IBM Security

Cost of a
Data Breach
Report 2019

Table
of Contents

Executive Summary

IBM Security and Ponemon Institute are pleased to release the 2019 Cost of a Data Breach Report.[1] Based on in-depth interviews with more than 500 companies around the world who experienced a data breach between July 2018 and April 2019, the analysis in this research study takes into account hundreds of cost factors, from legal, regulatory and technical activities, to loss of brand equity, customer turnover, and the drain on employee productivity.

Now in the 14th year of the Cost of a Data Breach Report, we included historical data showing trends for a range of metrics over a period of several years. The research continues to evolve, with consideration for the changing nature of information technology, data regulation, and security tools and processes. Above all, this report shows IT professionals, business leaders, researchers and the broader security community that, although the consequences of data breaches are severe, the study points to ways organizations can mitigate costs and potentially improve their overall security posture.

Cost of a data breach highlights

Global Averages 🌐	Average size of a data breach	25,575 records
Average total cost of a data breach	Cost per lost record	Time to identify and contain a breach
$3.92M	$150	279 days
	Highest country average cost of $8.19 million	Highest industry average cost of $6.45 million
	United States	Healthcare

---

[1]The years referenced in this report are for the year of publication. The data breach incidents studied in the 2019 report occurred between July 2018 and April 2019.

What's new in 2019

This year's Cost of a Data Breach Report explores several new avenues for understanding the causes and consequences of data breaches. For the first time, this year's report details the "long tail" of a data breach, demonstrating that the costs of a data breach can be felt for years after the incident. The report also examines organizational and security characteristics that can impact the cost of a data breach, including: the complexity of security environments; operational technology (OT) environments; extensive testing of incident response plans; and the process of closely coordinating development, security, and IT operations functions (DevSecOps).

Continuing to build on previous research, the 2019 report examines trends in the root causes of data breaches and the length of time to identify and contain breaches (the breach lifecycle), plus the relationship of those factors to the overall cost of a data breach. Following the 2018 report's initial examination of "mega breaches" of greater than 1 million lost or stolen records, we continue this research with comparative data for 2019. And for the second year, we examined the cost impacts of security automation, and the state of security automation within different industries and regions.

Key Findings[2]

Lost business was the biggest contributor to data breach costs

The loss of customer trust had serious financial consequences for the companies studied, and lost business was the largest of four major cost categories that contributed to the total cost of a data breach. The average cost of lost business for organizations in the 2019 study was $1.42 million, which represents 36 percent of the total average cost of $3.92 million.[3] The study found that breaches caused abnormal customer turnover of 3.9 percent in 2019. Whereas organizations that lost less than one percent of their customers due to a data breach experienced an average total cost of $2.8 million, organizations with customer turnover of 4 percent or more averaged a total cost of $5.7 million – 45 percent greater than the average total cost of a data breach.

Data breach costs impacted organizations for years

About one-third of data breach costs occured more than one year after a data breach incident in the 86 companies we were able to study over multiple years. While an average of 67 percent of breach costs came in the first year, 22 percent accrued in the second year after a breach, and 11 percent of costs occured more than two years after a breach. The long-tail costs of a breach were higher in the second and third years for organizations in highly regulated environments, such as the healthcare and finance industries. Organizations in a high data protection regulatory environment saw 53 percent of breach costs in the first year, 32 percent in the second year and 16 percent more than two years after a breach.

---

[2]The research in the Cost of a Data Breach Report is conducted by the Ponemon Institute and results are sponsored, analyzed and reported by IBM Security. The study is based on a non-scientific sample of 507 companies. The key findings are based on IBM and Ponemon analysis of the data and do not necessarily apply to organizations outside of the group that was studied.

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

The lifecycle of a data breach was longer

The time between when a data breach incident occured and when the breach was finally contained (also known as the breach lifecycle) grew noticeably between 2018 and 2019. The average time to identify a breach in 2019 was 206 days and the average time to contain a breach was 73 days, for a total of 279 days. This represents a 4.9 percent increase over the 2018 breach lifecycle of 266 days. However, the faster a data breach can be identified and contained, the lower the costs. Breaches with a lifecycle less than 200 days were on average $1.22 million less costly than breaches with a lifecycle of more than 200 days ($3.34 million vs. $4.56 million respectively), a difference of 37 percent.

Malicious attacks were the most common and most expensive root cause of breaches

The study found that data breaches originating from a malicious cyber attack were not only the most common of the breaches studied, but also the most expensive. Since 2014, the share of breaches caused by malicious attacks surged by 21 percent, growing from 42 percent of breaches in 2014 to 51 percent of breaches in 2019. It took substantially longer to identify and contain a breach in the case of a malicious attack: a combined 314 days, for a breach lifecycle that was 12.5 percent longer than the average breach lifecycle of 279 days. This finding helps explain why breaches caused by a malicious attack were 27 percent more costly than breaches caused by human error ($4.45 million vs. $3.5 million) and 37 percent more costly than a breach caused by system glitches ($4.45 million vs $3.24 million).

Breaches from system glitches and human error still cost millions

While malicious breaches were most common, inadvertent breaches from human error and system glitches were still the root cause for nearly half (49 percent) of the data breaches studied in the report. Human error as a root cause of a breach includes "inadvertent insiders" who may be compromised by phishing attacks or have their devices infected or lost/stolen. These were responsible for about one-quarter of breaches. System glitches, or inadvertent failures that could not be tied to a human action, accounted for another quarter of breaches. While less expensive than malicious attacks, system glitches and human error breaches are still costly, with an average loss of $3.24 million and $3.5 million respectively.

Small businesses face disproportionately larger costs relative to larger organizations

We found significant variation in total data breach costs by organizational size. The total cost for the largest organizations (more than 25,000 employees) averaged $5.11 million, which is $204 per employee. Smaller organizations with between 500 and 1,000 employees had an average cost of $2.65 million, or $3,533 per employee. Thus, smaller organizations have higher costs relative to their size than larger organizations, which can hamper their ability to recover financially from the incident.

Cloud migration, IT complexity, and third-party breaches were cost amplifiers

Out of 26 factors we studied contributing to the cost of a data breach, the five that contributed the most cost were third-party involvement, compliance failures, extensive cloud migration, system complexity, and operational technology (OT). If a third party caused the data breach, the cost increased by more than $370,000, for an adjusted average total cost of $4.29 million. Organizations undergoing a major cloud migration at the time of the breach saw a cost increase of $300,000, for an adjusted average cost of $4.22 million. System complexity increased the cost of a breach by $290,000, for an average cost of $4.21 million.

Encryption, business continuity management, DevSecOps and threat intelligence sharing were cost mitigators

Among the 26 cost factors we studied, there was a diverse set of cost mitigators that either helped reduce costs preventatively or in the aftermath of a breach. Extensive use of encryption, data loss prevention, threat intelligence sharing and integrating security into the software development process (DevSecOps) were all associated with lower-than-average data breach costs. Among these, encryption had the greatest impact, reducing breach costs by an average of $360,000. Business continuity management in the aftermath of a breach reduced the total cost of a data breach by an average of $280,000.
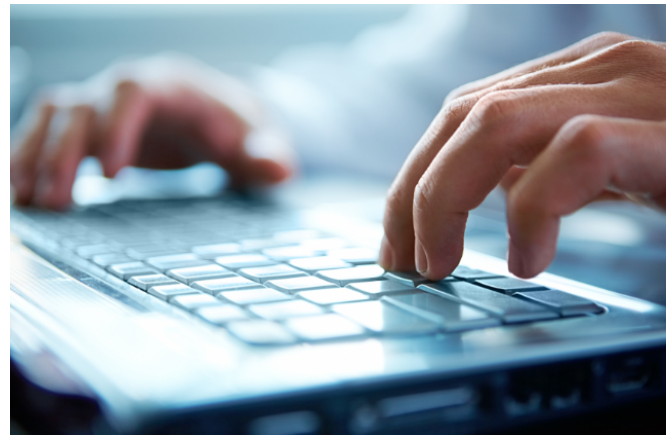
Companies studied that had an incident response team and extensive testing of their response plans saved over $1.2 million

An organization's ability to respond effectively after a data breach was strengthened by the presence of an incident response (IR) team that follows an incident response plan. In this year's research, we found that organizations with an incident response team amplified their cost-savings by also conducting extensive testing of their IR plan, such that the combined effect of the IR team and IR plan testing produced a greater cost savings than any single security process. Those organizations who conducted extensive testing of an IR plan had an average total cost of a breach that was $1.23 million less than those that neither had an incident response team or tested their incident response plan ($3.51 million vs. $4.74 million). Testing the incident response plan, through exercises such as tabletop exercises or simulations of the plan in an environment such as a cyber range, helped teams respond faster and potentially contain the breach sooner.

Automation of security reduced costs

Organizations that had deployed automated security solutions that reduce the need for direct human intervention – including the use of security solutions with artificial intelligence, machine learning, analytics, and automated incident response orchestration – saw significantly lower costs after experiencing a data breach. Organizations that had not deployed security automation experienced breach costs that were 95 percent higher than breaches at organizations with fully-deployed automation ($5.16 million average total cost of a breach without automation vs. $2.65 million for fully-deployed automation). Breach costs at organizations without automation deployed were far costlier in 2019 than in 2018, going up from an average of $4.43 million in 2018 to $5.16 million in 2019, an increase of more than 16 percent. Breaches at organizations with fully deployed automation decreased in cost from 2018 to 2019. Those breaches decreased in cost by 8 percent, from an average of $2.88 million in 2018 to $2.65 million in 2019.
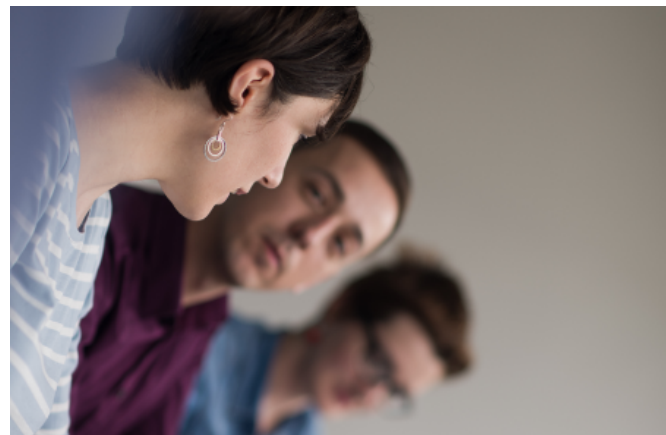
Region and industry impacted total costs

Continuing a multi-year trend, data breaches in the U.S. were vastly more expensive than those in other nations, with an average total cost of $8.19 million (more than double the global average). The U.S. average total cost has increased 130 percent over the 14 years of the study, up from $3.54 million in 2006. Organizations in the Middle East reported the highest average number of breached records (38,800 per incident, compared to global average of around 25,500.) For the ninth year in a row, healthcare organizations had the highest costs associated with data breaches at $6.45 million – over 60 percent more than the global average of all industries.

The odds of experiencing a data breach increased

The percentage chance of experiencing a data breach within two years was 29.6 percent in 2019, an increase from 27.9 percent in 2018. In 2014, organizations had a 22.6 percent chance of experiencing a breach within two years. In the span of six years, the likelihood of experiencing a breach within two years grew by 7 percentage points (700 basis points), representing a 31 percent increase in the odds of experiencing a breach within two years. In other words, organizations in the 2019 study were nearly one-third more likely to experience a breach within two years than they were in 2014.

About the Report

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.

In this section of the report, we describe what factors we study that affect the cost of a data breach and provide answers to the most frequently asked questions about the study.

How we gathered the data

For the 2019 Cost of a Data Breach Report, we recruited 507 organizations that have experienced a breach in the last year and interviewed more than 3,211 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 that was lost following the data breach.

In the course of our interviews, we also asked questions to determine what the organization spent on activities detecting the breach 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 studied that influence the cost are the root causes of the data breach and the time to detect and contain the incident (the data breach lifecycle).

507
companies studied

3,211
individuals interviewed

How the cost of a data breach is calculated

To calculate the cost of a data breach, we use an accounting method called activity-based costing (ABC). This method identifies activities and assigns a cost according to actual use. The ABC methodology is fully explained in the How We Calculate the Cost of a Data Breach section of this report.

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

Detection and escalation

Activities that enable a company to detect and report a 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

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 to data subjects that their personal information was lost or stolen

- Communication with regulators; determination of all regulatory requirements, engagement of outside experts

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)

Lost business cost

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

Examples:

- Cost of business disruption and revenue losses from system downtime

- Cost of lost customers and acquiring new customers (customer turnover)

- Reputation losses and diminished goodwill

For a more in-depth explanation of the methods used for this report, refer to the sections How We Calculate the Cost of a Data Breach, Organization Characteristics, and Research Limitations.

Cost of a Data Breach FAQs

What is a data breach?
A data 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 a 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 $150.

How do you collect the data?
Our researchers collected in-depth qualitative data through more than 3,211 separate interviews conducted over a 7-month period with 507 companies. Recruiting organizations began in October 2018 and interviews were completed April 30, 2019. Breaches studied occurred between July 2018 and April 2019. In each of the 507 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, an organization may decide to increase investments in cybersecurity due to new threats or regulations, but those investments 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 Report is the organization. In survey research, the unit of analysis is the individual. We recruited 507 organizations to participate in this study. Data breaches range from a low of 2,000 compromised records to slightly more than 100,000 records.

Can the average cost of a 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 mega data breaches, such as Equifax or Facebook. These are not the typical 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 of breaches involving one million or more records (mega breaches).

Why are we using simulation methods to estimate the cost of a mega data breach?

The sample size of 14 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.

Are you tracking the same organizations each year?

Each annual study involves a different sample of companies. Generally, we do not track the same sample of companies over time. However, for the 2019 report we looked at a sample of 86 companies that allowed us to look at the effects of a data breach over two or more years, enabling us to analyze those companies that took a long time to remediate the data breach and what the costs were. To be consistent, we recruit a sample of companies each year with a similar breakdown of characteristics such as the industry, headcount, geographic footprint and size of data breach. Since starting this research in 2005, we have studied the data breach experiences of 3,416 different organizations.

Complete Findings

In this section, we provide the complete detailed findings of this research.

- Global and industry cost differences
- Root causes of a data breach
- The four cost components
- Factors that influence cost
- Incident response effectiveness
- Effect of customer turnover
- Likelihood of a data breach
- The data breach lifecycle
- Long tail costs
- Impact of security automation
- Cost of a mega breach

Global and industry cost differences

This year's annual study was conducted in 16 countries or regional samples: the United States, India, the United Kingdom, Germany, Brazil, Japan, France, the Middle East, Canada, Italy, South Korea, Australia, Turkey, ASEAN, South Africa, and, for the first time, Scandinavia.

There were 17 industries represented in the sample (see the section Organization Characteristics for more on the industries included in the study sample).

Key findings:

The average total cost of a data breach in the U.S. for the companies studied has grown from $3.54 million in 2006 to $8.19 million in 2019, a 130 percent increase over 14 years.

$3.54ᴹ

US total cost in 2006

$8.19ᴹ

US total cost in 2019

The Middle East had the highest average number of breached records, 38,800, compared to the global average of 25,575.

38,800

Middle East average number of breached records.

25,575

Global average of breached records.

The average total cost of a data breach in the healthcare industry was $6.45 million, or 65 percent higher than the average total cost of a data breach.

$6.45ᴹ

Average total cost of a data breach in the healthcare industry.

65%

65 percent higher than the average total cost of a data breach.

Smaller organizations had higher costs relative to their size than larger organizations. The total cost for organizations with more than 25,000 employees averaged $204 per employee.

Organizations with between 500 and 1,000 employees had an average cost of $3,533 per employee.

$204

per employee

Breach costs at organizations with more than 25,000 employees averages $204 per employee.

$3,533

per employee

Breach costs at organizations with between 500 and 1,000 employees have an average cost of $3,533 per employee.

