn rate for our combined sample of 477 companies was 3.40 percent. Last year's average churn rate was 3.24 percent. Thus, organizations in countries with high churn rates can significantly reduce the costs of a data breach by emphasizing customer retention activities to preserve reputation and brand value.

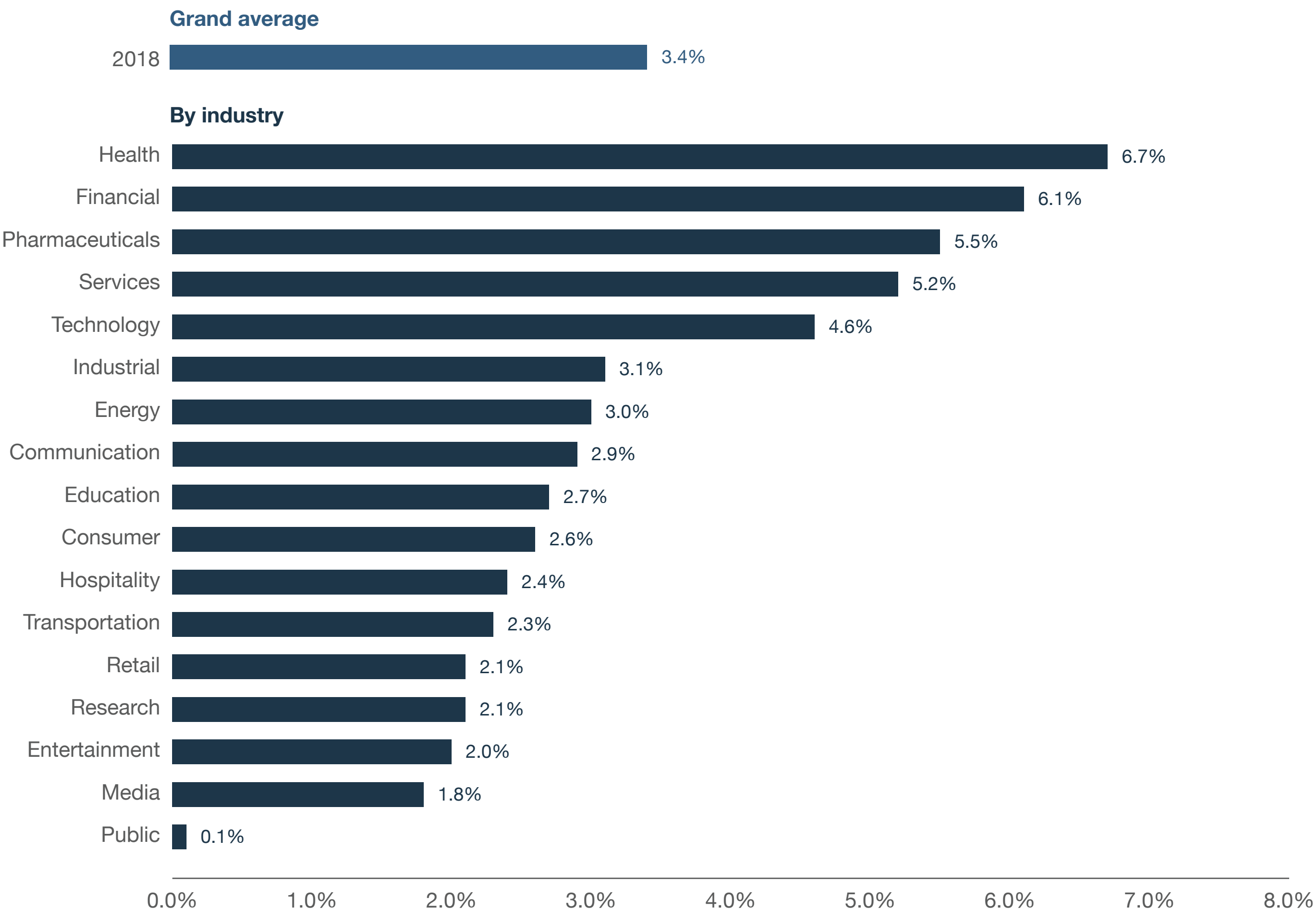
Figure 15. Abnormal churn rates by country sample



Certain industries are more vulnerable to churn. Figure 16 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, health, financial, pharmaceutical, and service organizations experienced relatively high abnormal churn. In contrast, public sector, media, and entertainment organizations experienced a relatively low abnormal churn[12].

Companies in certain industries are more vulnerable to churn when customers can easily take their business to another competitor. Customers also have high expectations for the protection of their data in highly regulated industries, such as healthcare and financial services. When these organizations have a data breach, customers' trust will decline and they will try to find a substitute. In contrast, the public sector, which has the lowest churn, has no competitor and customers have no other options.

Figure 16. Abnormal churn rates by industry



[12] 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

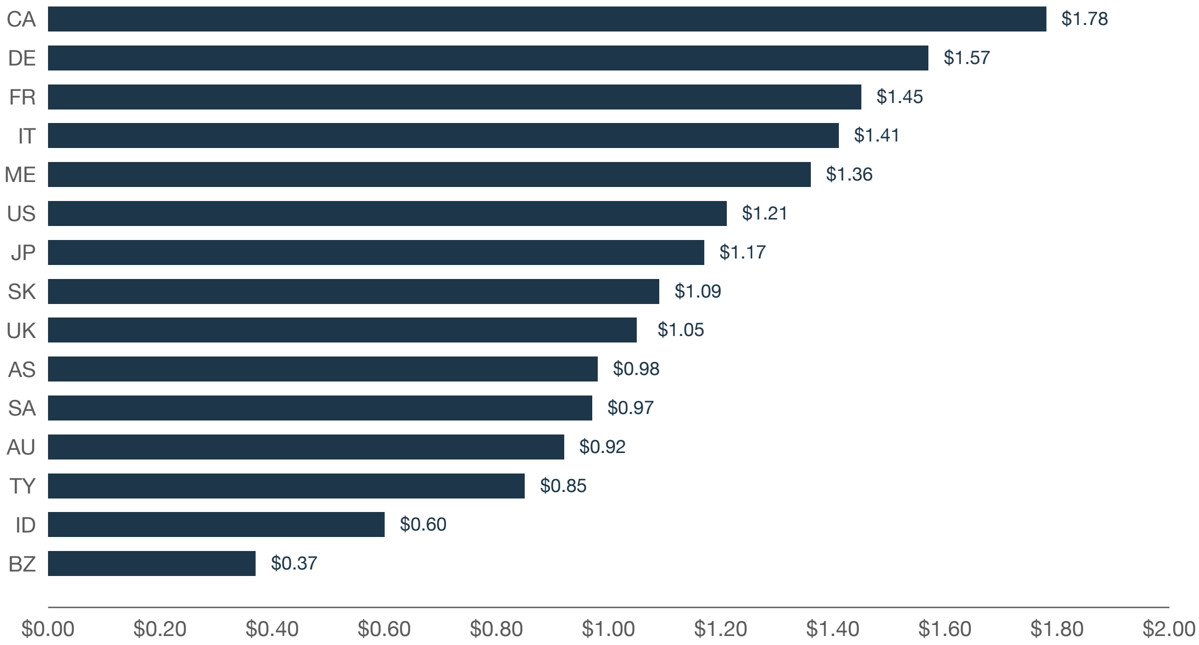
Detection and escalation costs are highest in Canada and lowest in Brazil. Detection and escalation costs include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors.

As shown in Figure 17, the average detection and escalation cost for Canada was $1.78 million. In contrast, the average cost for Brazil was only $0.37 million.