Figure 1:
Global study at a glance

Countries	Sample	PCT.	Currency	Years of study
United States	64	13%	US Dollar	14
India	45	9%	Rupee	8
United Kingdom	45	9%	GBP	12
Germany	36	7%	Euro	11
Brazil	35	7%	Real	7
Japan	33	7%	Yen	8
France	32	6%	Euro	10
Middle East*	28	6%	AED/SAR	6
Canada	27	5%	CA Dollar	5
Italy	26	5%	Euro	8
South Korea	26	5%	KRW	2
Australia	25	5%	AU Dollar	10
Turkey	22	4%	TRY	2
ASEAN#	21	4%	SGD	3
South Africa	21	4%	ZAR	4
Scandinavia+	21	4%	Krone	1
Total	507	100%		

* Middle East 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, Philippines, Malaysia, Thailand and Vietnam
+ Scandinavia is a cluster of companies located in Denmark, Sweden, Norway and Finland

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

Figure 2:

Global average total cost of a data breach

Measured in US$ millions
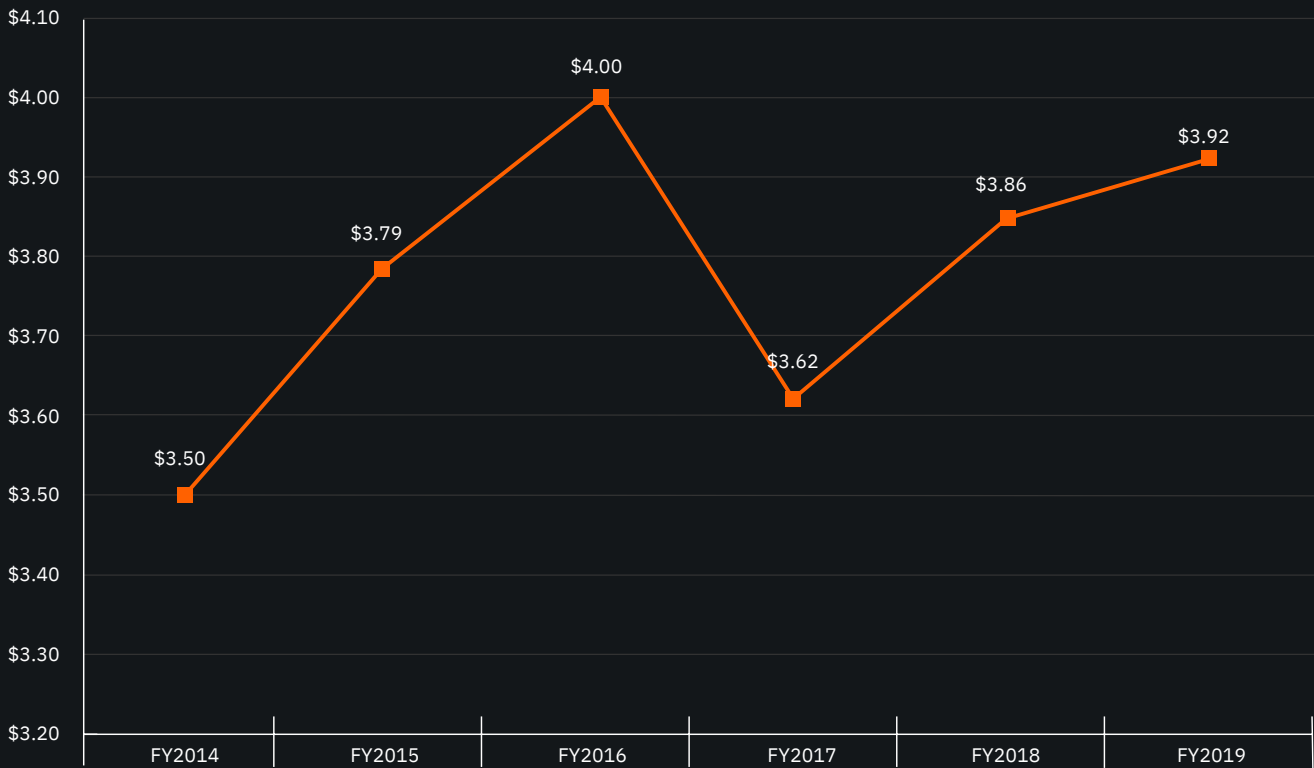
The global average cost of a data breach increased to $3.92 million.

Figure 2 presents the global average total cost of a data breach over six years. The consolidated average total cost of a breach in 2019 increased by 1.5 percent from 2018. In the six years since 2014, the average total cost of a data breach has increased by 12 percent, from $3.5 million.

Figure 3:

Average data breach cost per record

Measured in US$
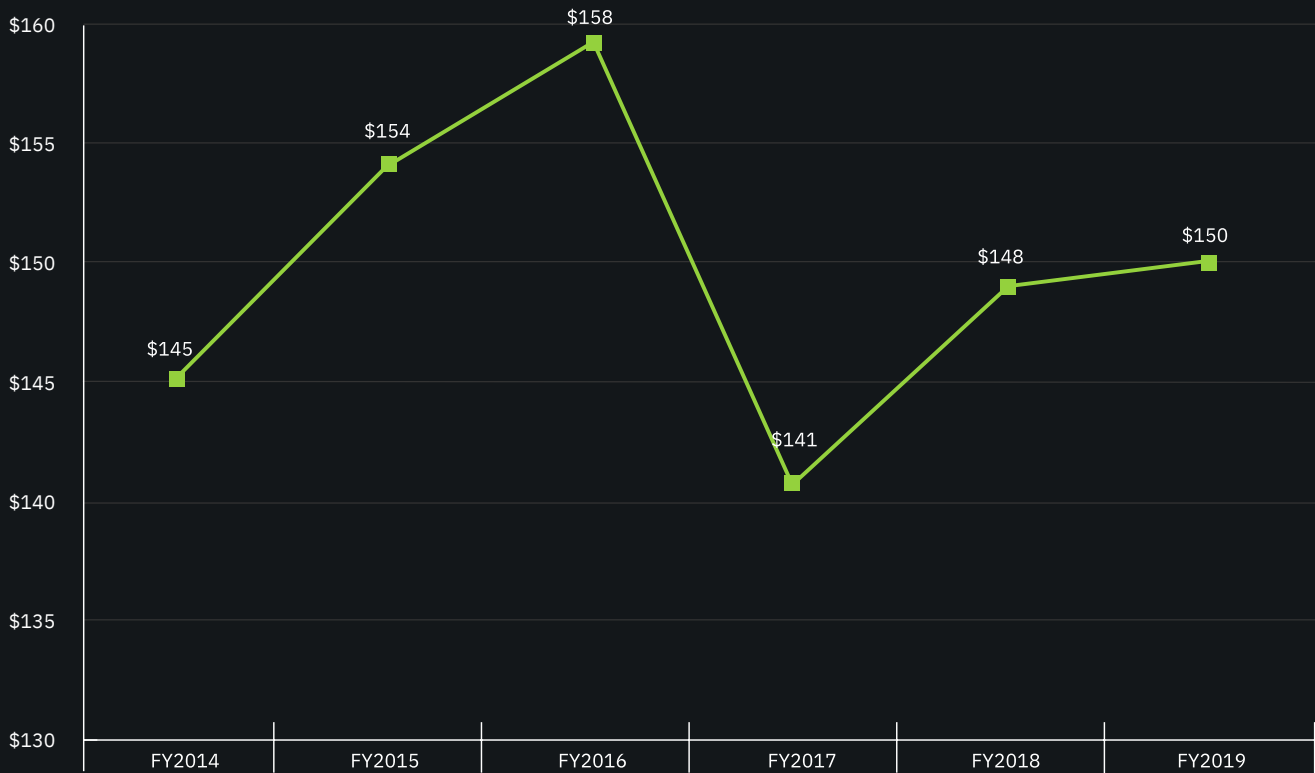
The average cost per compromised record has increased slightly.

Figure 3 shows the average data breach cost per compromised record over the past five years. Similar to the average total cost of a data breach, there was a slight increase of 1.3 percent since 2018.

Figure 4:

Total cost of a data breach by organizational size

Measured in US$ millions

The cost of a data breach varies by organizational size.

Figure 4 shows the total cost of a data breach by headcount, which is a surrogate for organizational size. The total cost for the largest organizations (more than 25,000 employees) averaged $5.11 million, which was $204 per employee. Smaller organizations with between 500 and 1,000 employees had an average cost of $2.65 million, or $3,533 per employee. Thus, smaller organizations had higher costs relative to their size than larger organizations, and a breach could harm their ability to recover financially from the incident.

Figure 5:

Cost of a data breach by country or region

Measured in US$ millions
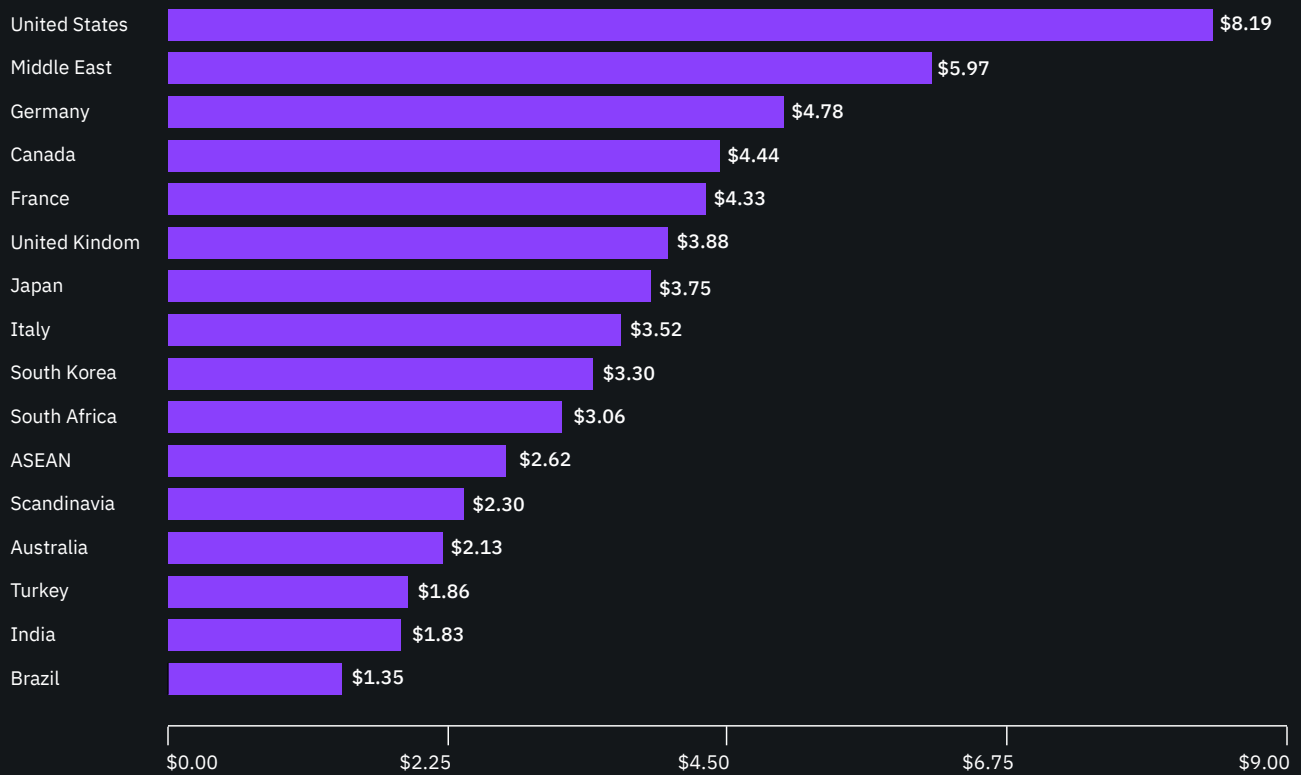
The average organizational cost of
a data breach varies by country.

Figure 5 shows the 2019 average total cost of a data
breach by country. Organizations in the United States had
the highest total average cost at $8.19 million, followed
by the Middle East at $5.97 million. In contrast, Indian
and Brazilian organizations had the lowest total average
cost at $1.83 million and $1.35 million, respectively.

Figure 6:

Cost per record by country or region

Measured in US$

Country	Cost
United States	$242
Germany	$193
Canada	$187
Middle East	$173
France	$163
Sout Africa	$155
United Kingdom	$155
South Korea	$153
Italy	$146
Japan	$141
Scandinavia	$130
ASEAN	$129
Australia	$110
Turkey	$95
India	$72
Brazil	$69
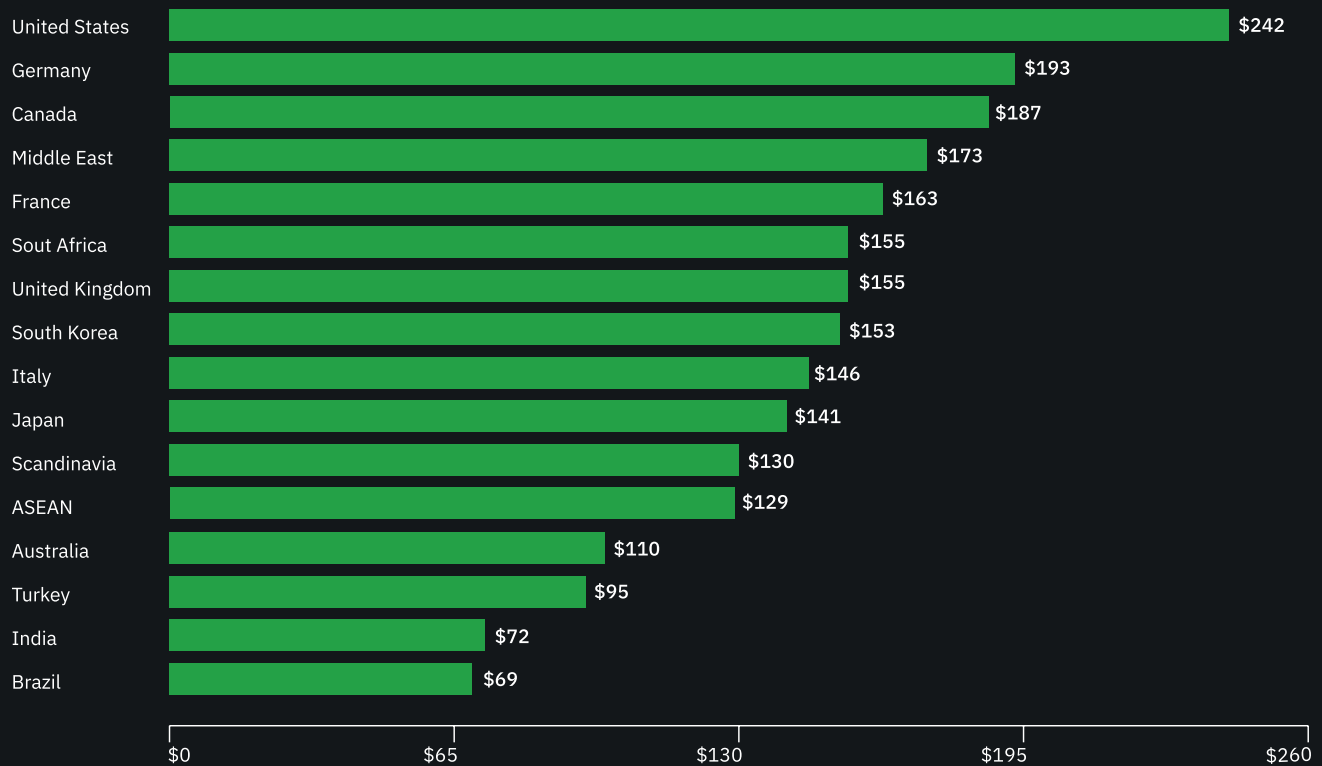
**The average per record cost of
a data breach varied by country.**

Figure 6 shows this year's study's average per record
cost of a data breach by country or region. Organizations
in the United States had the highest total per record cost
at $242, followed by Germany at $193 and Canada at
$187.

Figure 7:

Average number of records per breach by country or region

Global average = 25,575

Country/Region	Value
Middle East	38,800
India	35,636
United States	32,434
Brazil	26,523
France	26,300
Germany	25,610
Italy	24,577
United Kingdom	23,636
South Korea	23,600
Canada	23,071
Turkey	22,551
ASEAN	22,500
South Africa	22,060
Scandinavia	21,663
Japan	20,445
Australia	19,800
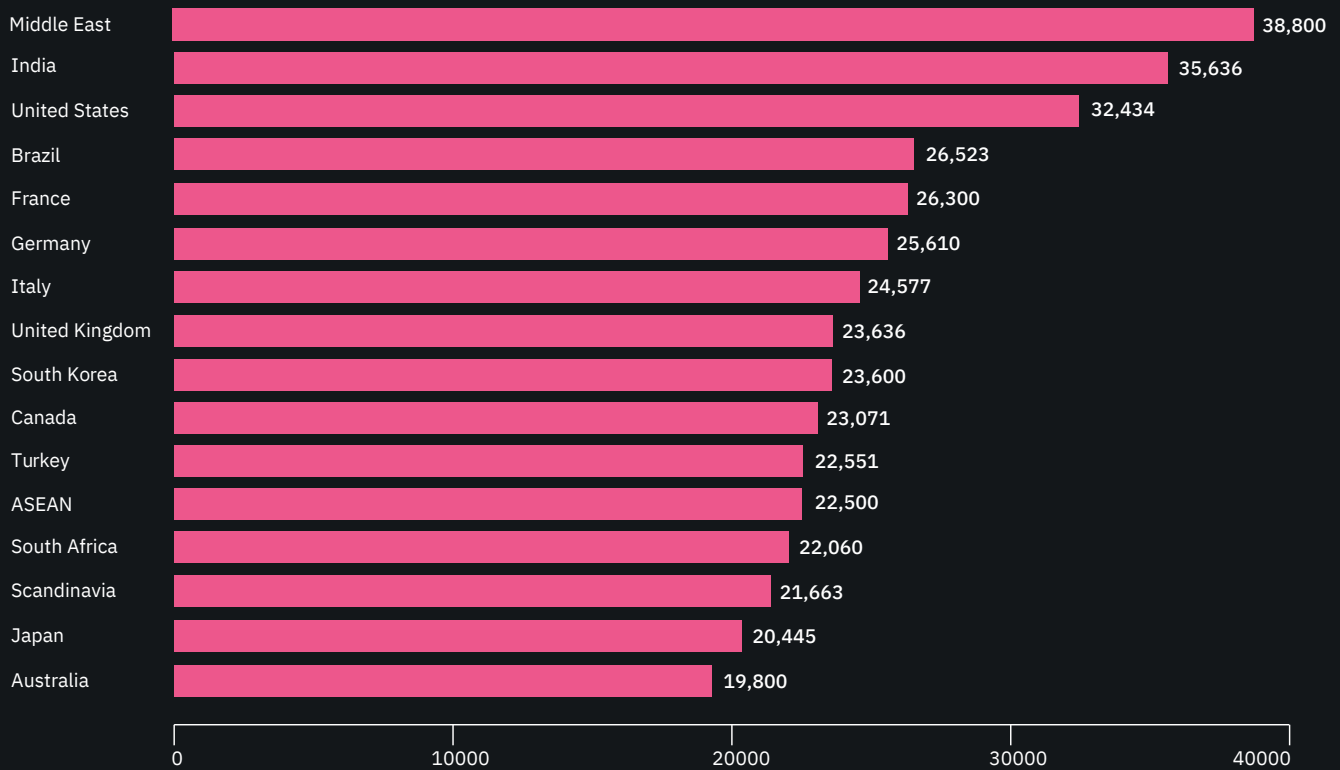
Number of exposed or compromised records varied by country or region.

Figure 7 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 3.9 percent since 2018. Organizations in the Middle East, India, and the U.S. had the largest average number of breached records. Scandinavia, Japan and Australia had the smallest average number of breached records.

Figure 8:

Average total cost of a breach by number of records lost

Measured in US$ millions
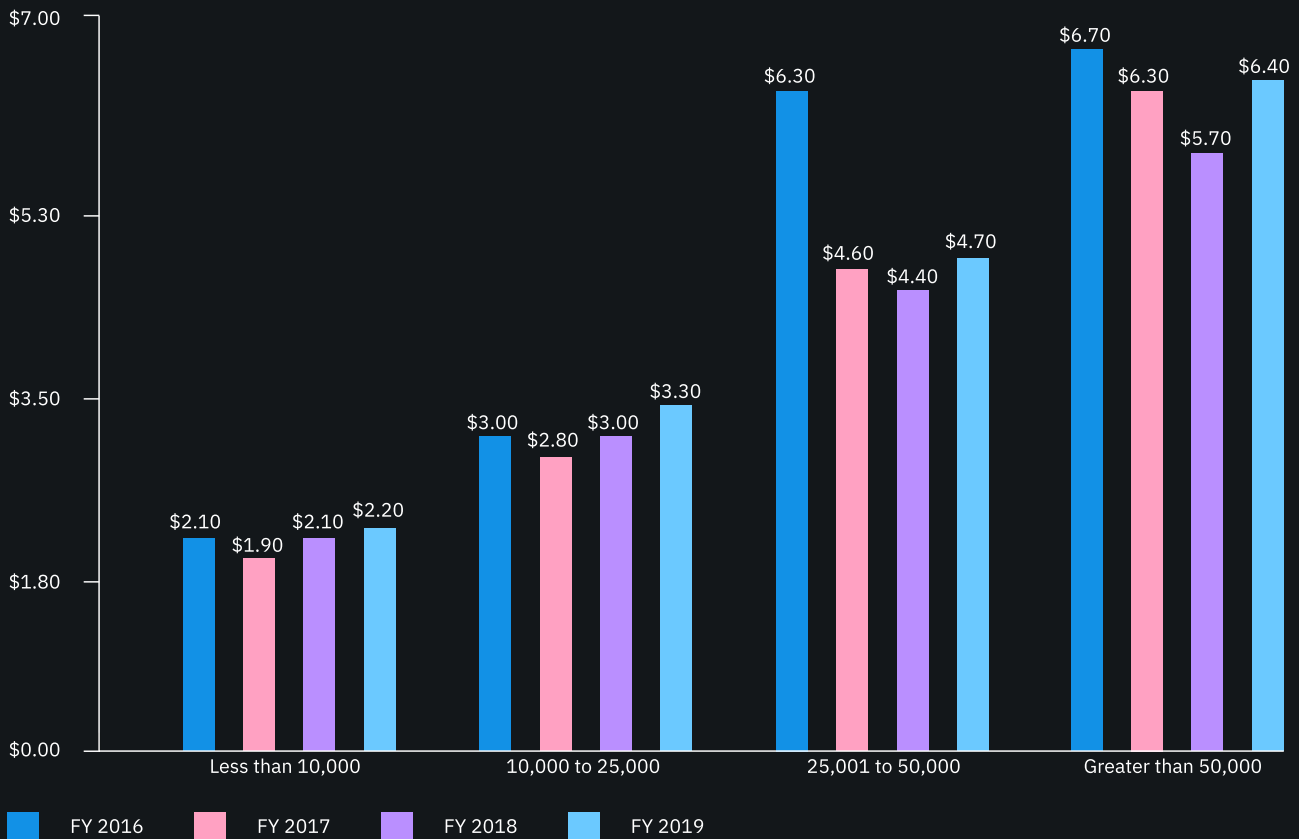
The relationship between data breach size and cost are linearly related.

Figure 8 shows the relationship between the number of records lost and the average total cost of a data breach. As can be seen, data breaches with less than 10,000 compromised records incurred a cost of $2.2 million in 2019. Data breaches with more than 50,000 compromised records were nearly three times more costly than those with less than 10,000 compromised records in 2019, at $6.4 million.

Figure 9:

Percentage change in key data breach metrics, 2018-2019

By country or region

■ Abnormal customer turnover	■ Size of data breach
■ Average total cost	■ Per record cost

Categories (top to bottom): ASEAN, Australia, Brazil, Canada, France, Germany, India, Italy, Japan, Middle East, South Africa, South Korea, Turkey, United Kingdom, United States. X-axis: -10%, 0%, 10%, 20%, 30%.
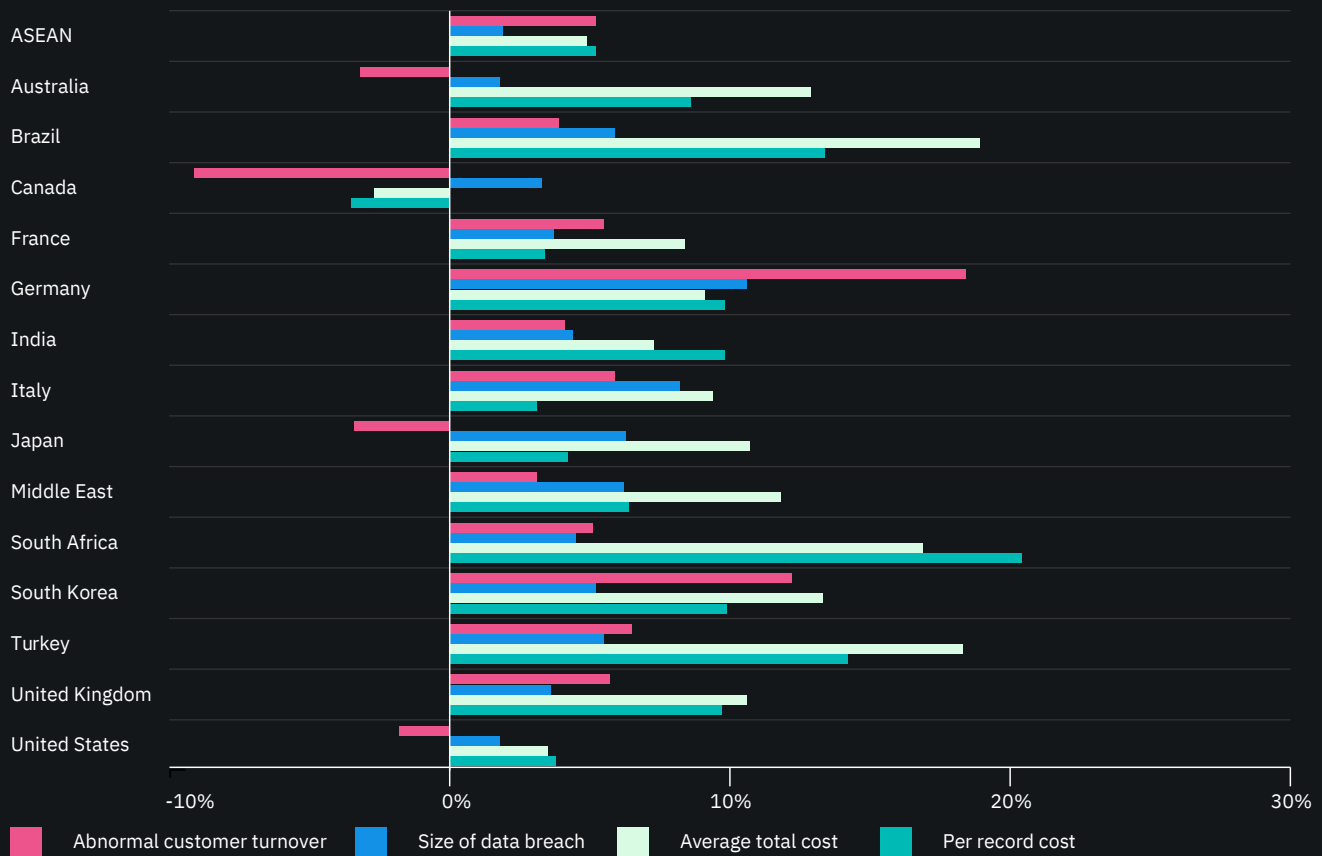
The net change since 2018 study of key metrics of data breach cost and size varies for each country.[4]

Figure 9 presents the percentage change in four metrics over the past year for each country.[5] These metrics are: (1) abnormal customer turnover (greater-than-expected loss of customers since the breach occurred), (2) average size of a data breach (number of records lost or stolen), (3) average total cost of a data breach and (4) per record cost.

As shown, only four countries experienced a net decrease in abnormal customer turnover. These are Australia, Canada, Japan and the United States. In addition, only Canada experienced a net decrease in the average total and per record cost of a data breach. All countries experienced a net increase in the size of a data breach.
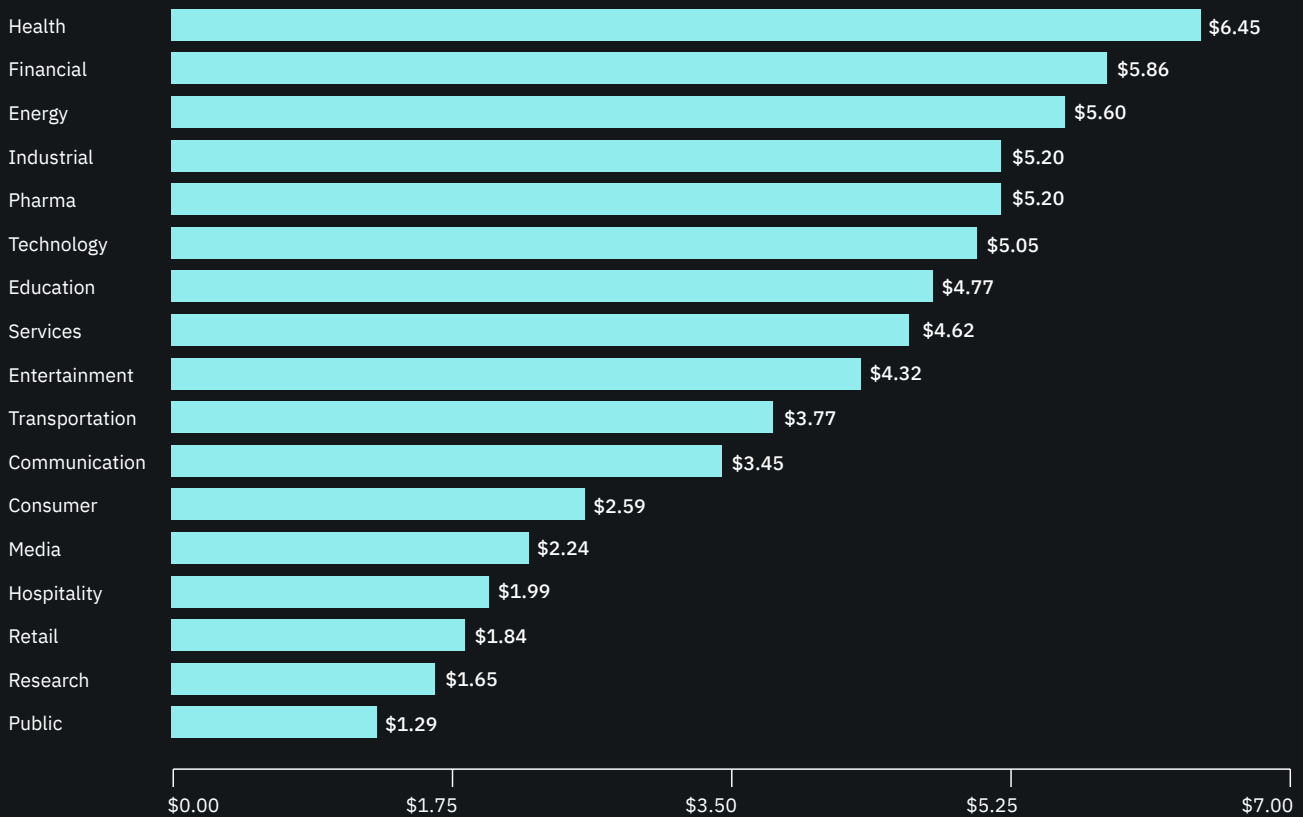
[4]Scandinavia is not included in this analysis because this is the first year this region is included.

[5]The percentage change shown in Figure 9 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.

Figure 10:

Average total cost of a data breach by industry

Measured in US$ millions

Industry	Cost
Health	$6.45
Financial	$5.86
Energy	$5.60
Industrial	$5.20
Pharma	$5.20
Technology	$5.05
Education	$4.77
Services	$4.62
Entertainment	$4.32
Transportation	$3.77
Communication	$3.45
Consumer	$2.59
Media	$2.24
Hospitality	$1.99
Retail	$1.84
Research	$1.65
Public	$1.29

$0.00 $1.75 $3.50 $5.25 $7.00

Organizations subject to more rigorous regulatory requirements had a higher cost of a data breach.

Figure 10 shows healthcare, financial services, energy and pharmaceuticals experienced an average total cost of a data breach significantly higher than less regulated industries such as media, hospitality, retail and research organizations. Public sector organizations traditionally had a lower cost of a data breach because they are unlikely to experience a significant loss of customers as a result of a data breach.

Figure 11:

Average cost per record by industry sector

Measured in US$

Industry	Cost
Health	$429
Financial	$210
Technology	$183
Pharmaceutical	$178
Services	$178
Energy	$165
Industrial	$160
Education	$142
Entertainment	$138
Communication	$132
Consumer	$131
Transportation	$130
Hospitality	$123
Media	$123
Retail	$119
Research	$117
Public	$78

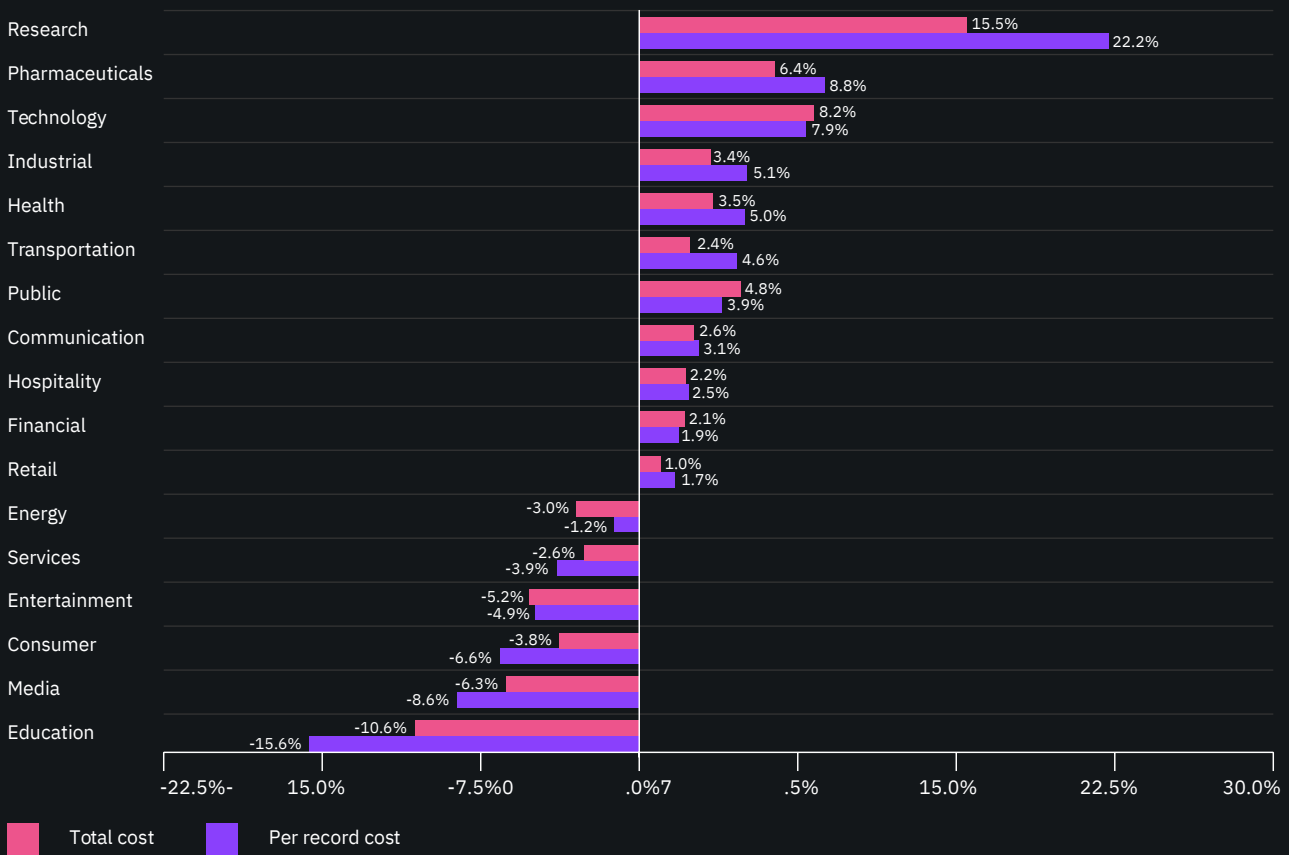$0 $125 $250 $375 $500
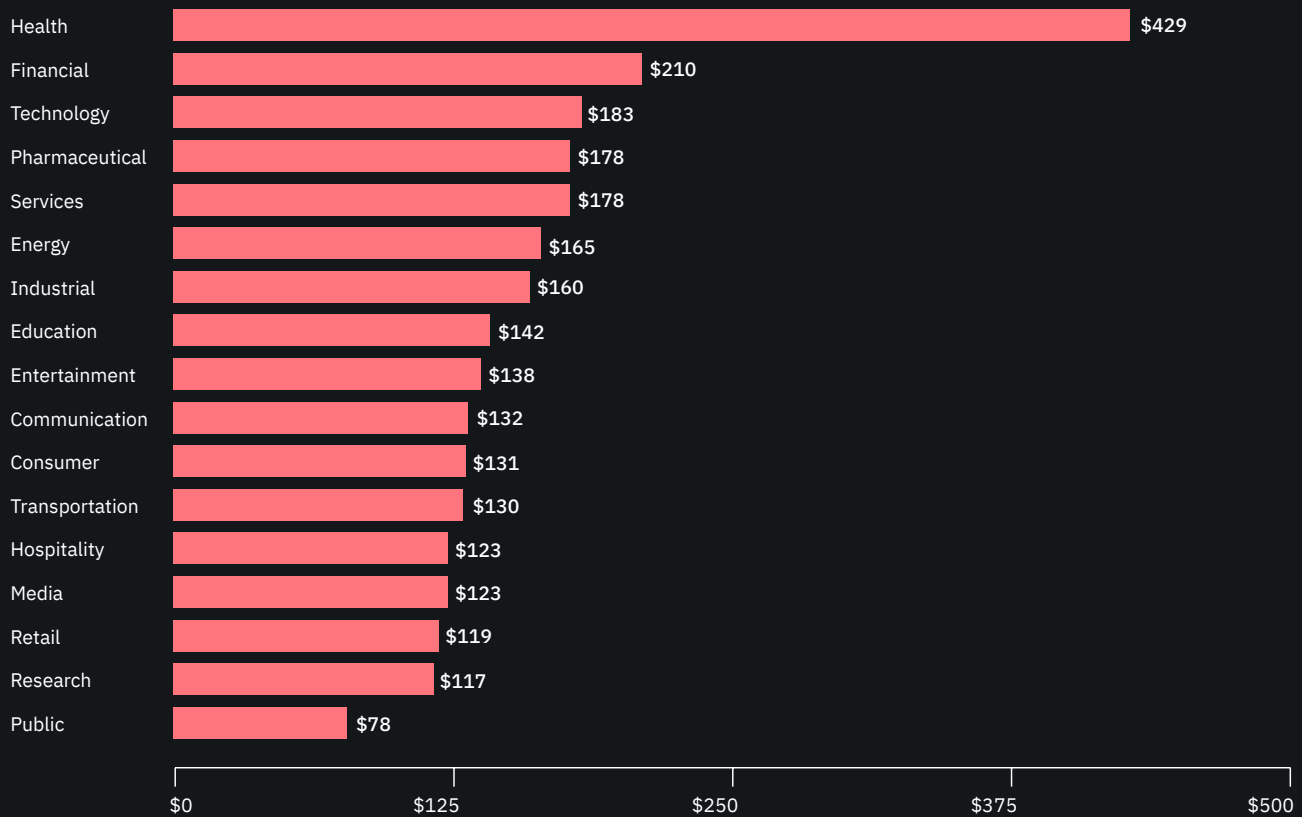
Certain industries had higher data breach costs.