> "We take pride in our privacy practices and are particularly sensitive to making sure our data breaches affect as few customers as possible. We are investing in forensic analysis and cyber analytics. While the costs are increasing today, we think it will help us reduce the cost of data breaches in the future."
>
> — SVP/Canada/Transportation

Figure 17. Detection and escalation costs

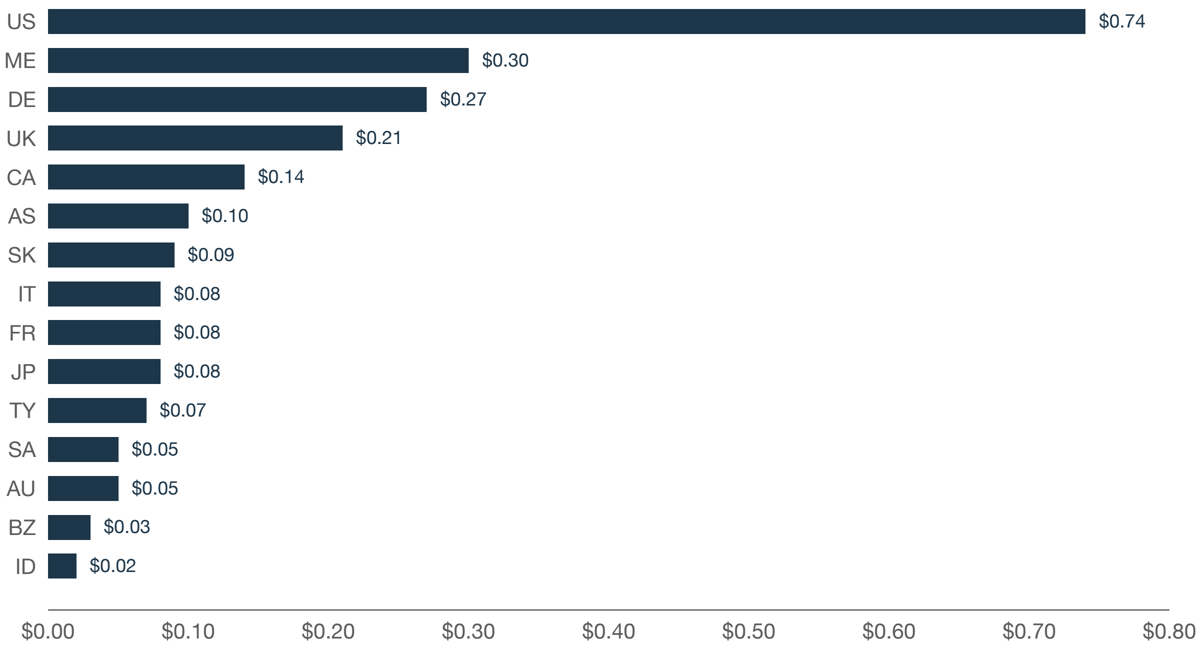
Measured in US$ millions



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. As shown in Figure 18, by far, notification costs for US organizations were the highest at $740,000, whereas they were the lowest for India at $20,000, as shown in Figure 16. US notification costs are higher because of data breach notification regulations. We anticipate that in the future GDPR will result in huge increases throughout the world in notification costs.

Figure 18. Notification costs

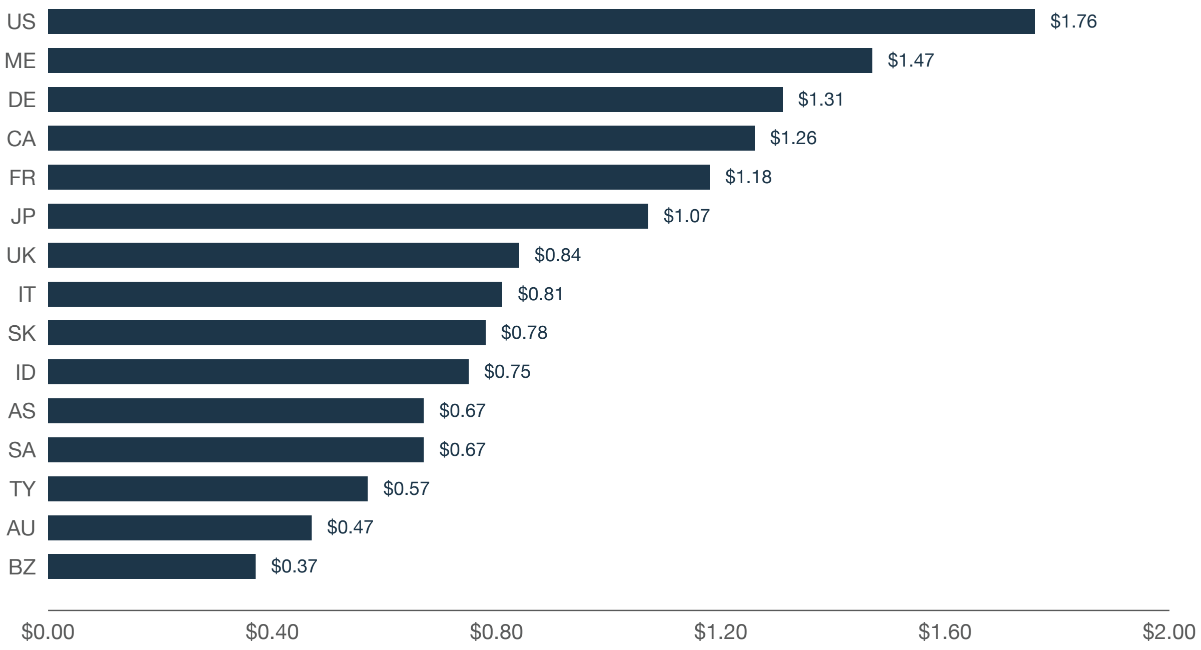
Measured in US$ millions



Post data breach response costs are highest in the US and the Middle East. The costs associated with post data breach response in the United States were $1.76 million and $1.47 million in the Middle East, as shown in Figure 19. Post data breach costs include help desk activities, inbound communications, legal expenditures, product discounts, reestablishing a new account or credit card, and regulatory interventions. The US and Middle East have higher costs because of their investments in activities designed to resolve the data breach as efficiently as possible with minimal loss of customers.

Figure 19. Post data breach response costs

Measured in US$ millions

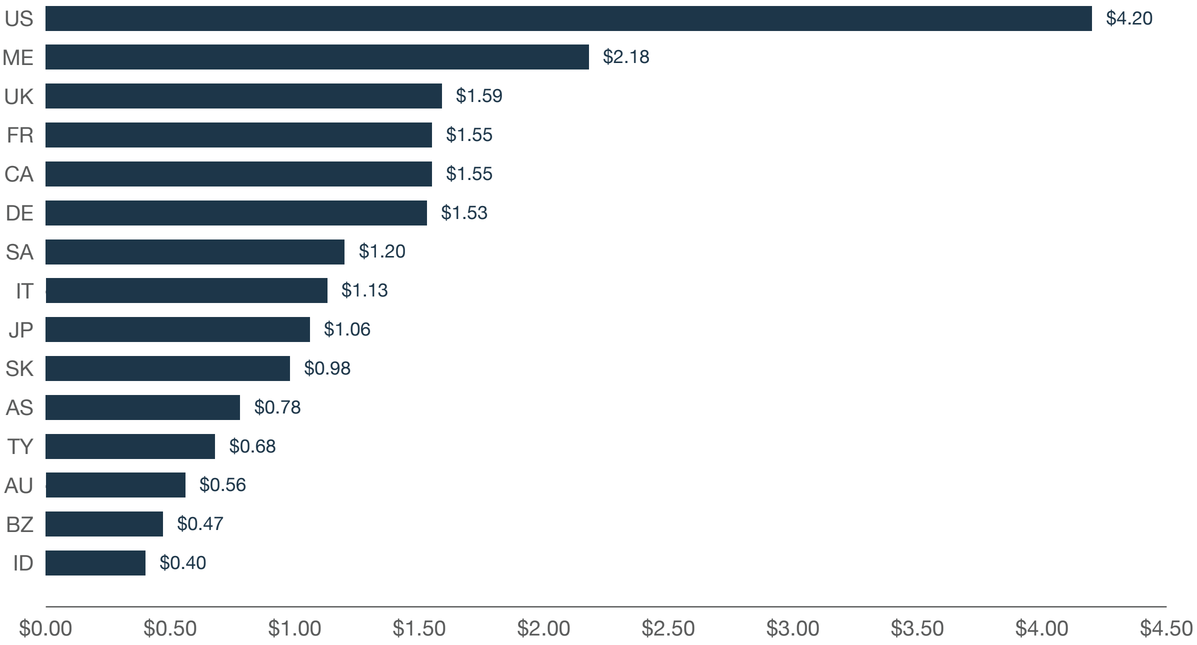


US organizations pay the highest price for losing customers after a data breach. According to Figure 20, the cost of lost business was particularly high for US organizations ($4.20 million). This cost component includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses, and diminished goodwill[13].

US companies have higher costs because customers have more options and their loyalty is harder to preserve. With current notification laws, customers have greater awareness of data breaches and have higher expectations regarding how companies should help them following the breach.

Figure 20. Lost business costs

Measured in US$ millions



[13] Goodwill is an accounting term used to describe the excess value of an organization above its financial assets.