Figure 11 compares this year's per record costs for the consolidated sample by industry classification. Similar to Figure 10, industries such as healthcare and financial organizations have a per record data breach cost substantially higher than the overall mean of $150. Public sector, research, retail and hospitality had a per record cost well under the overall mean value.

It is important to note that the highest per record cost of $429 was experienced by healthcare organizations. A reason for the much higher cost is the fact that all healthcare companies in this study are located in the United States, which had the highest per record cost. In other countries, healthcare was classified as a public sector organization.

Figure 12:

Percentage net change in cost per record and total cost by industry, 2018-2019

	Total cost	Per record cost
Research	15.5%	22.2%
Pharmaceuticals	6.4%	8.8%
Technology	8.2%	7.9%
Industrial	3.4%	5.1%
Health	3.5%	5.0%
Transportation	2.4%	4.6%
Public	4.8%	3.9%
Communication	2.6%	3.1%
Hospitality	2.2%	2.5%
Financial	2.1%	1.9%
Retail	1.0%	1.7%
Energy	-3.0%	-1.2%
Services	-2.6%	-3.9%
Entertainment	-5.2%	-4.9%
Consumer	-3.8%	-6.6%
Media	-6.3%	-8.6%
Education	-10.6%	-15.6%

Since the 2018 study, some industries saw net increases in costs while other saw costs decline.

Figure 12 shows a one year net change from the 2018 to 2019 studies, in total and per record cost, by industry. Research companies had the largest increase since the 2018 study. Meanwhile, education and media companies had the largest net decrease.

Root causes of a data breach

Not all data breaches are created alike. A breach caused by a criminal hacker or a malicious insider is materially different from a breach caused by human error or system failure. In this year's report, we examined three root causes of data breaches and the costs associated with the different causes.

Key facts:

51%

Malicious attacks caused a majority (51 percent) of data breaches.

25%

Malicious attacks were the costliest, with a per record cost that was 25 percent higher than breaches caused by human error or system glitches.

21%

Malicious attacks have increased as a share of breaches, up 21 percent between the 2014 and 2019 studies.

Figure 13:
Data breach root causes

- Malicious or criminal attack
- System glitch
- Human error

24%

51%

25%
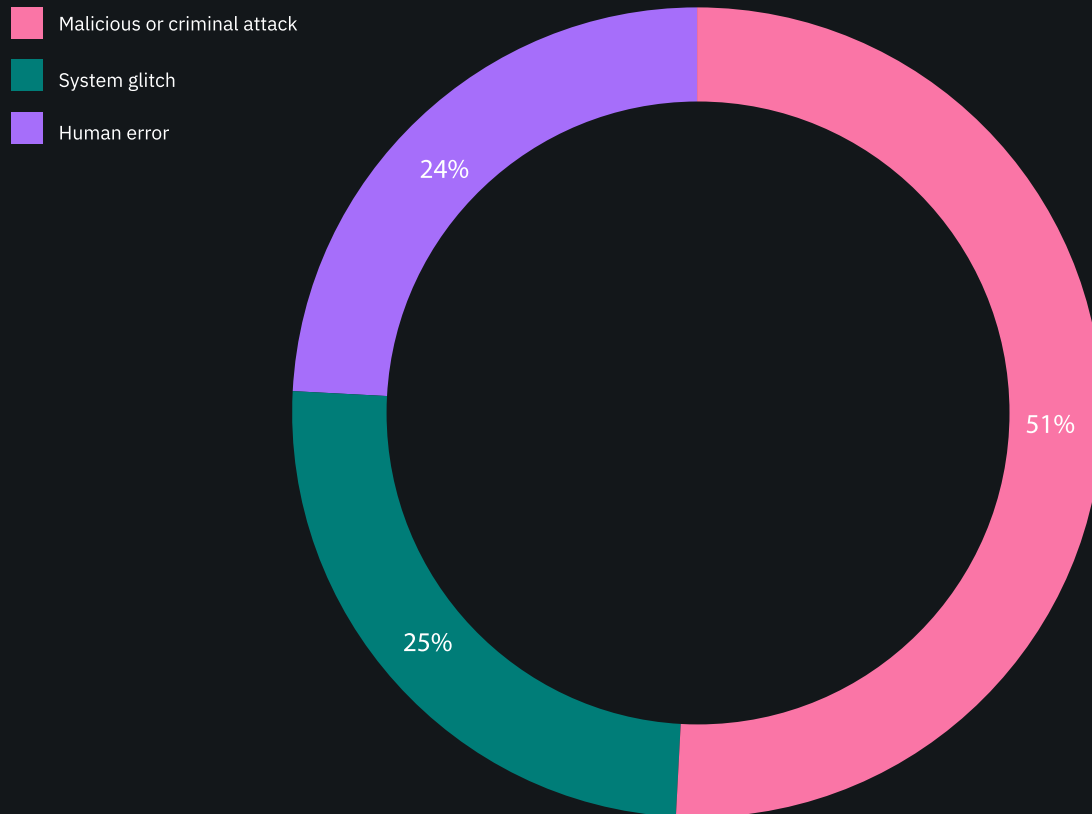
Malicious or criminal attacks
caused the most data breaches.[6]

Figure 13 provides a summary of the main root causes of data breaches on a consolidated basis for organizations in all countries. Fifty-one percent of incidents involved a malicious or criminal attack, 25 percent involved system glitches, including both IT and business process failures[7] and 24 percent were due to negligent employees or contractors (human error).

[6]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).

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

Figure 14:

Per record cost for three data breach root causes

Measured in US$
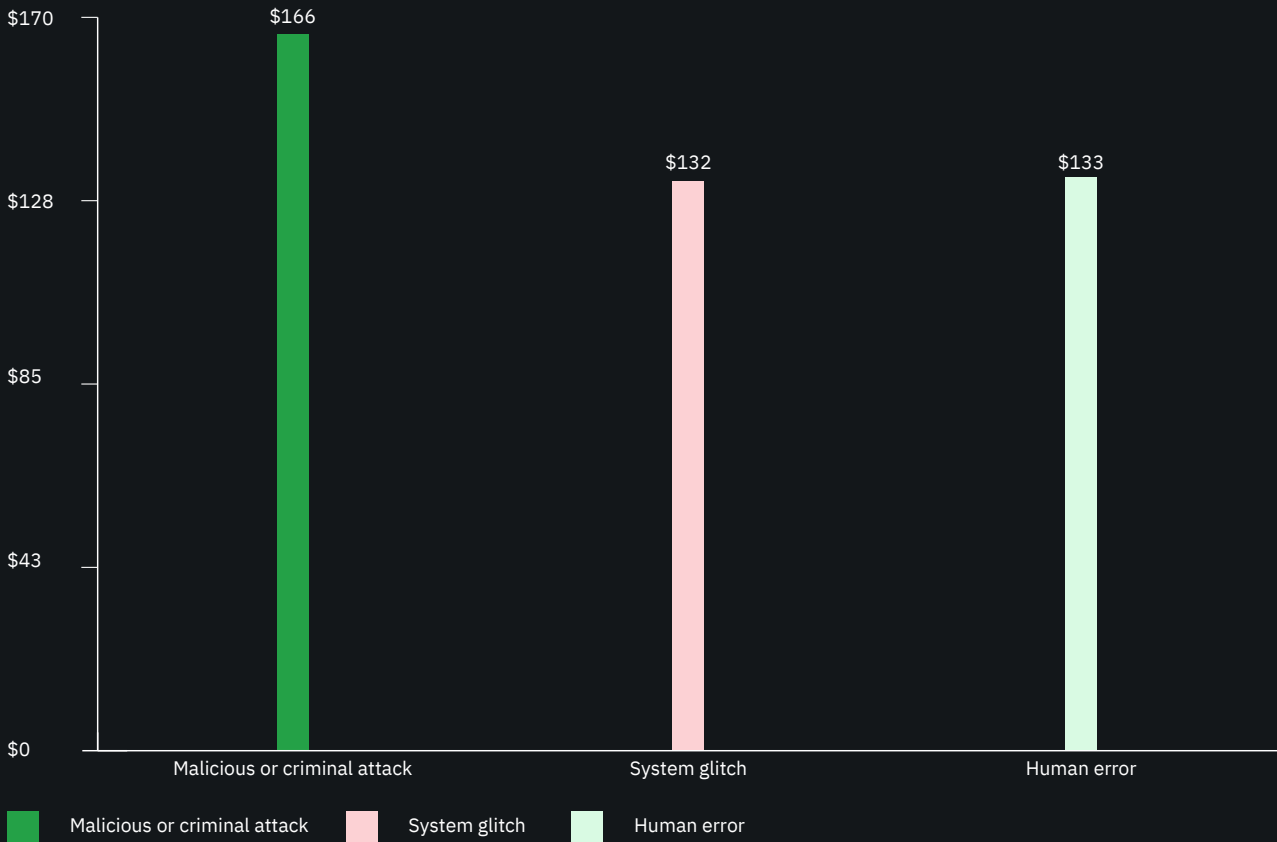
**Malicious or criminal attacks were
the costliest.**

Figure 14 reports the per record cost of a data breach
for three root causes. In the 2019 study, the cost of data
breaches due to malicious or criminal attacks was $166
per record. This is approximately 25 percent higher
than the per record cost for breaches caused by system
glitches and human error, which were $132 and $133,
respectively.

Figure 15:

Total cost for three data breach root causes

Measured in US$ millions

|		
▢ Malicious or criminal attack	▢ System glitch	▢ Human error
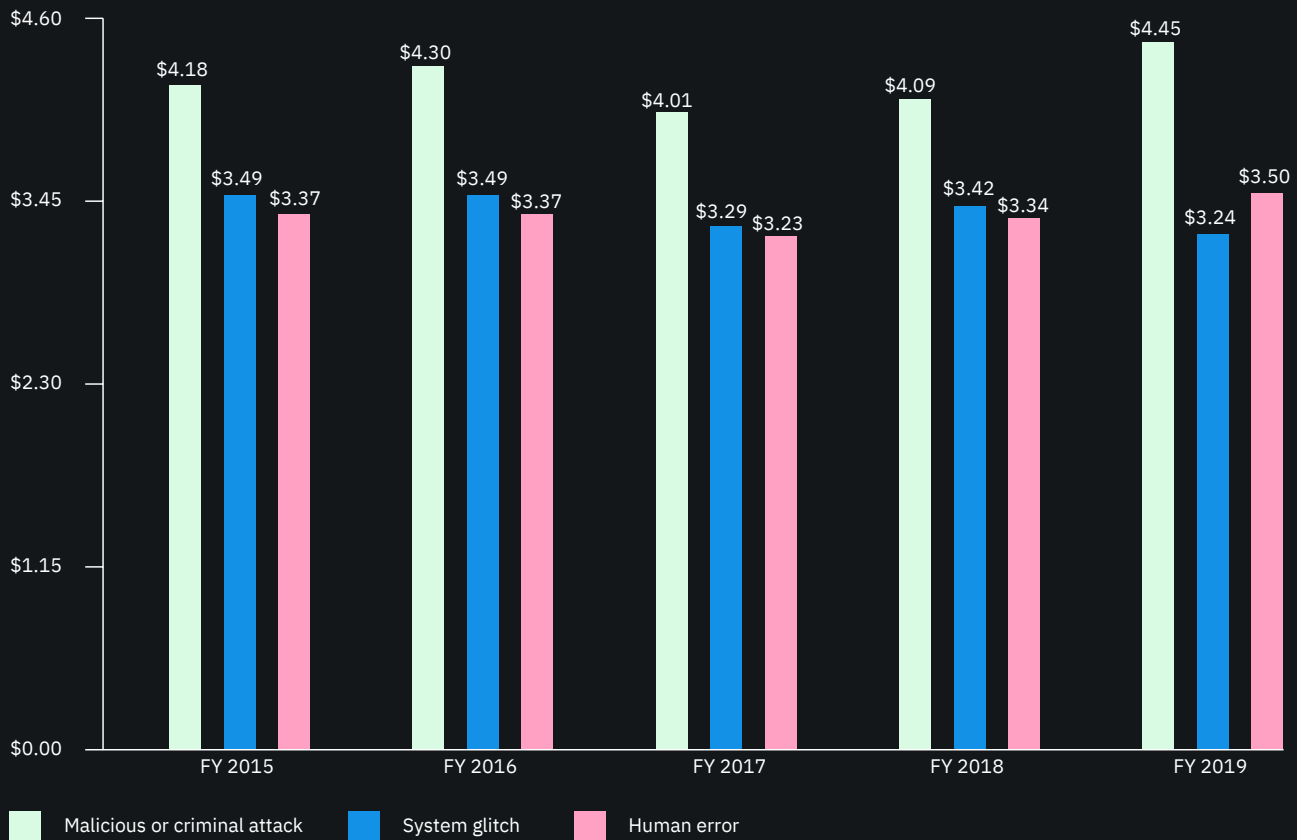
Costs from three root causes have been consistent over time.

Figure 15 shows the average total cost for three data breach root causes. Over the five-year period of the 2014 to 2019 studies, the pattern of root causes has stayed fairly constant. Consistently, malicious or criminal attacks were the most costly type of attack.

Figure 16:

Growth in malicious or criminal attacks as root cause of breaches

Malicious attacks share of all breaches
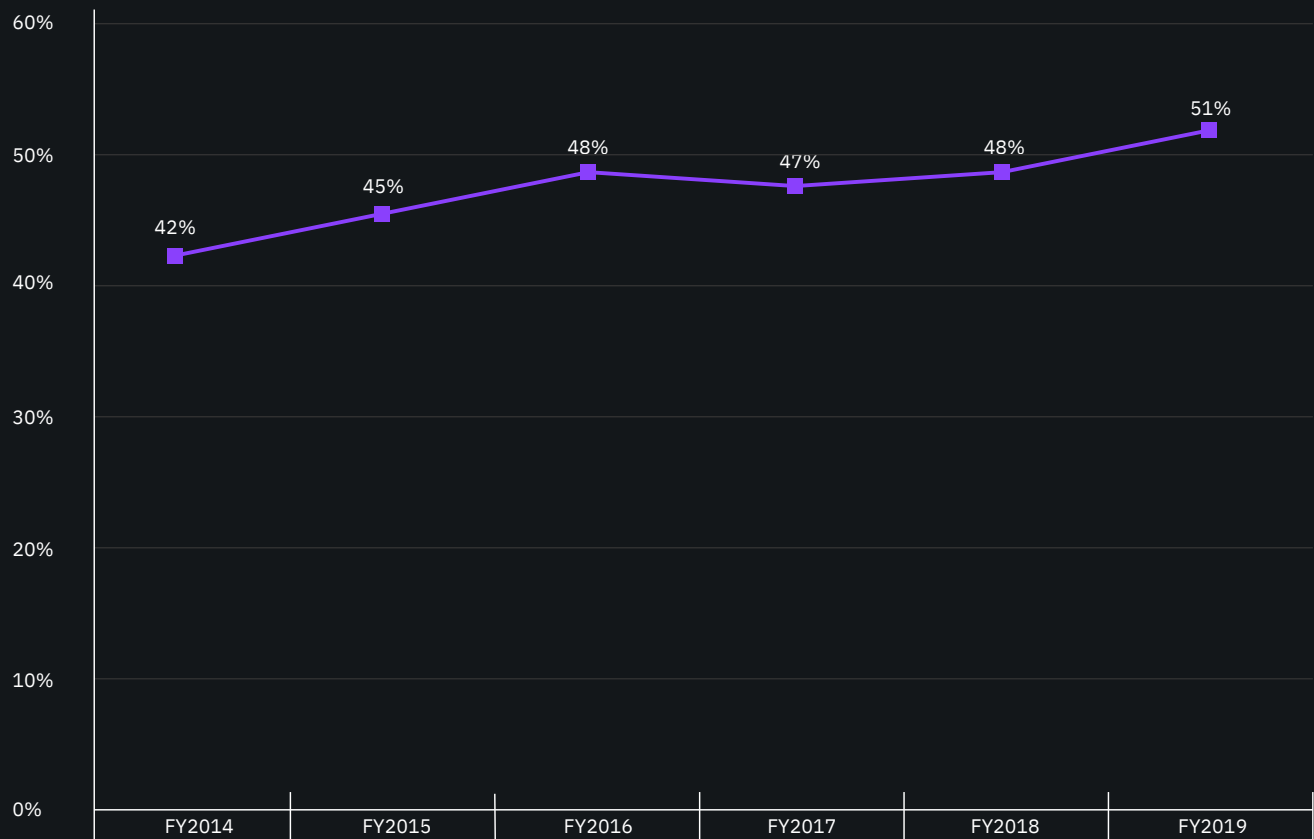
Malicous attacks continued to increase.

According to **Figure 16,** since the 2014 study, the share of breaches caused by malicious and criminal attacks has grown from 42 percent to 51 percent. In other words, between the 2014 and 2019 studies, the share of breaches caused by malicious or criminal attacks grew by 21 percent.

The four cost components

Our study looked 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 four cost centers are:

Detection and escalation

Activities that enable a company to detect the breach and report it to appropriate personnel.

Post data breach response

Processes set up to help customers communicate with the company (e.g., call centers), as well as costs associated with redress and reparation.

Notification

Activities that enable the company to notify individuals who had data compromised in the breach and regulators.

Lost business

Activities associated with cost of lost business including revenue loss, business disruption, system downtime, and new customer acquisition.

Key findings:

The cost of lost business averaged $1.42 million, or 36 percent of the total cost of a data breach for companies studied.

Lost business has consistently been the largest cost factor from the 2015 to 2019 studies, but has declined slightly as a share of the total cost.

$1.42^M   or   36%

The cost of lost business averaged $1.42 million

36 percent of the total cost of a data breach

Figure 17:

Data breach total cost broken down into four cost categories

Measured in US$ millions

Detection & escalation

Notification

Post breach cost

Lost business cost

Total cost
$3.92M

$1.22
(31.1%)

$0.21
(5.4%)

$1.07
(27.3%)

$1.42
(36.2%)
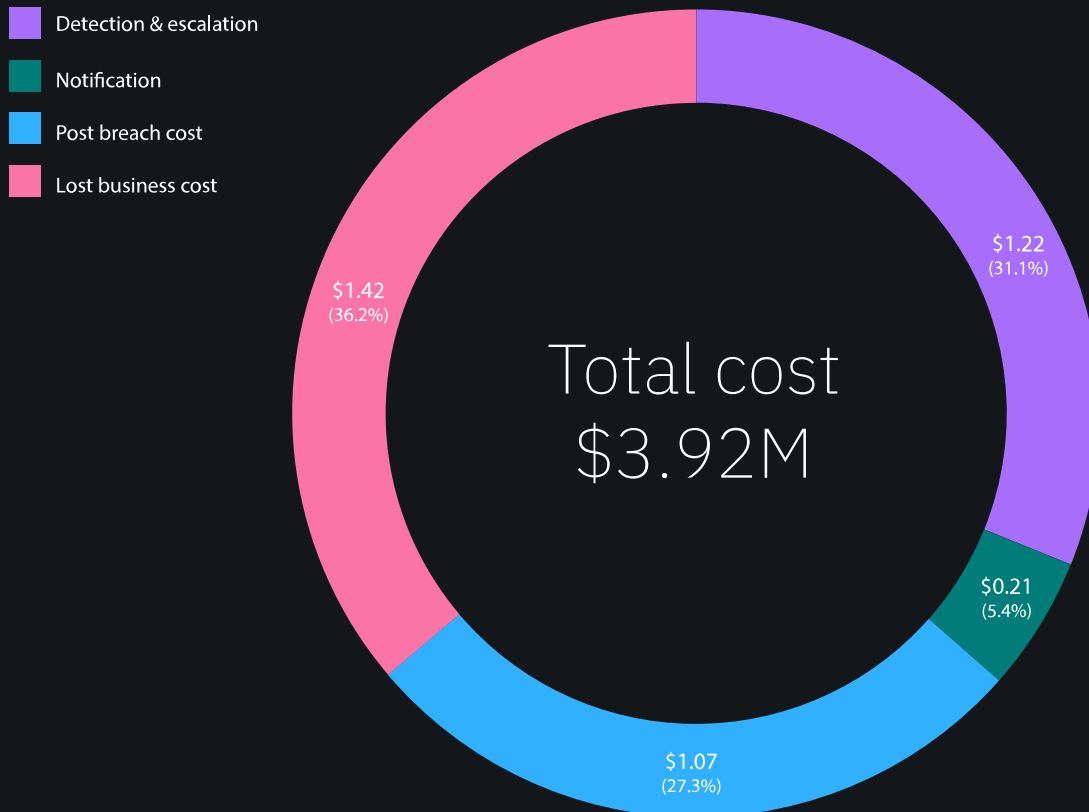
Lost business was the biggest of four cost factors.

Figure 17 shows the four cost categories or centers that were used to determine the cost of a data breach. The most costly component was lost business followed by detection and escalation.

Figure 18:
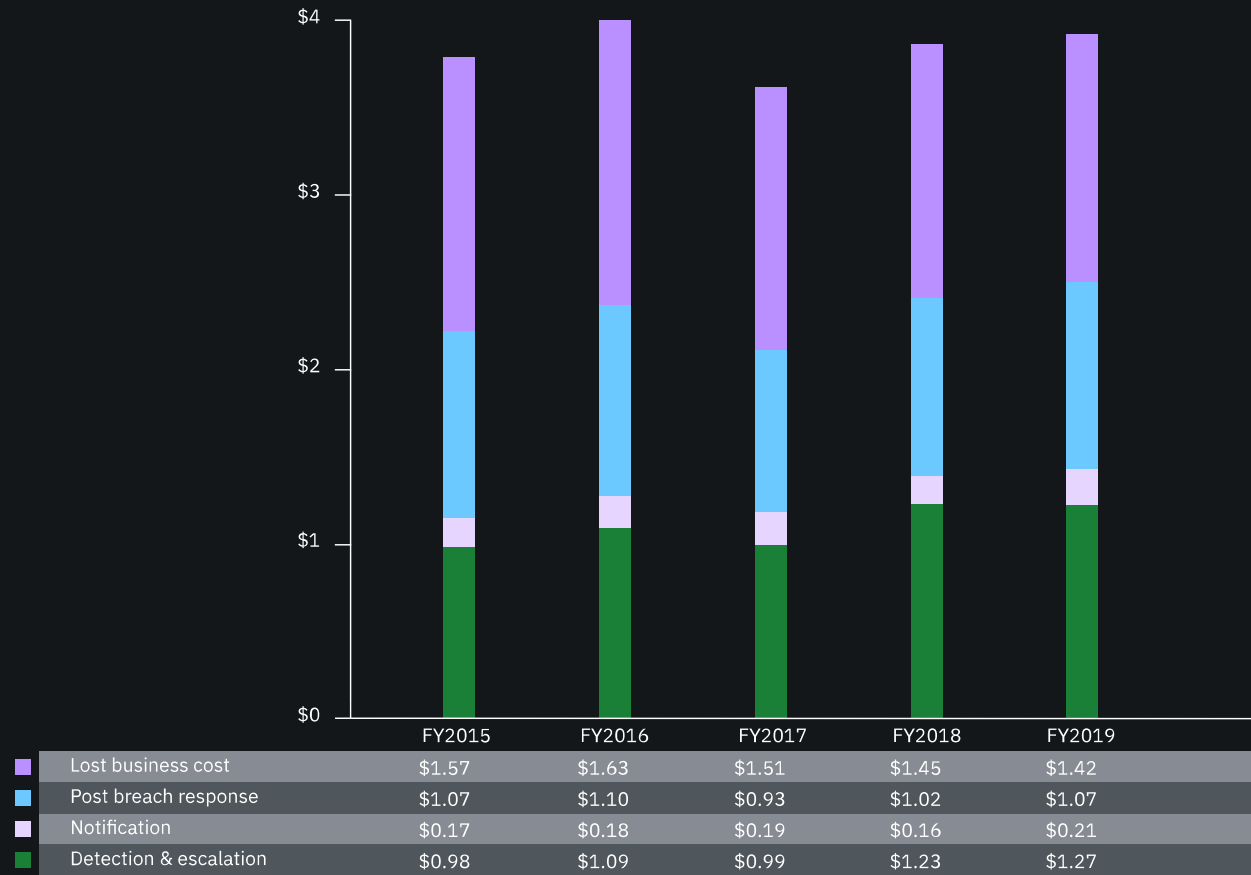
Data breach components average total cost

Measured in US$ millions

		FY2015	FY2016	FY2017	FY2018	FY2019
▪	Lost business cost	$1.57	$1.63	$1.51	$1.45	$1.42
▪	Post breach response	$1.07	$1.10	$0.93	$1.02	$1.07
▪	Notification	$0.17	$0.18	$0.19	$0.16	$0.21
▪	Detection & escalation	$0.98	$1.09	$0.99	$1.23	$1.27

Lost business cost consistently stayed the highest cost component for five years.

Figure 18 presents the trend in the average total cost of the cost components from the 2015 to 2019 studies. As shown, the financial consequences of losing customers were the most severe.

Factors that influence cost

Factors from the make-up of the security team an organization has in place, to the complexity of the IT environment, tended to influence the cost of a data breach. In our cost analysis, we looked at 26 factors and how much they increased or decreased the cost of a data breach. Four new factors were included in this year's cost analysis: (1) extensive tests of the incident response plan, (2) using a DevSecOps approach, (3) OT infrastructure and (4) system complexity.

Key findings:

The formation of the incident response (IR) team and extensive tests of the IR plan reduced the average total cost by as much as $360,000 and $320,000, respectively.

$360,000

IR team reduced total cost by $360,000

$320,000

Testing the IR plan reduced total cost by $320,000

Automation technologies, including artificial intelligence and automation in incident response orchestration, were also major factors that reduce the total cost.

A DevSecOps approach that instills security testing and design into the development process saved $10.55 per compromised record, while system complexity increased costs by $10.96 per record.

$10.55

Development process saved $10.55 per compromised record

$10.96

System complexity increased costs by $10.96 per record

Cloud and digital transformation increased the the total cost of a data breach. Extensive cloud migration, extensive use of mobile platforms, and extensive use of IoT devices were all significant cost.

Figure 19:

Factors impacting the per record cost of a data breach

Change in US$ from average global cost per record of US $150

Factor	Value
Formation of the IR team	(13.66)
Extensive use of encryption	(13.59)
Extensive tests of the IR plan	(12.25)
Business continuity management	(10.56)
DevSecOps approach	(10.55)
Employee training	(10.31)
Participation in threat sharing	(9.27)
Artificial intelligence platform	(8.97)
Use of security analytics	(7.68)
Board-level involvement	(7.07)
Extensive use of DLP	(6.91)
CISO appointed	(6.85)
Insurance protection	(6.05)
Data classification schema	(5.11)
CPO appointed	(2.08)
Identity theft protection	(0.56)
Consultants engaged	4.17
Rush to notify	5.61
Extensive use of IoT devices	5.95
Lost or stolen devices	6.75
Extensive use of mobile platforms	9.33
OT infrastructure	10.09
System complexity	10.96
Extensive cloud migration	11.39
Compliance failures	13.47
Third-party breach	14.04

Axis: (16.00) — (8.00) — 0 — 8.00 — 16.00

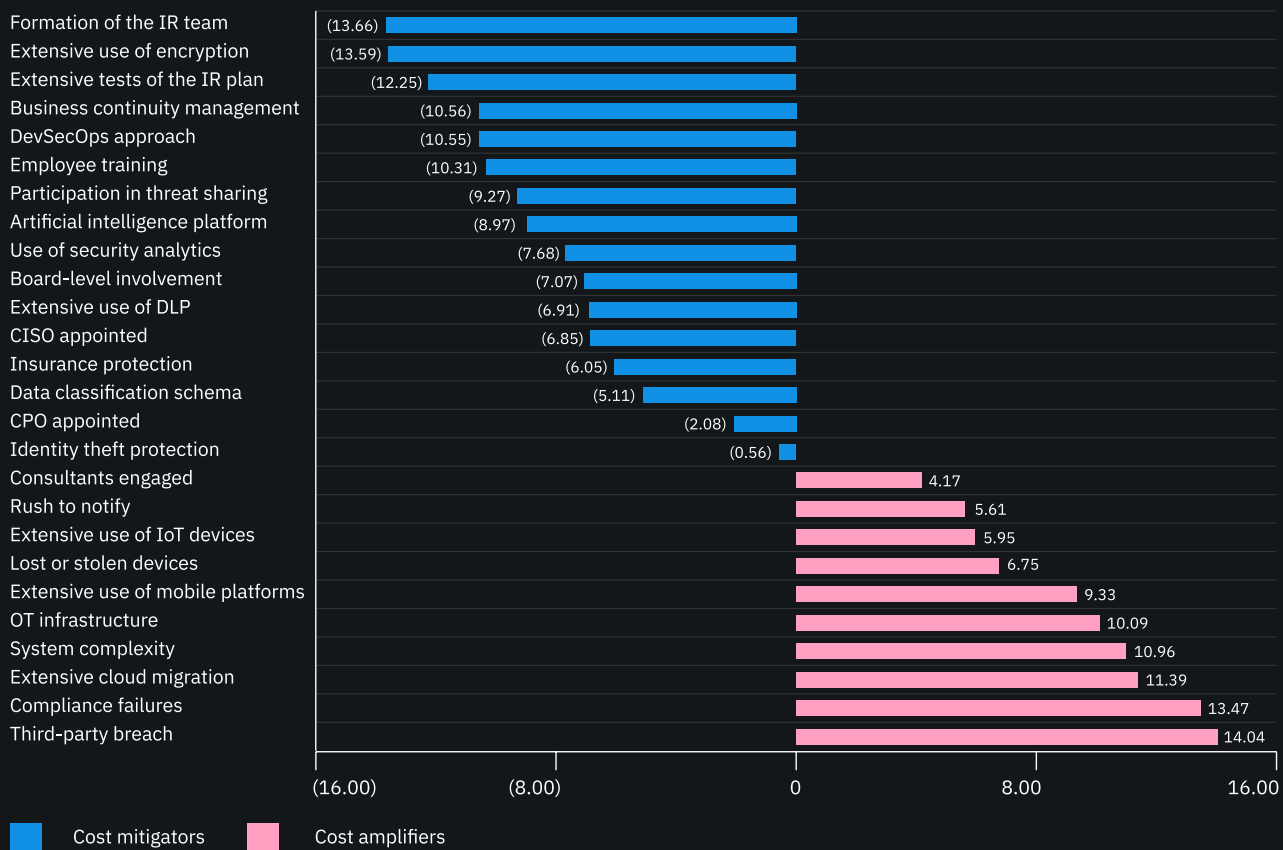■ Cost mitigators   ■ Cost amplifiers

Figure 19 provides a list of the 26 factors studied and how they impacted the per record cost of a data breach, showing those that decreased (cost mitigators) or increased (cost amplifiers) the per record cost of $150.

Figure 20:

How factors increased or decreased the total cost of a data breach

Difference from average total cost of US $3.92 million

Factor	Value
Formation of the IR team	-$360,000
Extensive use of encryption	-$360,000
Extensive tests of the IR plan	-$320,000
Business continuity management	-$280,000
DevSecOps approach	-$280,000
Employee training	-$270,000
Participation in threat sharing	-$240,000
Artificial intelligence platform	-$230,000
Use of security analytics	-$200,000
Board-level involvement	-$180,000
Extensive use of DLP	-$180,000
CISO appointed	-$180,000
Insurance protection	-$160,000
Data classification schema	-$130,000
CPO appointed	-$50,000
Identity theft protection	-$10,000
Consultants engaged	$110,000
Rush to notify	$150,000
Extensive use of IoT devices	$160,000
Lost or stolen devices	$180,000
Extensive use of mobile platforms	$240,000
OT infrastructure	$260,000
System complexity	$290,000
Extensive cloud migration	$300,000
Compliance failures	$350,000
Third-party breach	$370,000

■ Cost mitigators   ■ Cost amplifiers

Figure 20 shows the impact of the 26 factors studied on the total cost of a data breach, showing those that decreased (cost mitigators) or increased (cost amplifiers) the average total cost of $3.92 million.

Incident response effectiveness

An organization's ability to respond effectively after a data breach was strengthened by the presence of an incident response (IR) team that followed an incident response plan. In our research, we examined the effect of another factor: testing the IR plan through activities such as practicing a breach response using tabletop exercises and/or in a simulated environment such as a cyber range. Combined, the formation of an IR team and testing the IR plan mitigate data breach costs more than any single security process.

Key findings:

Formation of the IR team lowered the total cost of a data breach by an average of $360,000 from the mean cost of $3.92 million.