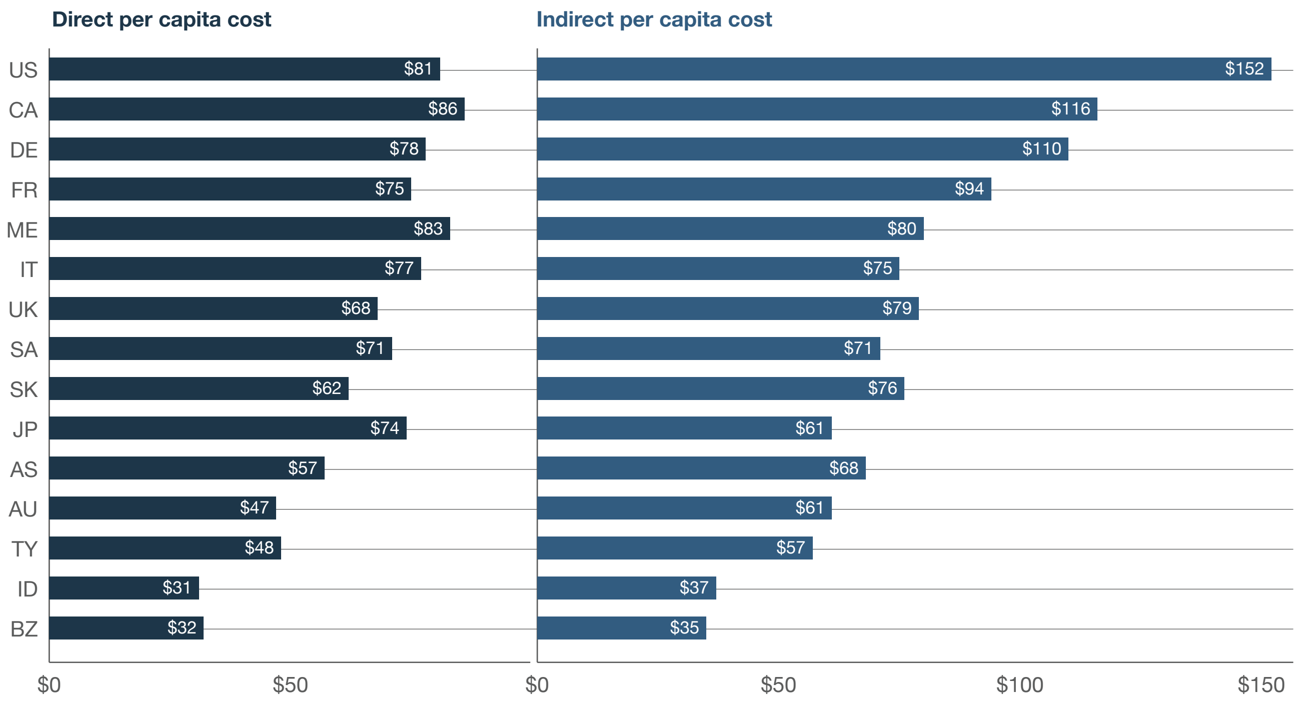
Direct and indirect costs

Organizations in the Middle East and Canada have the highest direct costs and US 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 21, the US had the highest indirect per capita cost at $152 and Canada had the highest direct per capita cost at $86.

Figure 21. Direct and indirect per capita data breach costs

Measured in US$

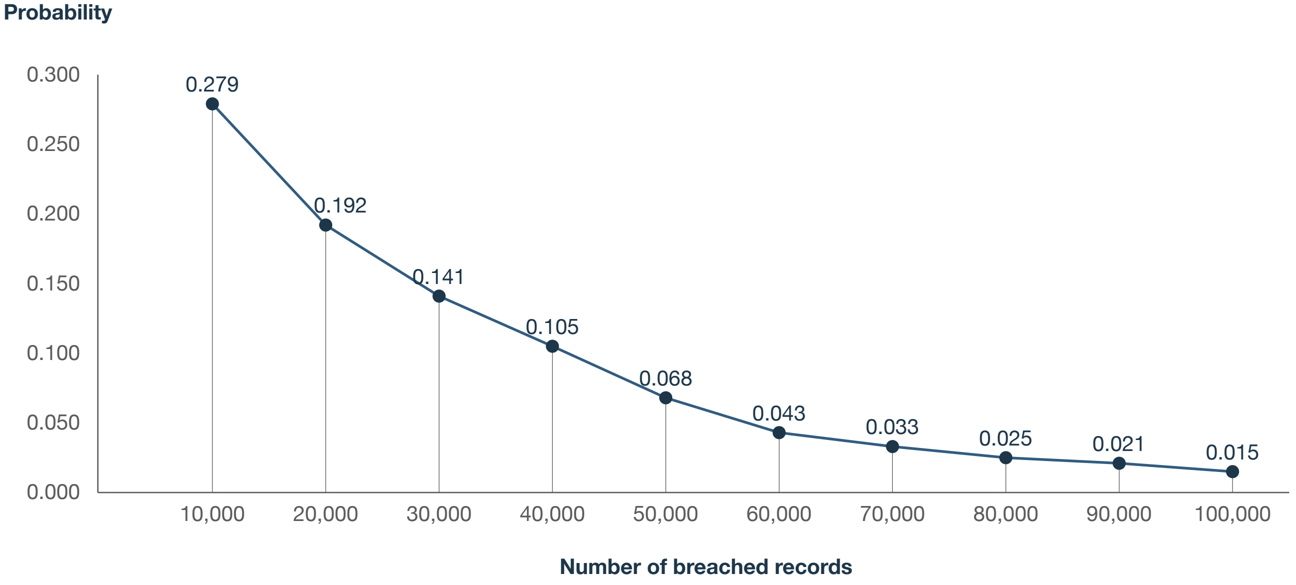


The likelihood an organization will have another data breach

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 were lost or stolen and the country or regional location of the breach incident. As shown in this research, companies in certain locations are more vulnerable to a data breach.

Figure 22 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[14]. As can be seen, the likelihood of a 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 27.9 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 22. Probability of a data breach involving 10,000 to 100,000 records



[14] 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 477 participating companies.

Organizations in South Africa, India and Brazil are more likely to have another data breach. Figure 23 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.

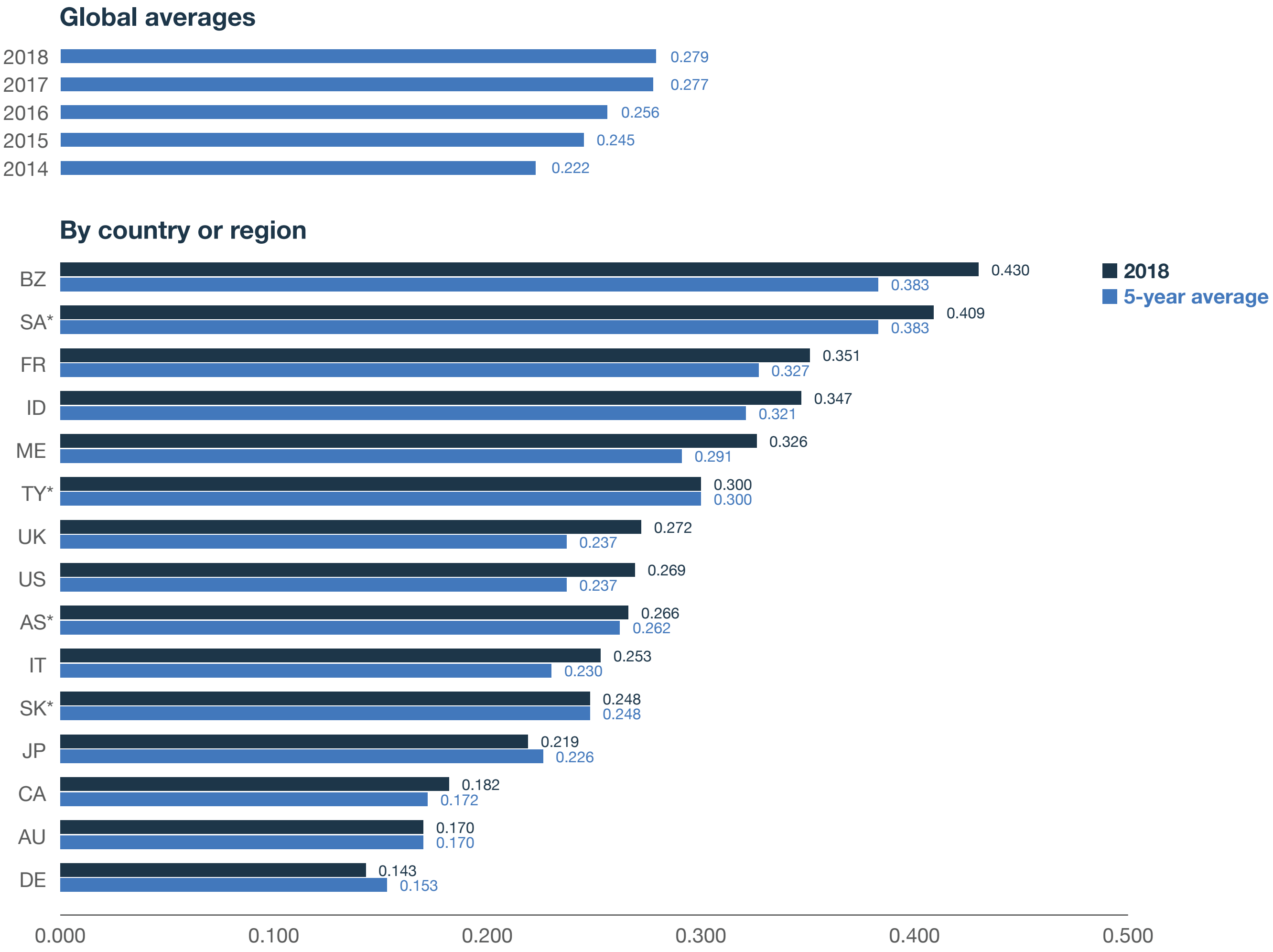
Brazil, South Africa, and France appear to have the highest estimated probabilities of a data breach at 43.0 percent, 40.9 percent, and 35.1 percent, respectively. Germany and Australia have the lowest probability of data breach at 14.3 percent and 17.0 percent, respectively.

It is interesting to note that 9 of 13 countries showed an increase in the probability of data breach because of past data breach experience and location. 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.

> "We worry that our company will be targeted because we are part of an economy that is growing at a very fast pace in an unregulated environment. Companies are underestimating the threats against their data."
>
> — Director of Information Security/India/Technology

Figure 23. The 2018 probabilities of a data breach compared to five-year averages

A minimum of 10,000 compromised records



Global averages

By country or region

* Historical data are not available in all years.

The time to identify and contain data breaches impacts 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 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 24, since last year, the MTTI and MTTC of a data breach increased. In this year's study, for our consolidated sample of 477 companies, the MTTI was 197 days. The MTTC was 69 days. Last year's MTTI and MTTC were 191 and 66 days, respectively. The stealth of recent attacks increases the time it takes to identify and contain these types of data breaches.

Figure 24. Days to identify and contain the data breach over the past year

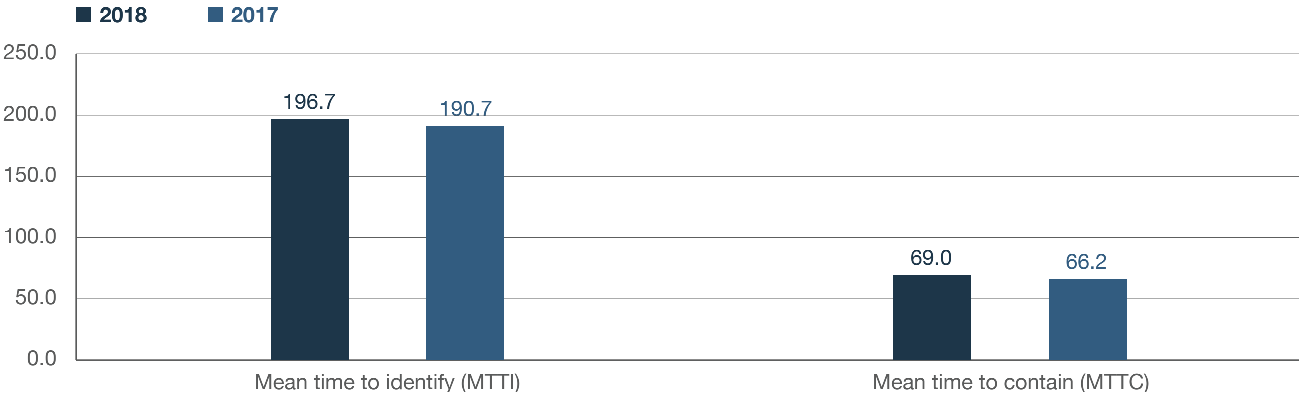
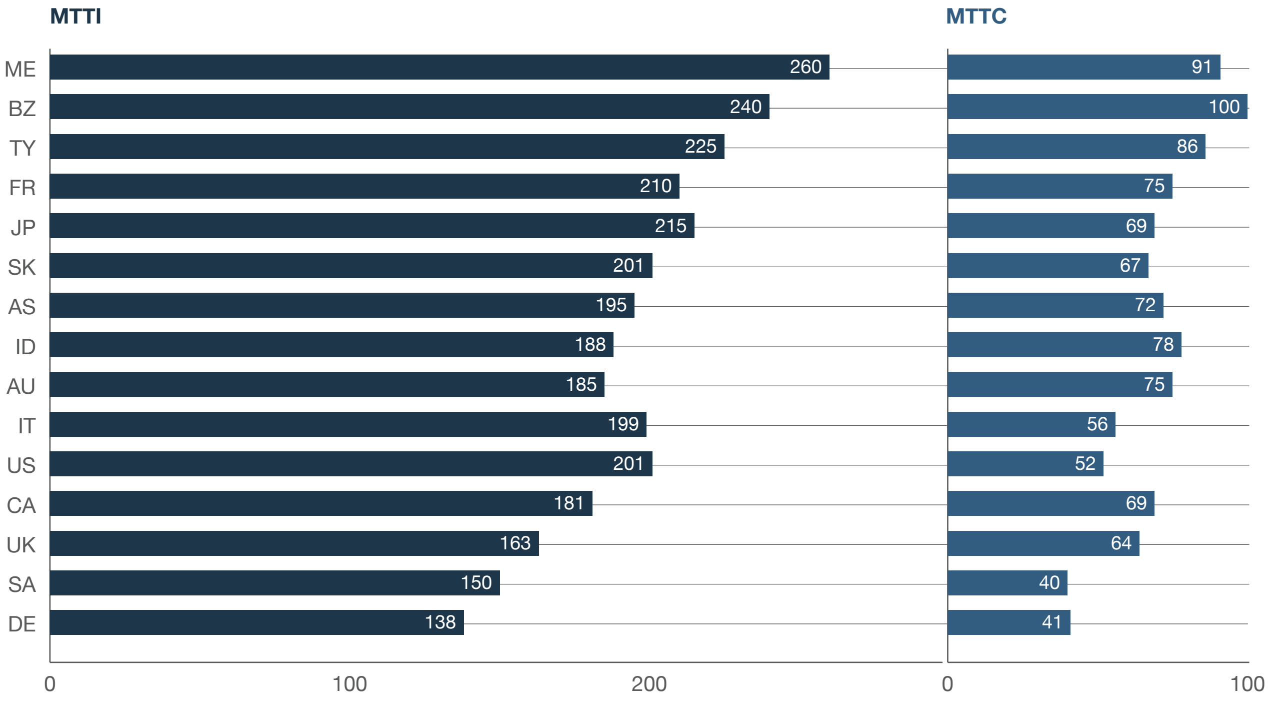


Figure 25 reports the MTTI and MTTC for each country or regional sample. As can be seen, Brazil has the highest days to contain and the Middle East has the highest days to identify. In contrast, Germany has both the lowest days to identify and South Africa reports the shortest time to contain and the second shortest time to identify a data breach.