$360,000

IR team lowers the total cost of a data breach by an average of $360,000

Extensive testing of the IR plan reduced the total cost of a data breach by an average of $320,000 from the mean cost of $3.92 million.

$320,000

IR plan reduces the total cost of a data breach by an average of $320,000

Organizations that both formed an IR team and extensively tested the IR plan saw the greatest savings – $1.23 million less than organizations that neither formed an IR team or tested the IR plan.

$1.23^M

Savings from IR teams and testing the IR plan – $1.23 million less than organizations that neither formed an IR team or tested the IR plan.

Figure 21:

Combined effect of incident response team and testing the incident response plan

Total breach cost measured in US$ millions
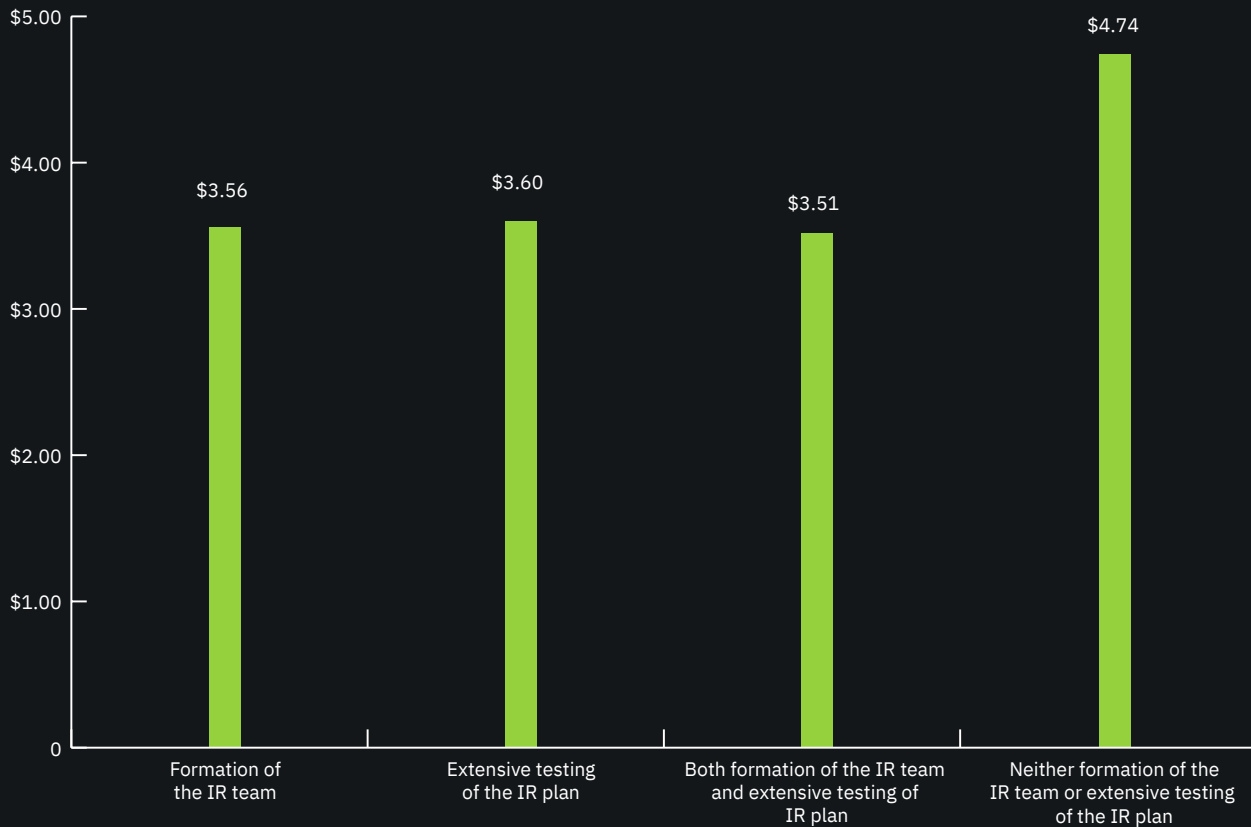
Incident response plan testing increased the cost-saving effectiveness of an incident response team.

Figure 21 shows the average total cost of a data breach under four separate conditions pertaining to the company's incident response (IR) activities, namely: (1) formation of the IR team, (2) extensive testing of the IR plan, (3) both the formation of the IR team and extensive testing, and (4) neither IR activity. Companies that formed an IR team experienced an average total cost of $3.56 million. Companies that only performed

extensive testing of the IR plan experienced a total cost of $3.60 million. Companies that both formed the IR team and performed extensive testing of the IR plan averaged a total cost of $3.51 million. In contrast, companies that neither formed an IR team or tested the IR plan had the highest total cost of data breach at $4.74 million.

The effect of abnormal customer turnover

With lost business appearing to be the biggest cost component of a data breach, our research dug down further to examine the costs associated with greater-than-expected customer turnover. The more customers lost following a breach, the higher the average total cost of a data breach.

Key findings:

The global average customer turnover rate was 3.9 percent, an increase from last year's report of customer turnover rate of 3.4 percent.

3.9%

2019 abnormal
customer turnover rate

3.4%

2018 abnormal customer
turnover rate

Healthcare, financial services and pharmaceuticals had more trouble than other industries retaining customers after a breach.

Organizations should emphasize customer retention activities to reduce total data breach costs.

Figure 22:

Average cost of a data breach by abnormal customer turnover rate

Measured in US$ millions
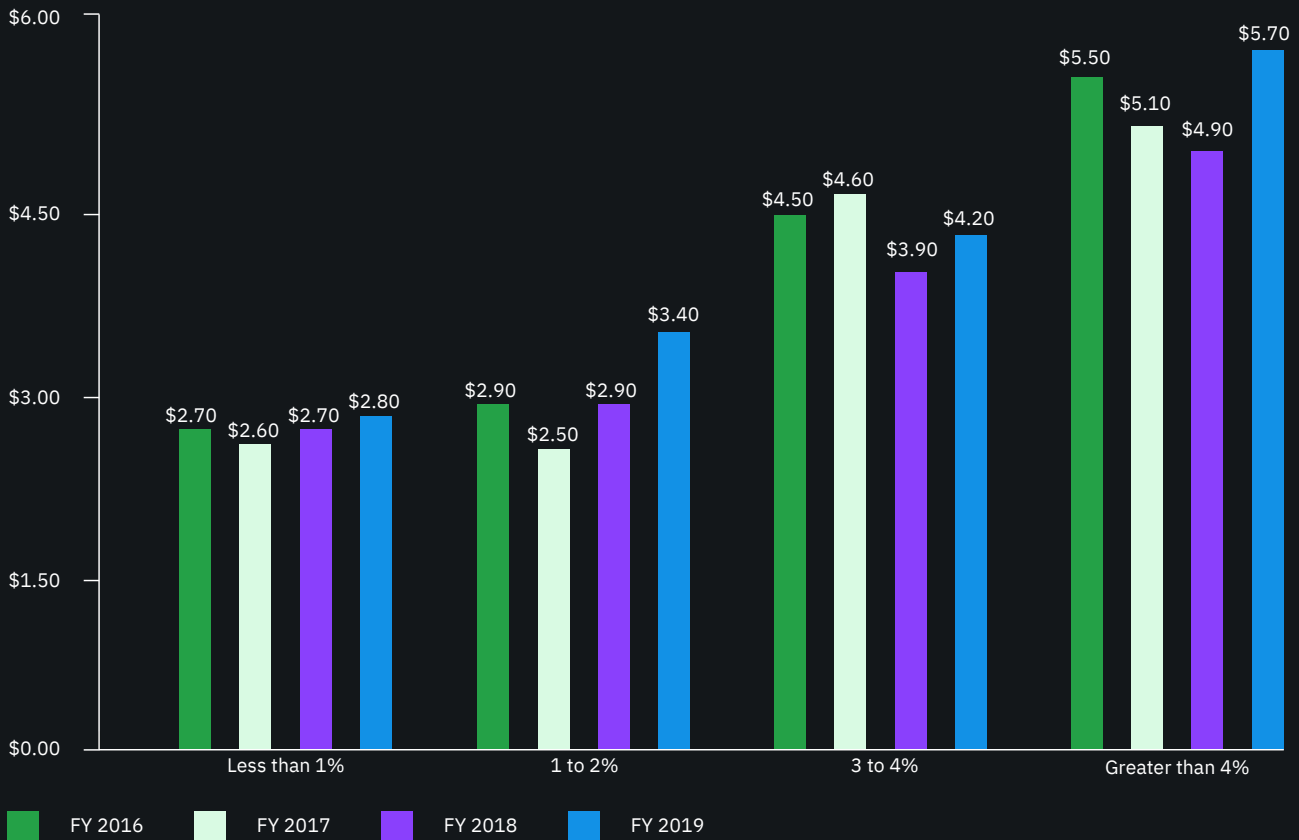
Customer turnover influence on costs varied by rate and year.

Figure 22, reports the average total cost of a data breach for four abnormal customer turnover rates, from less than one percent to more than four percent over the period of the 2016 to 2019 studies. Companies that experienced less than a one percent loss of existing customers had an average total cost of $2.8 million, vs. an average cost of $5.7 million for companies that experienced a customer turnover greater than 4 percent.

Figure 23:

Abnormal customer turnover by country or region

Global average of abnormal customer turnover = 3.9%

Country	Value
France	4.7%
Italy	4.5%
Japan	4.3%
United States	3.6%
Middle East	3.6%
Germany	3.5%
United Kingdom	3.0%
India	3.0%
Australia	2.8%
ASEAN	2.8%
South Africa	2.6%
South Korea	2.6%
Brazil	2.6%
Canada	2.4%
Turkey	2.4%
Scandinavia	2.2%

0.0%   1.3%   2.5%   3.8%   5.0%
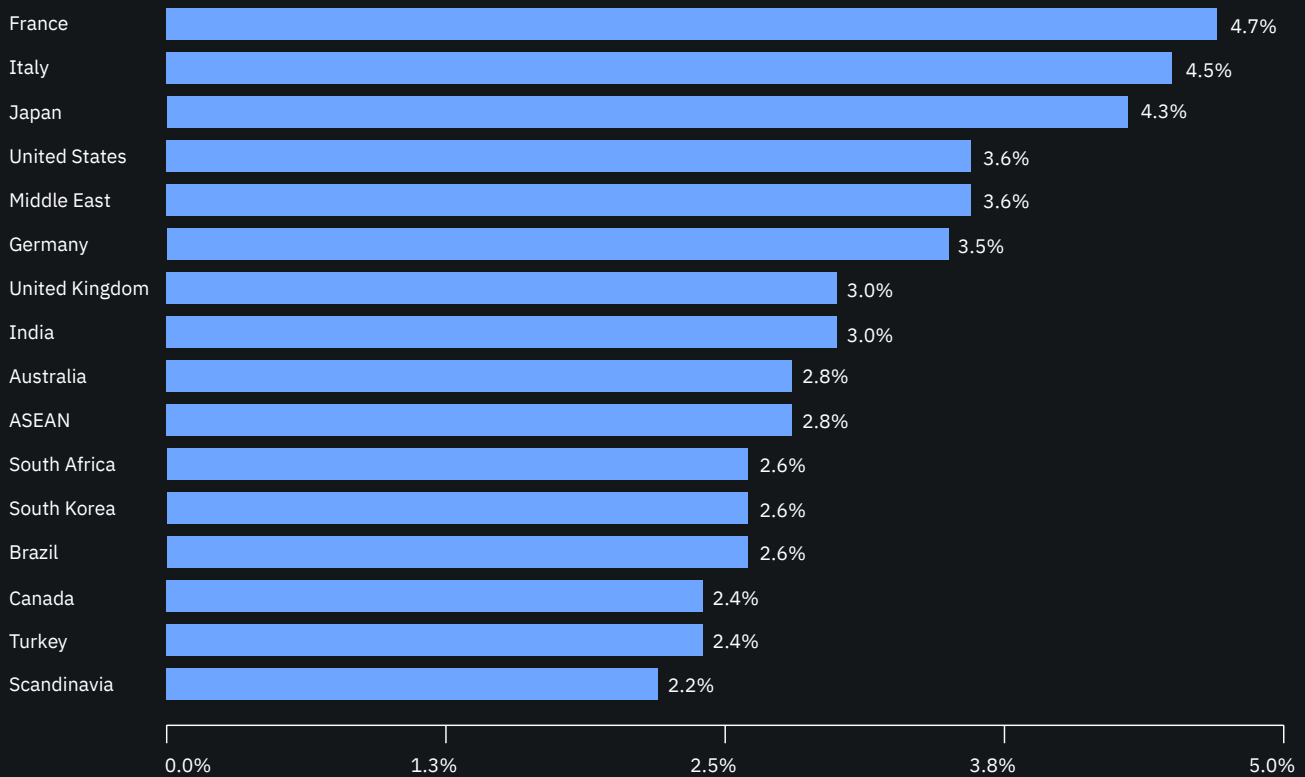
Certain countries were more vulnerable to customer turnover.

Figure 23, reports the average abnormal customer turnover rates for all country or regional samples represented in this research. Results showed marked differences among countries. France, Italy and Japan experienced the highest abnormal customer turnover rates, whereas, Scandinavia, Turkey and Canada had the lowest.

Figure 24:

Abnormal customer turnover by industry

Global average of abnormal customer turnover = 3.9%

Industry	Rate
Health	7.0%
Financial	5.9%
Pharmaceuticals	5.5%
Services	5.0%
Technology	4.9%
Industrial	3.3%
Energy	3.3%
Communication	3.1%
Consumer	2.7%
Hospitality	2.5%
Retail	2.4%
Entertainment	2.3%
Education	2.2%
Transportation	2.1%
Research	1.9%
Media	1.8%
Public	0.4%

0.0%   1.8%   3.5%   5.3%   7.0%
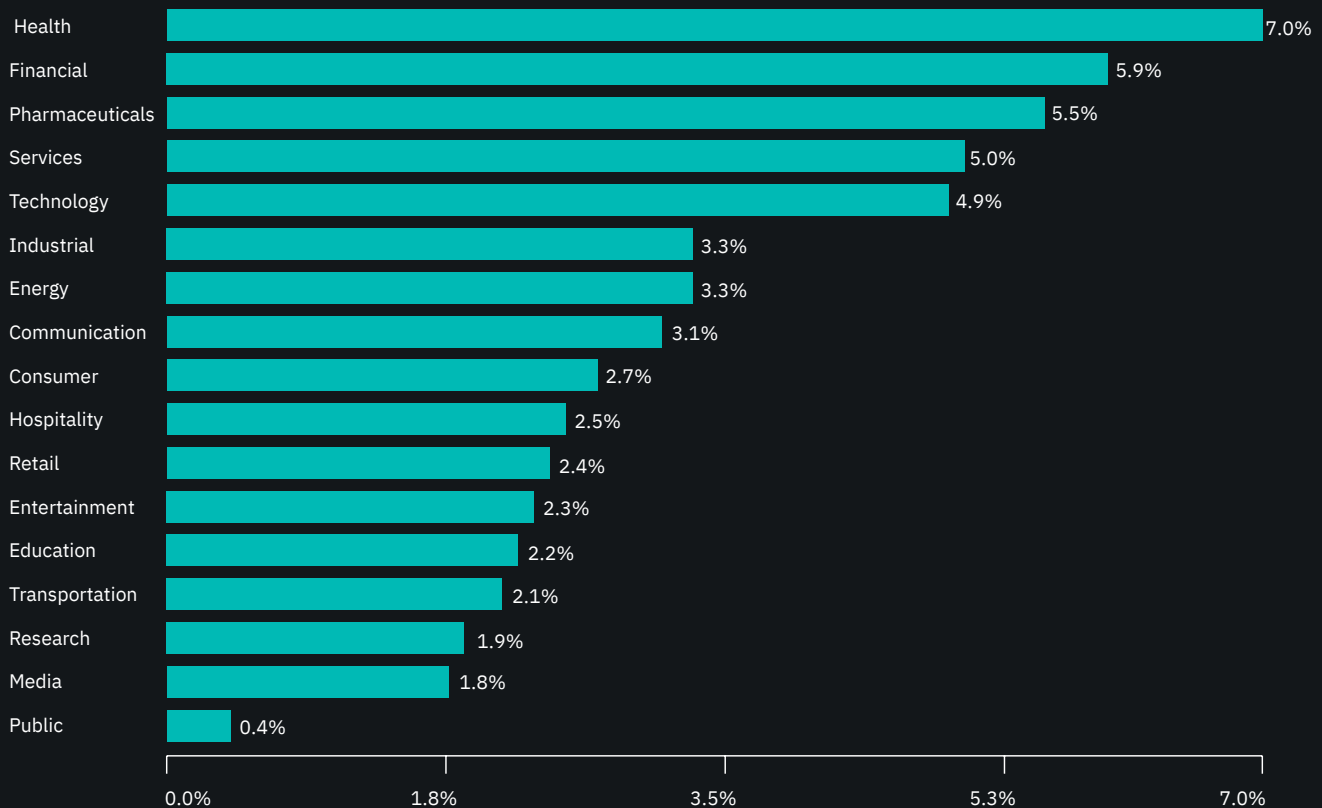
Healthcare, financial services and pharmaceuticals had difficulty retaining customers following a data breach.

Figure 24, reports the abnormal customer turnover rate of 17 industries. The small sample size in this research prevents us from generalizing the effect of industry on customer turnover rates. However, health, financial, pharmaceutical and service organizations experienced much higher than the average 3.9 percent rate of abnormal customer turnover. In contrast, public sector, media and transportation organizations experienced a relatively low abnormal customer turnover.[8]

Companies in certain industries appear to be more vulnerable to turnover when customers could easily take their business to another competitor. Customers seem to be more willing to take their business elsewhere in highly regulated industries, such as healthcare and financial services. In contrast, the public sector, which had the lowest customer turnover, generally has no competitors, leaving customers without other options.