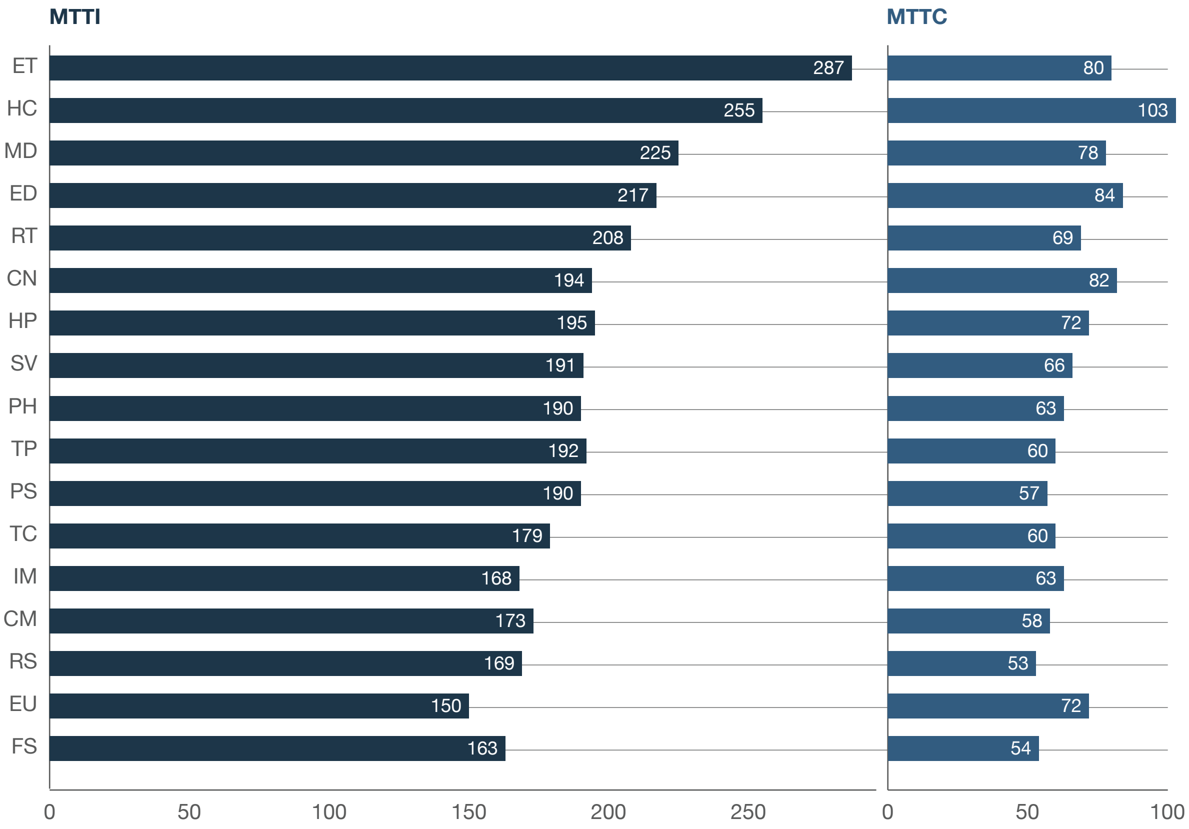
Figure 25. Days to identify and contain the data breach by country or regional sample



Days to identify and contain the data breach by industry sector

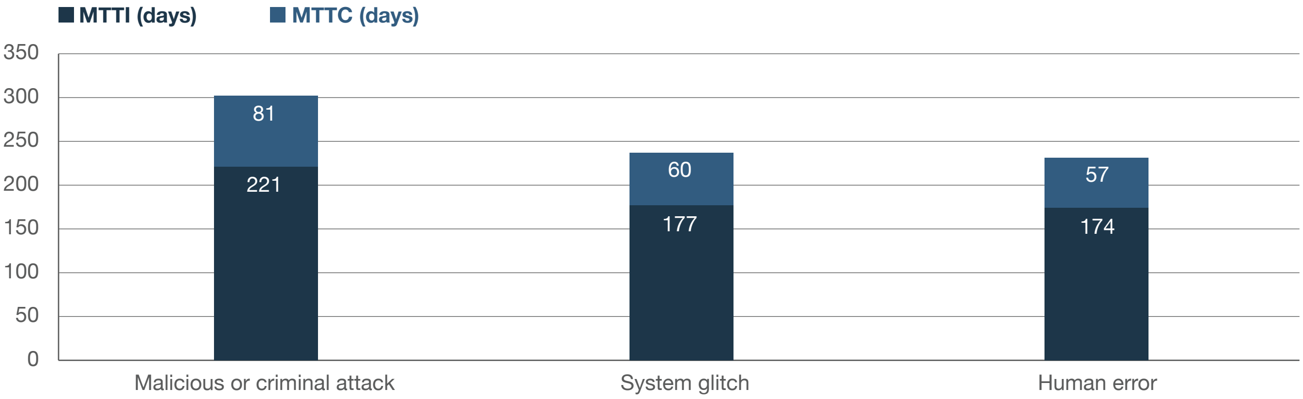
Figure 26 reports the MTTI and MTTC by industry sector. As can be seen, companies in the entertainment industry have the highest days to identify at 287 days, while healthcare companies have the highest days to contain at 103 days. In contrast, companies in research at 150 days and financial services at 163 days have the lowest days to identify. And, with respect to containment, research, financial services, and energy & utilities have the lowest number of days at 53, 54, and 72 days, respectively.

Figure 26. Days to identify and contain the data breach by industry sector



Malicious or criminal attacks take longer to identify and detect. Figure 27 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 (221 and 81 days, respectively). They are much lower for data breaches caused by human error (174 and 57 days, respectively).

Figure 27. Days to identify and contain data breach incidents by root cause

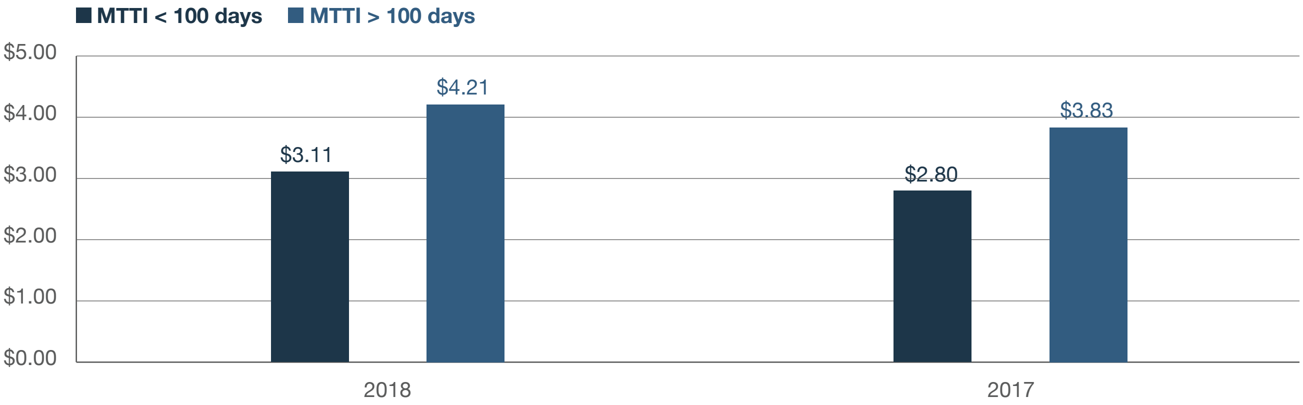


The failure to quickly identify the data breach increases costs. Figure 28 shows a relationship between total data breach costs and breach identification for 477 companies. We bifurcated the consolidated sample according to those with an MTTI below 100 days and those with an MTTI above 100 days. If the average time to identify a breach (MTTI) was under 100 days, the estimated average total cost of a data breach was $3.11 million. If it was over 100, the estimated cost was $4.21 million, representing $1.1 million additional cost.

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 $2.80 million (less than 100 days to identify) and $3.83 million (100 days or greater to identify).

Figure 28. Relationships between mean time to identify and average total cost

Measured in US$ millions

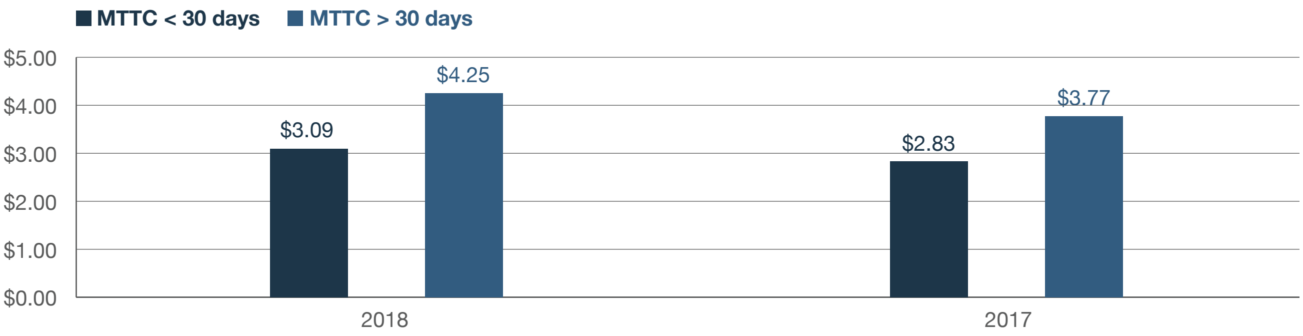


The time to contain a data breach affects the cost. Figure 29 shows a relationship between total data breach cost and breach containment for 477 companies. We bifurcated the consolidated sample between those with an MTTC below and above 30 days. For companies that contained the breach in less than 30 days, the estimated average total cost of a data breach was $3.09 million — compared to $4.25 million for the companies who took more than 30 days to contain the breach.

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 $2.83 million (less than 30 days to contain) and $3.77 million (30 days or greater to contain), as shown in Figure 29.

Figure 29. Relationships between mean time to contain and average total cost

Measured in US$ millions

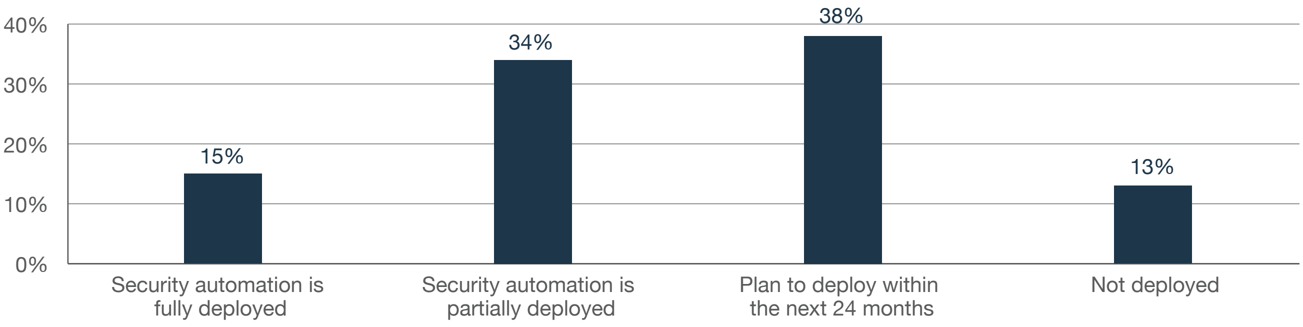


Security automation impacts costs

In this year's study, we examine the relationship between data breach cost and the state of automation experienced by companies that deploy, or do not deploy, automated methods and technologies. In this context, security automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. Such technologies depend upon artificial intelligence, machine learning, analytics, and orchestration.

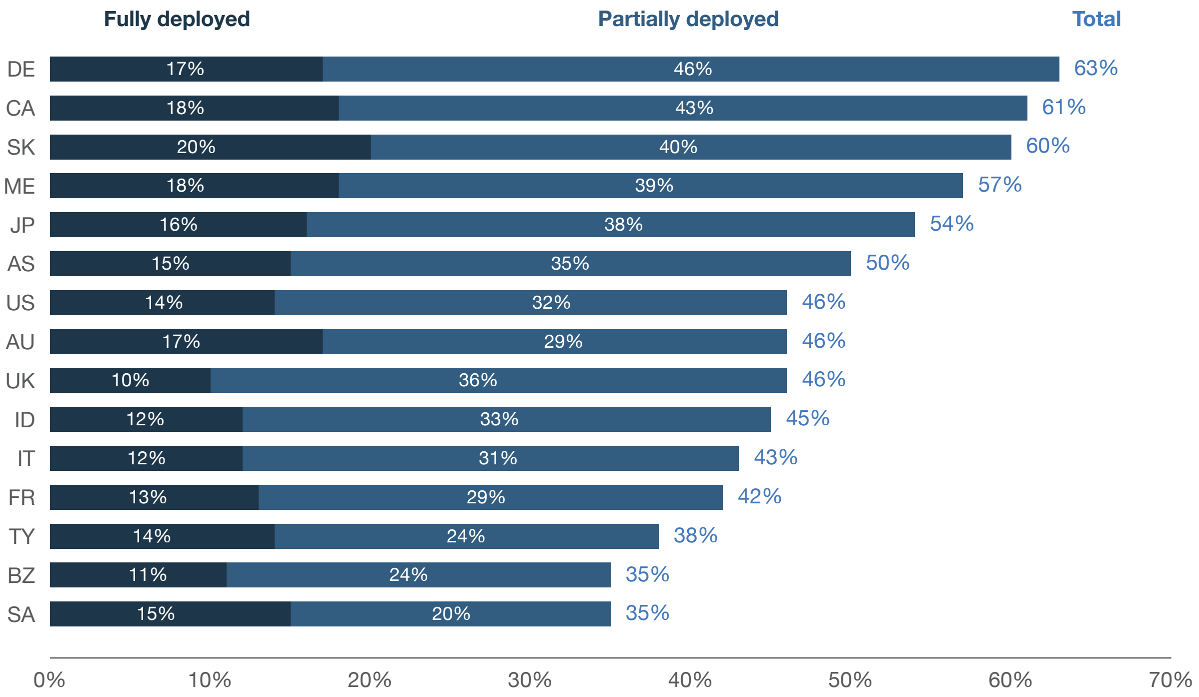
Figure 30 shows the state of security automation for our global sample of 477 companies. As can be seen, only 15 percent of companies report full deployment and 34 percent report partial deployment. Another 38 percent do not deploy today, but they do plan to deploy security automation technologies within the next 24 months. Finally, 13 percent do not deploy, and have no plan to deploy, security automation.

Figure 30. State of security automation



According to Figure 31, the state of security automation varies significantly across country or regional samples. Specifically, German, Canadian, and South Korean companies report the highest deployment rate. In contrast, companies in South Africa, Brazil, and Turkey report the lowest deployment rate.

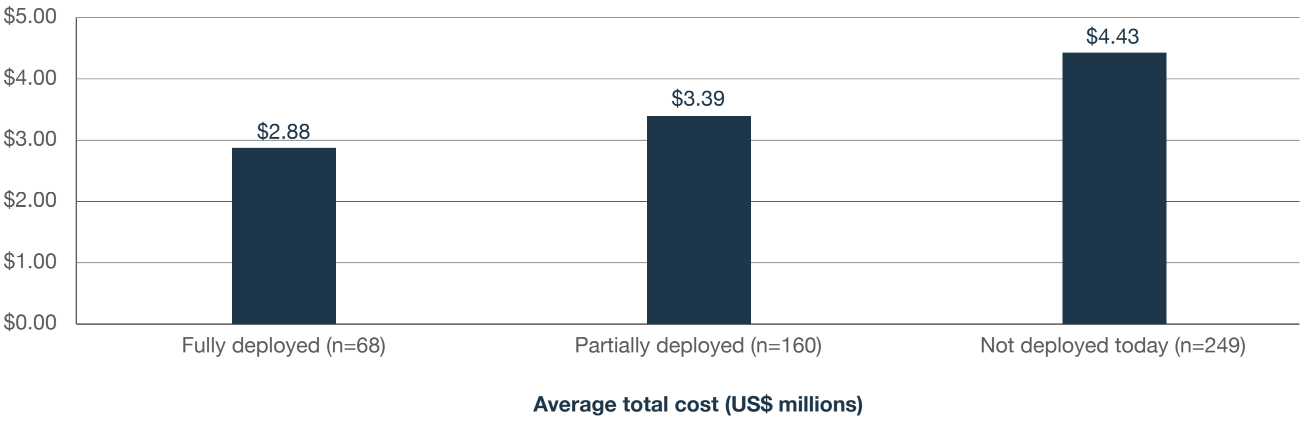
Figure 31. State of security automation by country or region



Results show the average total cost of a data breach is $2.88 million for organizations that fully deploy security automation. In contrast, organizations that do not deploy automation realize a much higher total cost of a data breach at $4.43 million — or a net total cost difference of $1.55 million as shown in Figure 32.