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

The likelihood an organization will have another data breach

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.

Key findings:

29.6%

Companies studied estimated the probability of experiencing a data breach in the next two years at 29.6 percent

31%

The estimated probability of a data breach within two years has grown by 31 percent from 2014 to 2019

1.2%

The likelihood of a data breach steadily decreased as the number of breached records increased; there is a 1.2 percent chance of a breach involving 100,000 records in the next two years

Figure 25:

Probability of a data breach in the next two years

Minimum of 10,000 records
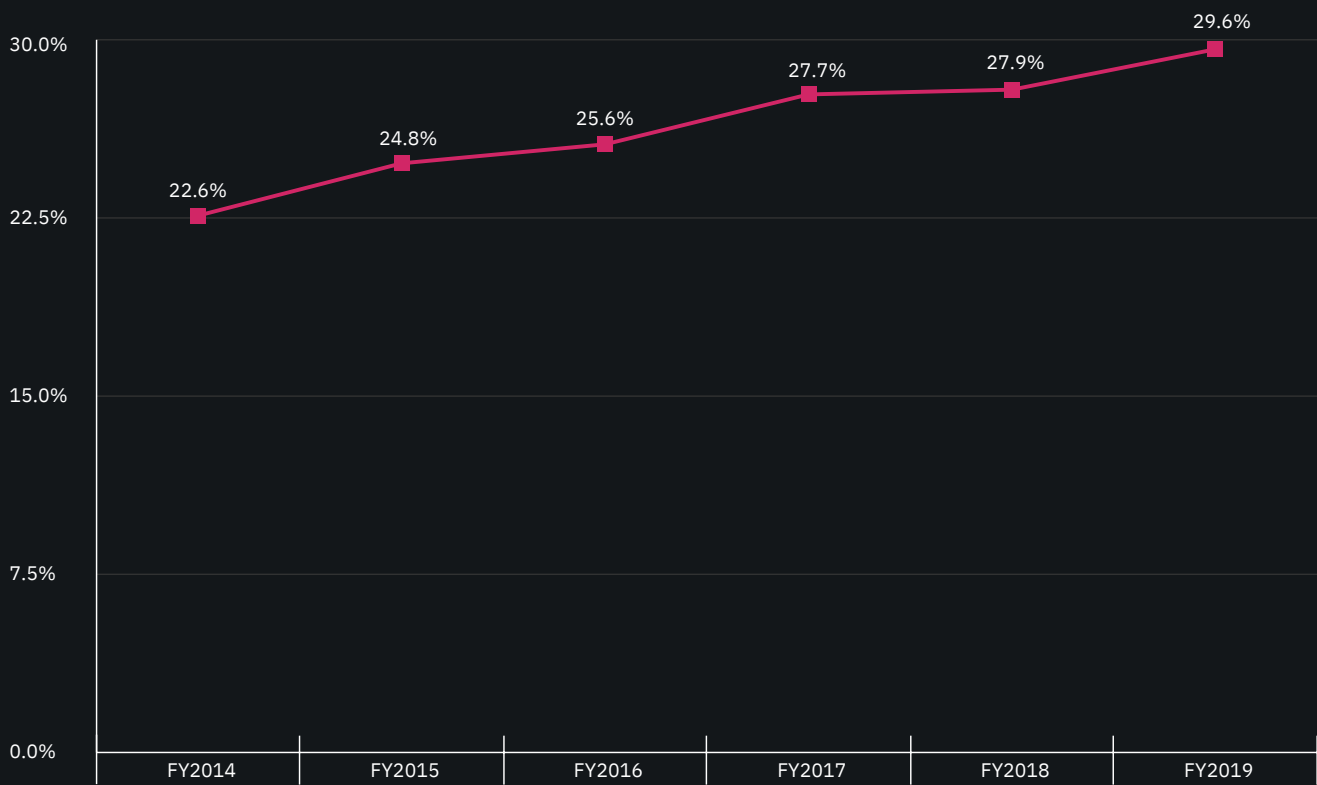
The likelihood of experiencing a data breach grew.

Figure 25, shows the percentage chance of experiencing a data breach within two years has increased from 22.6 percent in 2014 to 29.6 percent in 2019. The difference from 2014 to 2019 represents a 31 percent growth rate in the likelihood of experiencing a breach within two years.

Figure 26:

Probability of a data breach by number of records lost

Over the next two years, involving minimum of 10,000 and maximum of 100,000 records
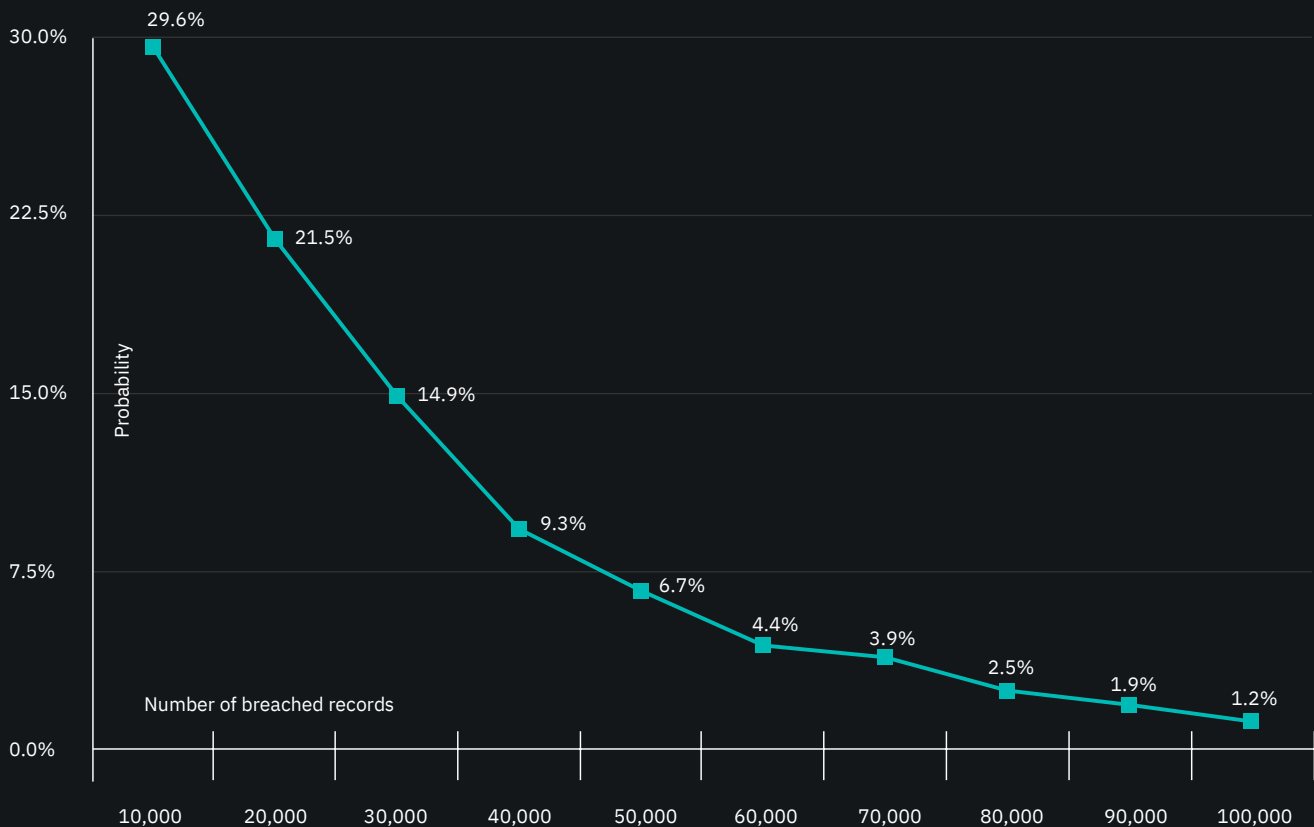
Data breaches involving large numbers of records may be less likely.

Figure 26, shows the subjective probability distribution of data breach incidents involving a minimum of 10,000 and a maximum of 100,000 compromised records over the 24 month time period following the interviews.[9] 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 29.6 percent over a 24-month period. The chance of a data breach involving a minimum of 100,000 records is estimated at approximately 1.2 percent.

[9]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 after the interview. An aggregated probability distribution was extrapolated for each one of the 507 participating companies.

The data breach lifecycle

This research looks at the time elapsed between when an organization is breached and the time the breach is contained, referred to as the breach lifecycle. This lifecycle is broken down into the mean time to identify (MTTI) and mean time to contain (MTTC) metrics, which can be used to determine the effectiveness of an organization's incident response and containment processes. We also examined the relationship between the lifecycle of a breach and its total cost.

Key findings:

The lifecycle of a data breach in the 2019 study was 279 days, 4.9 percent longer than the 2018 lifecycle of 266 days

279days

lifecycle of a
data breach in 2019

4.9%

2019 lifecycle is 4.9 percent longer than the 2018 lifecycle of 266 days

The lifecycle of a breach caused by a malicious attack was 314 days, 12.5 percent longer than the average lifecycle

314days

lifecycle of a breach caused by a malicious attack

12.5%

longer than the average lifecycle

A breach with a lifecycle longer than 200 days was 37 percent more expensive than a breach with a lifecycle shorter than 200 days ($4.56 million vs. $3.34 million)

$4.56M vs $3.34M

Cost of a breach with lifecycle longer than 200 days

Cost of a breach with lifecycle shorter than 200 days

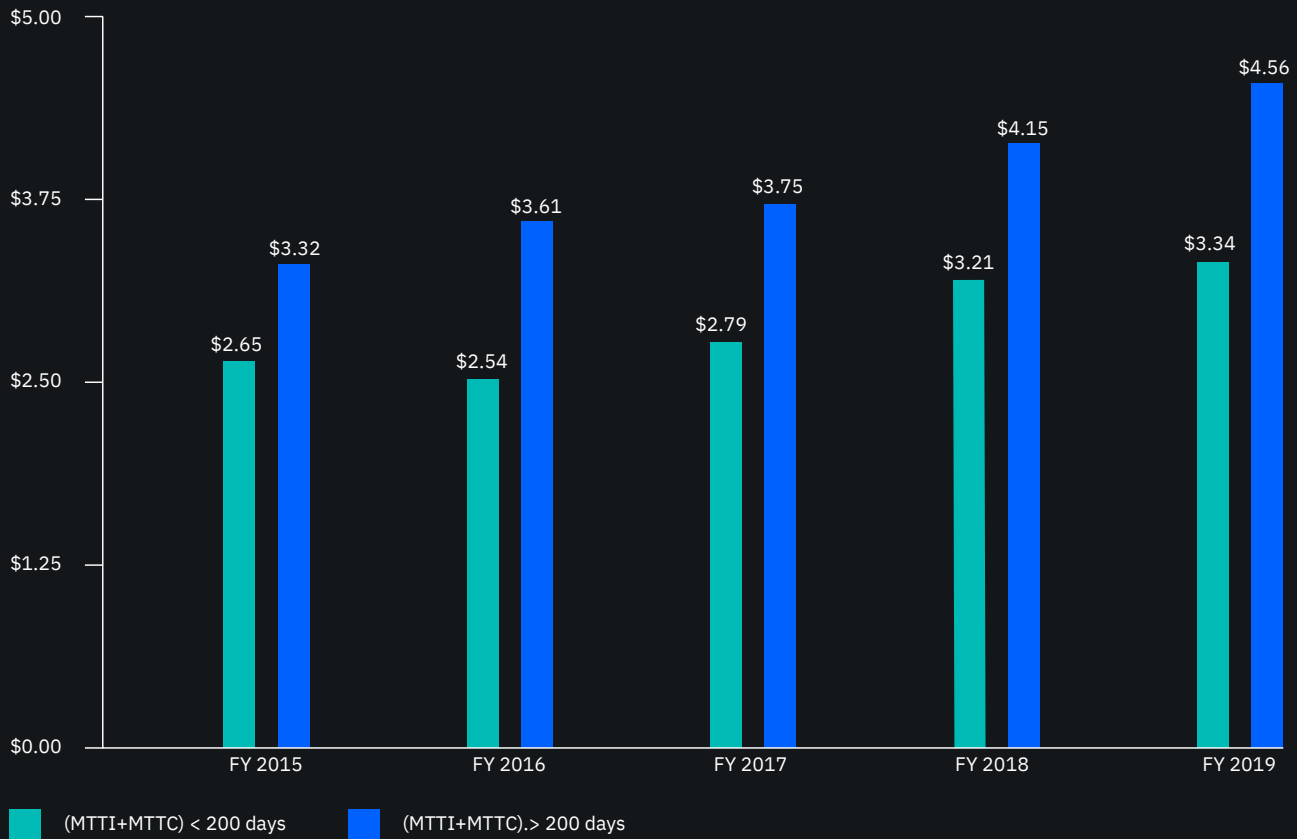**Figure 27:**

Days to identify and contain a data breach

	Mean time to identify (MTTI)	Mean time to contain (MTTC)
FY2019	206	73
FY2018	197	69
FY2017	191	66
FY2016	201	70
FY2015	206	69

07   5   150   225   300

■ Mean time to identify (MTTI)   ■ Mean time to contain (MTTC)
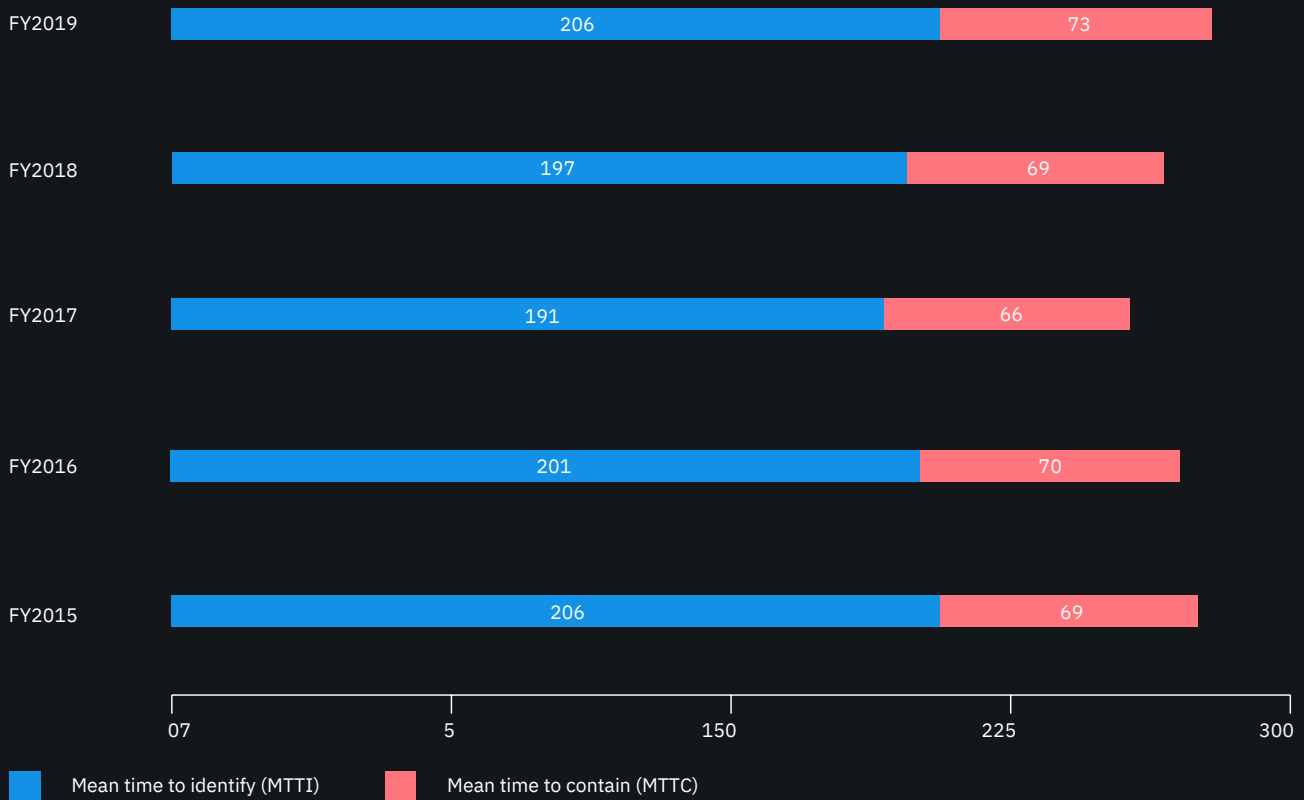
The faster a data breach was identified and contained, the lower the costs.

Figure 27, shows that, since the 2018 study the MTTI and MTTC of a data breach increased. In this year's study, the MTTI was 206 days and the MTTC was 73 days for a combined 279 days, an increase of 4.9 percent from last year's study when the MTTI and MTTC were 197 and 69 days (combined 266 days), respectively.

Figure 28:

Relationship between total cost of a breach and duration of data breach lifecycle

Measured in US$ millions

Legend:
- (MTTI+MTTC) < 200 days
- (MTTI+MTTC).> 200 days

The duration of the data breach lifecycle related to cost.

Figure 28, shows that organizations that have a lifecycle of more than 200 days had a much higher cost. It is also evident that the cost of a data breach has steadily increased over time.