Figure 32. Security automation decreases the total cost

Measured in US$ millions



The cost of a mega data breach

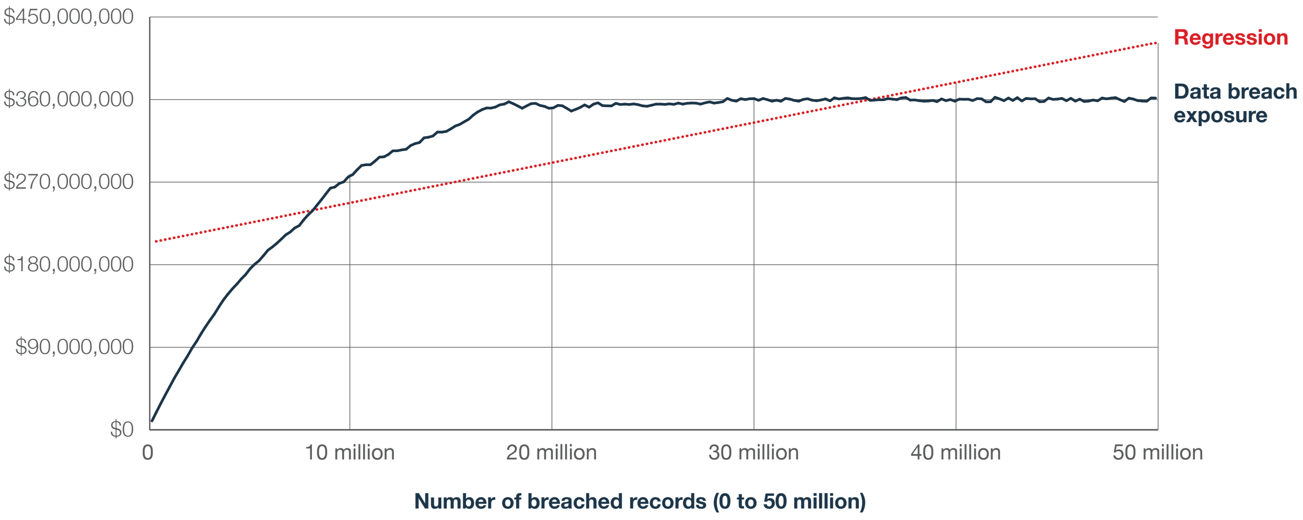
For the first time, we attempt to measure the cost of a data breach involving more than one million compromised records, or what we refer to as a mega breach. We recruited 11 companies that experienced such a data breach over the past two years. These companies are not included in the analysis of the 477 companies because the costs they incur would skew the cost of a data breach presented in this report.

Because the sample size of 11 companies experiencing a mega breach is too small to perform a statistically significant analysis using activity-based cost methods, we use an analytic approach called Monte Carlo simulation[15]. This analytic approach allows us to estimate both the total cost and per capita cost of the mega breach based on a range of possible (random) outcomes through repeated trials. In total, we performed more than 150,000 trials. The mean or average of all sample means provides a most likely outcome at each size of a data breach — ranging from 1 million to 50 million compromised records.

As shown in Figure 33, the analysis reveals a parabolic cost curve. That is, while the total cost of a mega breach increases, the per capita cost decreases. Thus, a data breach involving one million compromised records yields an estimated total cost of $39.49 million and a per capita cost of $41.55. At 50 million records, the total cost could be as high as $350 million, but the estimated per capita cost is $7.63.

Figure 33. Simulated mega breach cost curve

Measured in US$

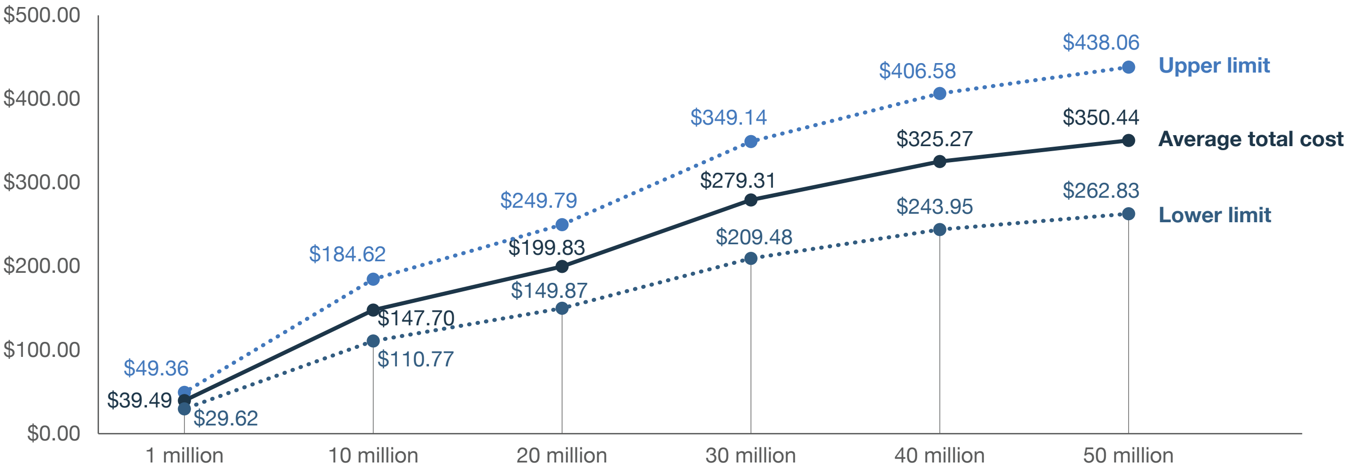


[15] Monte Carlo simulations are used to model the probability of different outcomes in a process that cannot easily be predicted due to the intervention of random variables. It is a technique used to understand the impact of risk and uncertainty in prediction and forecasting models.

Figure 34 shows a more precise range at the 95 percent level of confidence of the total average cost of mega breaches. A data breach involving one million compromised records yields an estimated total cost of $39.49 million, with a range from $29.62 to $49.36. At 50 million records, the total cost could be as high as $350.44 million, with a range from $262.83 to $438.06.

Figure 34. A more precise range of the total average cost of mega breaches

Measured in US$ millions



As in our activity-based costing model, we report a breakdown of the four cost components in the mega breach: detection and escalation, notification, post data breach response and lost business cost, as shown in Figure 35. We used the 11 companies in our mega breach sample to confirm the validity of these four cost categories.

Figure 35. Four components of mega data breach

Number of breached records	Detection & escalation	Notification	Post data breach response	Lost business cost	Total cost
1,000,000	$ 11,682,870	$ 567,130	$ 12,225,694	$ 15,012,731	$ 39,488,426
10,000,000	$ 44,851,852	$ 1,878,009	$ 48,039,120	$ 52,926,157	$ 147,695,139
20,000,000	$ 62,481,481	$ 3,174,306	$ 67,170,833	$ 67,005,556	$ 199,832,176
30,000,000	$ 88,407,407	$ 4,151,389	$ 91,763,194	$ 94,989,352	$ 279,311,343
40,000,000	$ 102,537,037	$ 5,903,009	$ 106,411,343	$ 110,413,657	$ 325,265,046
50,000,000	$ 110,998,725	$ 6,498,576	$ 115,028,472	$ 117,919,213	$ 350,444,986

Figure 36 shows the estimated total cost at six size levels of data breach ranging from 1 to 50 million lost or stolen records. Drawing from our mega cost framework, a data breach involving 1 million compromised records yields a total cost of $39.49 million dollars. At 50 million records, we estimate a total cost of $350.44 million dollars.

Figure 36. Average total cost of mega breach

Measured in US$ millions

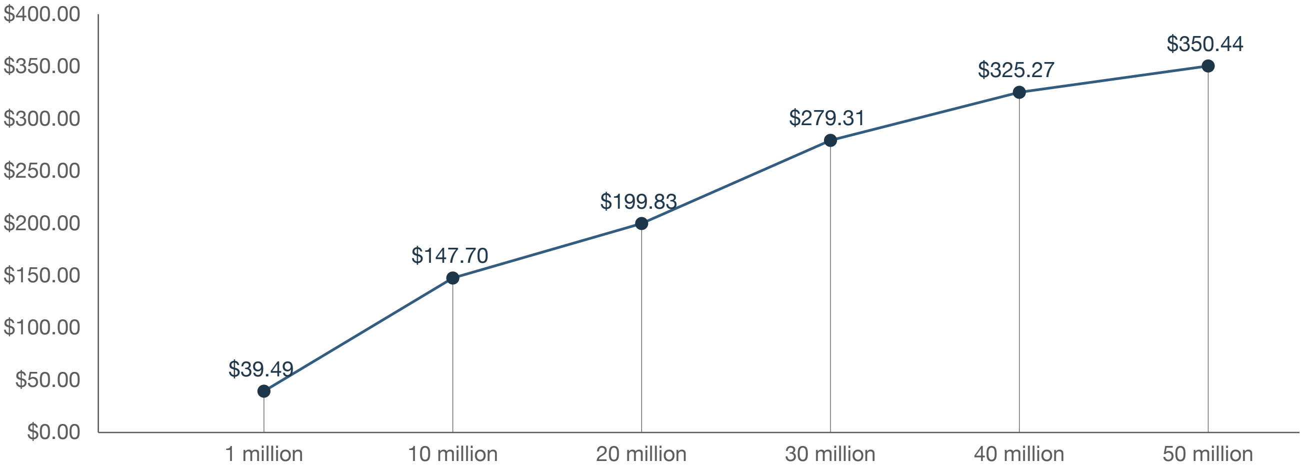
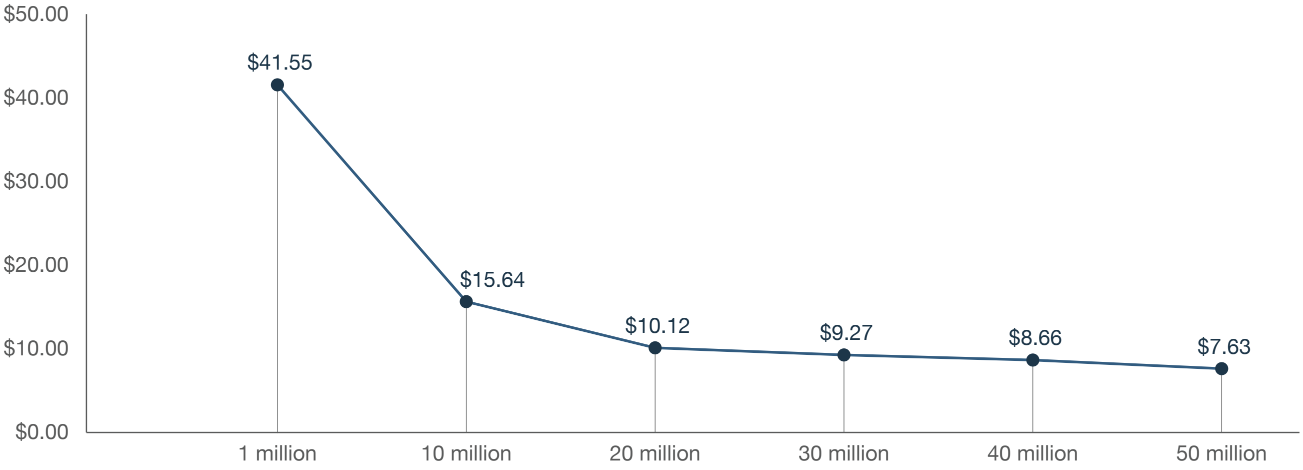


Figure 37 shows the estimated per capita cost of mega breach at six size levels of data breach ranging from one to 50 million lost or stolen records. According to our framework, a data breach involving 1 million compromised records yields a per record cost of $41.55. At 50 million records, we estimate a per capita cost of $7.63. Per capita cost flattens out beyond 50 million records.

Figure 37. Per capita cost of a mega breach

Measured in US$



Part 5. How We Calculate the Cost of a 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 based on actual use. Companies participating in this benchmark research are asked to estimate the cost for all the activities necessary to resolving 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

Typical activities conducted in the aftermath of discovery include the following:

> 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 Full Detailed Findings section (Part 4). The four cost centers are:

> **Detection and escalation:** Activities that enable a company to reasonably detect the breach of personal data either at risk (in storage) or in motion and to report the breach of protected information to appropriate personnel within a specified time period.
> **Notification:** Activities that enable the company to notify individuals who had data compromised in the breach (data subjects) as regulatory activities and communications. Also included are costs that relate to communication with data protection regulators and other related parties.
> **Post data breach response:** Processes set up to help individuals or customers affected by the breach to communicate with the company, as well as costs associated with redress activities and reparation with data subjects and regulators.
> **Lost business:** Activities associated with cost of lost business including customer churn, business disruption, and system downtime. Also included in this category are the costs of acquiring new customers and costs related to revenue loss.

Other considerations in our analysis

Twenty-two factors that impact the per capita cost of a data breach

An important outcome of our research is that we are able to identify 22 meaningful factors that decrease or increase the per capita cost of a data breach. Factors that decrease cost (e.g., cost savings) include: participation in threat sharing, employee training, BCM involvement, cyber analytics, extensive use of encryption, a well-functioning incident response team and more.

In contrast, factors that increase the cost of a data breach include: third party involvement, extensive cloud migration, compliance failure, and the extensive use of mobile platforms. This year we examined two new factors that influence the cost: the use of an AI platform as part of automation and the proliferation of Internet of Things (IoT) devices in the workplace.

Impact of automation on data breach costs

In this year's study, we examine the influence of automation on the cost of a data breach by gathering data from companies that deploy, or do not deploy, automated methods and technologies. In this context, security automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. Such technologies depend upon artificial intelligence, machine learning, analytics, and orchestration.

Results show the average total cost of a data breach is $2.88 million for organizations that fully deploy security automation. In contrast, organizations that do not deploy automation realize a much higher total cost of a data breach at $4.43 million — or a net total cost difference of $1.55 million.

Part 6. Organizational Characteristics and Benchmark Methods

Figure 38 shows the distribution of benchmark organizations by their primary industry classification. 17 industries were represented in this year's study. The largest sectors were financial, services, and industrial & manufacturing companies. Financial service companies include banks, insurance, investment management, brokerage, and payment processors.

Figure 38. Distribution of the sample by industry

Sample size (n) = 477

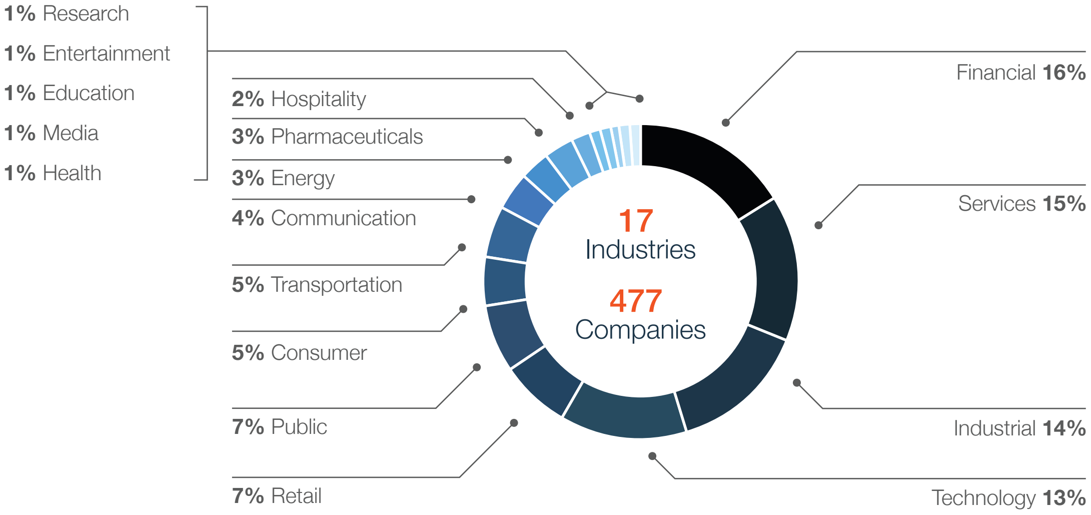
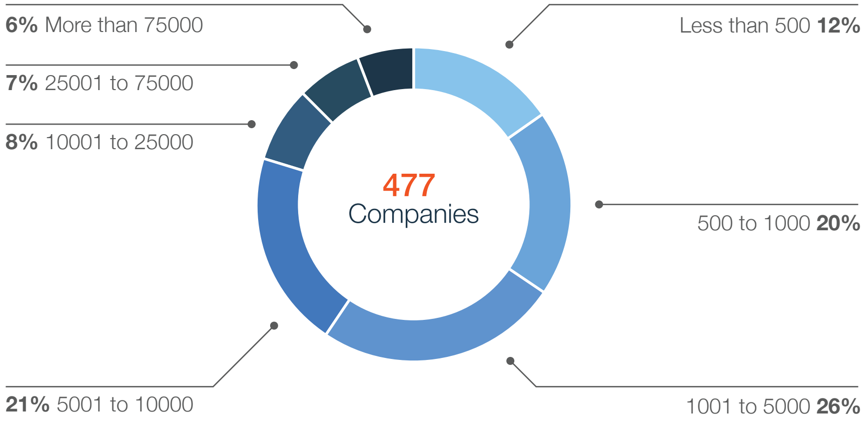


Figure 39 shows the distribution of benchmark organizations by total headcount. The largest segment included companies with 1,001 to 5,000 employees. The smallest segment included companies with more than 75,000 employees.

Figure 39. Global headcount of participating companies

Sample size (n) = 477

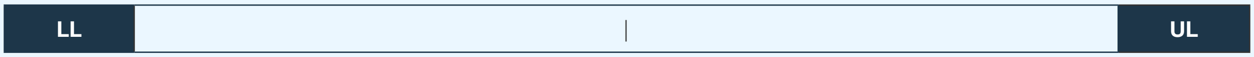


Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant. The benchmark instrument required individuals to rate direct cost estimates for each cost category by marking a range variable 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]



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 7. 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, 477 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. 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.