Figure 29:

Days to identify and contain data breach incidents by root cause

Malicious or criminal attack	230	84
System glitch	181	62
Human error	181	61

0   100   200   300   400

■ Mean time to identify (days)   ■ Mean time to contain (days)
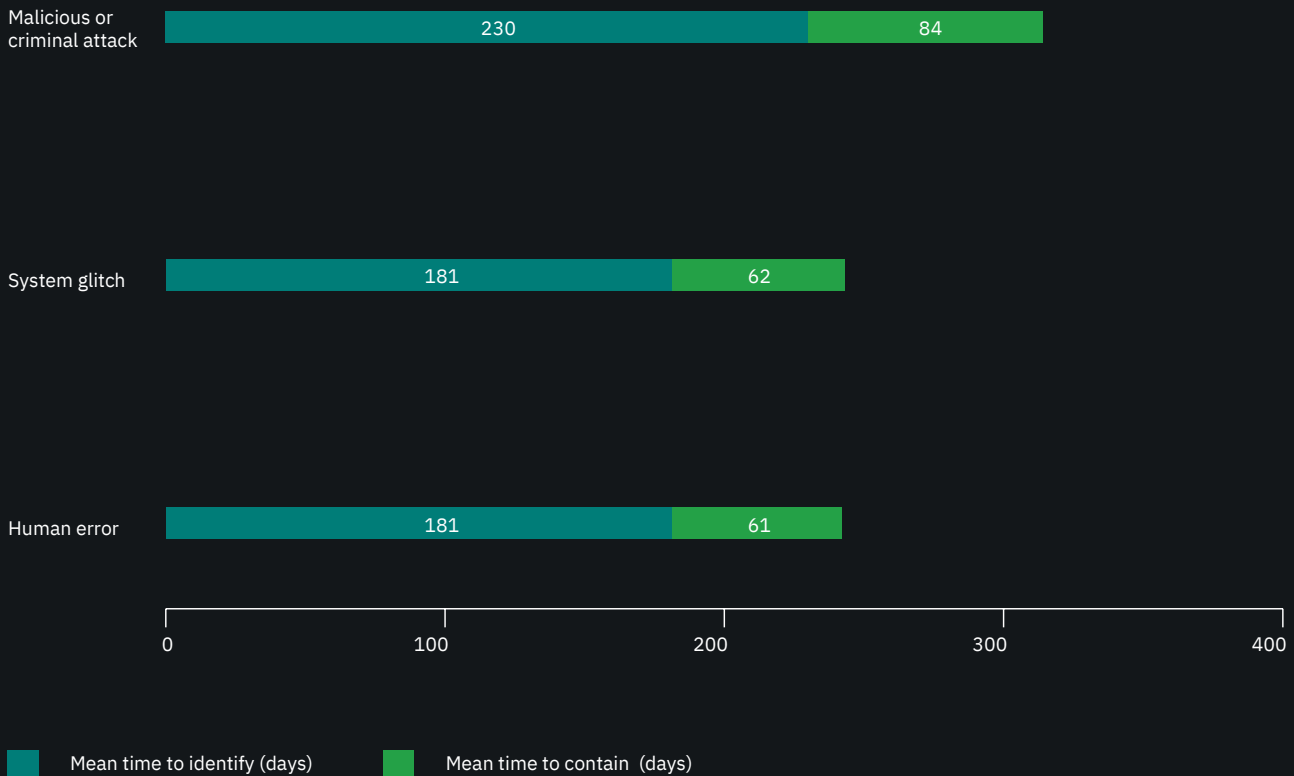
A data breach caused by a malicious or criminal attack takes much longer to identify and contain.

Figure 29, shows how the data breach lifecycle of a malicious or criminal attack in the 2019 report took an average of 314 days. In contrast, a breach caused by system glitch or human error was faster to resolve, in 243 and 242 days, respectively.

Figure 30:

Days to identify and contain data breach incidents by by country or region

Mean MTTI = 206 days; Mean MTTC = 73 days

	Mean time to identify	Mean time to contain
Middle East	279	102
Brazil	250	111
France	225	87
Japan	232	79
Turkey	216	90
Scandinavia	225	74
India	221	77
South Korea	216	71
Italy	213	70
Australia	200	81
ASEAN	190	69
United States	196	49
United Kingdom	171	72
Canada	176	65
South Africa	175	56
Germany	131	39

■ Mean time to identify   ■ Mean time to contain
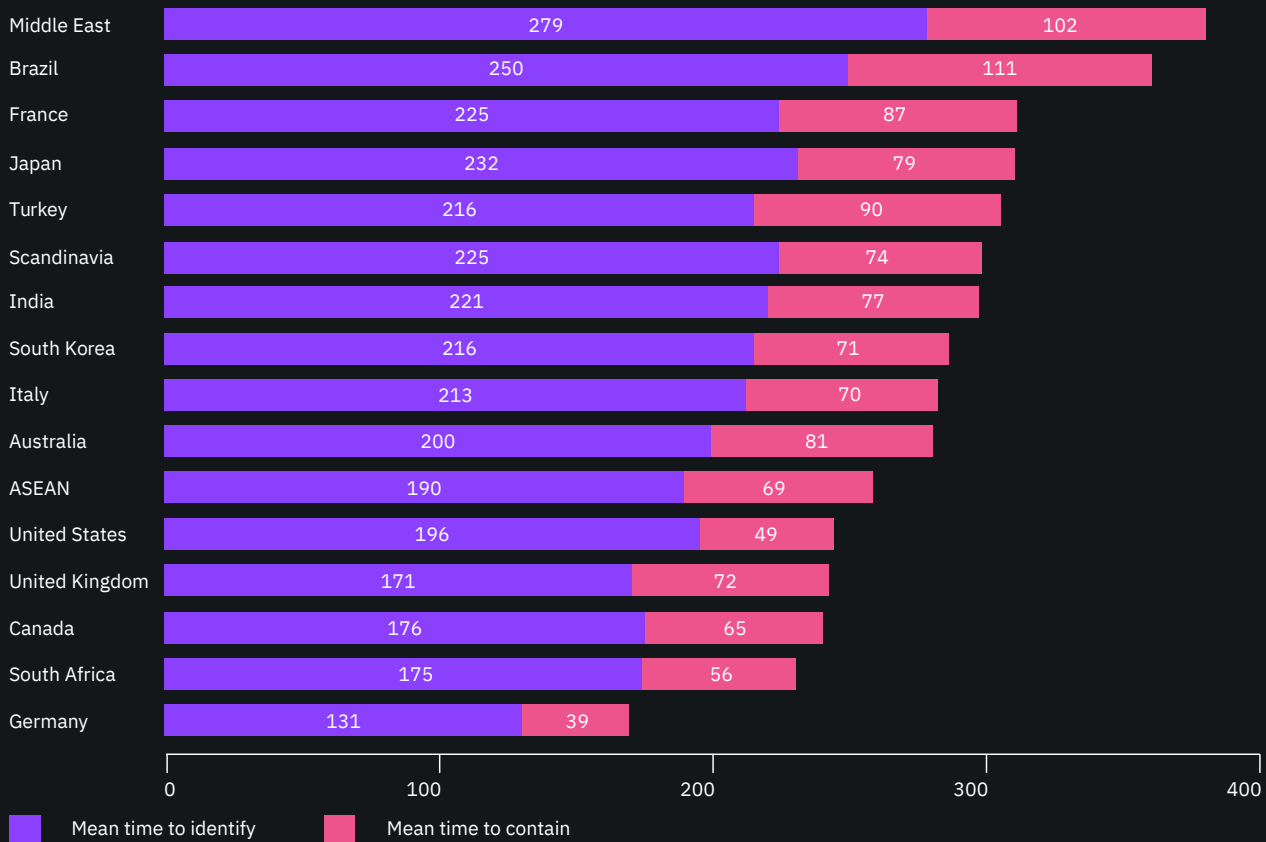
There were big regional differences in the data breach lifecycle.

Figure 30, shows that organizations in the Middle East and Brazil took the most time in the data breach lifecycle, at 381 days and 361 days, respectively. German organizations took far less time to identify and contain a data breach (170 days).

Figure 31:

Days to identify and contain a data breach by industry sector

Mean MTTI = 206 days; Mean MTTC = 73 days

Industry	Mean time to identify	Mean time to contain
Health	236	93
Public	231	93
Entertainment	224	90
Retail	228	83
Consumer	226	81
Industrial	220	82
Services	210	76
Education	212	71
Media	201	80
Transportation	203	72
Hospitality	200	75
Pharmaceuticals	191	66
Energy	197	57
Communication	191	60
Technology	187	59
Research	187	57
Financial	177	56

■ Mean time to identify   ■ Mean time to contain

There were also significant industry differences in the data breach lifecycle.

Figure 31, shows that organizations in the healthcare and public sector took the most time in the data breach lifecycle, 329 days and 324 days, respectively. Financial organizations took far less time to identify and contain a data breach (233 days).

Long tail costs

The consequences of a data breach lingered long after the incident, in a sample of 86 companies whose costs were estimated over multiple years after experiencing a breach. According to this analysis, an average of 67 percent of the costs of a data breach were incurred within the first year. However, 22 percent of costs were incurred in the second year and 11 percent of costs occured more than two years after a data breach. Organizations in high regulatory environments experienced a longer tail of costs: 53 percent in the first year, 31 percent in the second year and 16 percent more than two years after the incident.

Key findings:

About two-thirds of the cost of a data breach occured in the first year for 86 of the companies studied

67%
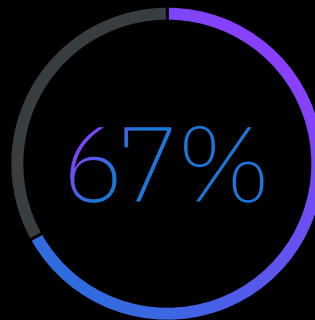
But in highly-regulated environments, just over half of breach costs occured in the first year for 86 of the companies studied

53%
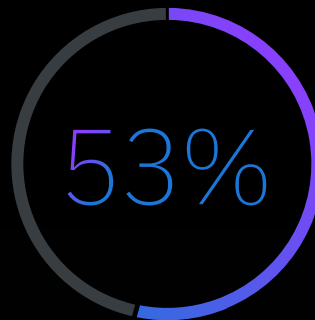
Figure 32:

Distribution of total data breach costs over time

Time elapsed	Pct %
Year 1	67%
Year 2	22%
> 2 years	11%
Total	100%
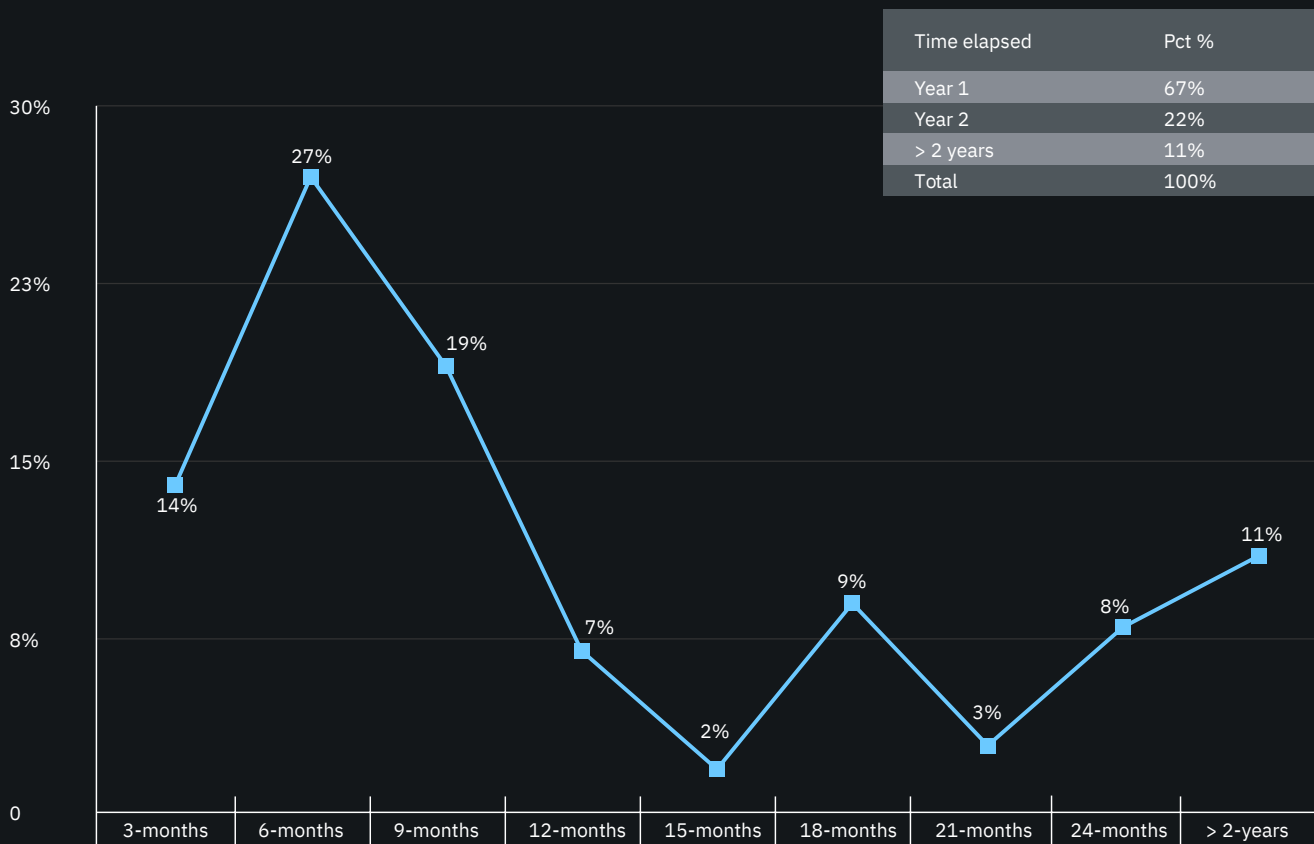
The first year was the worst year.

Figure 32, shows that data breach costs dropped off substantially after the first year for 86 of the companies studied, but 22 percent of the costs occured in the second year after a breach and 11 percent of costs came more than two years after a breach.

Figure 33:

Distribution of total breach costs over time for low and high regulatory environments

Time elapsed	Low	High
Year 1	81%	53%
Year 2	14%	31%
> 2 years	5%	16%
Total	100%	100%

Low regulatory environment   High regulatory environment
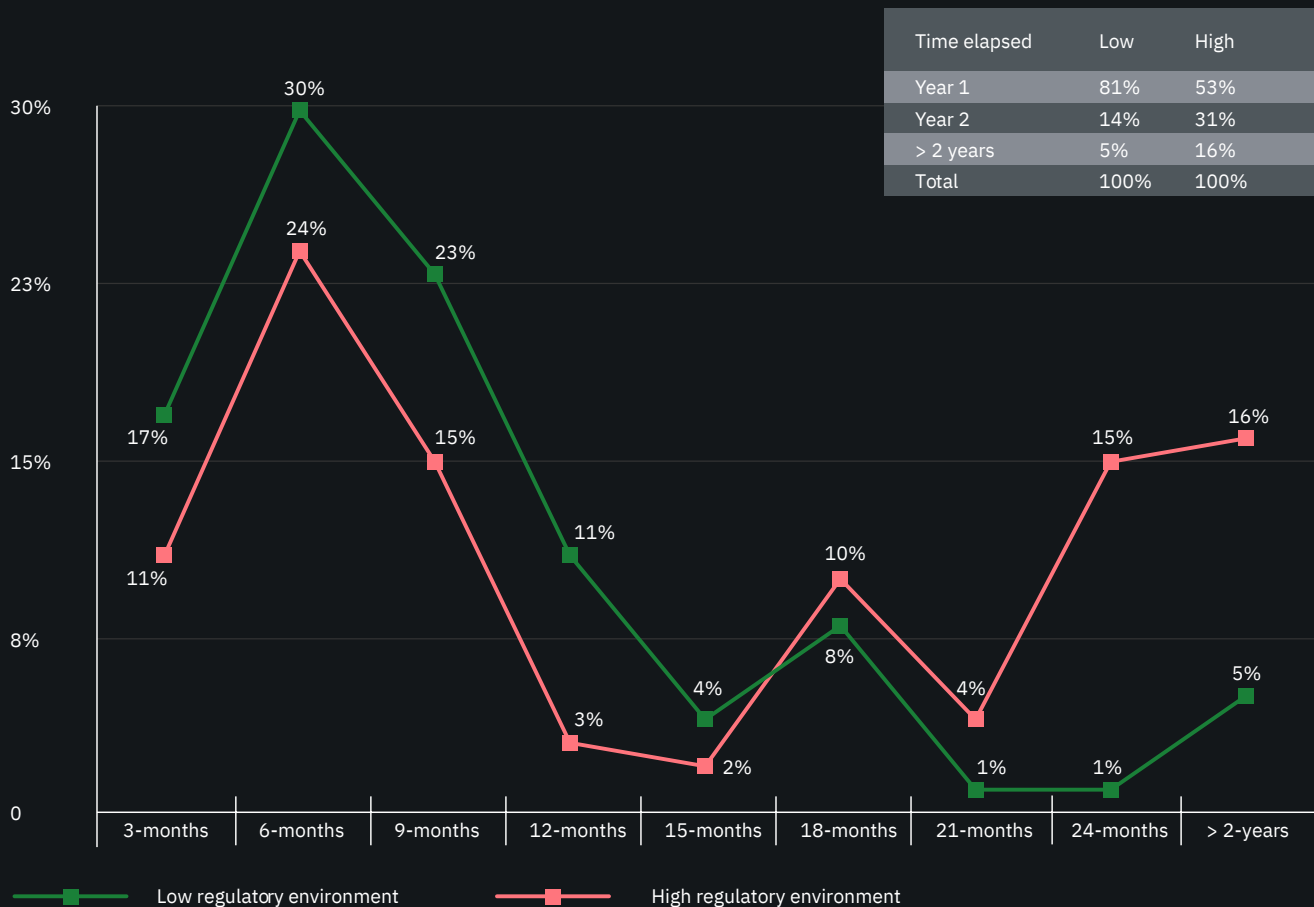
Highly regulated industries had a longer tail of data breach costs.

According to **Figure 33**, organizations studied in high data protection regulatory environments experienced 53 percent of the cost of a data breach in the first year, 31 percent in the second year and 16 percent more than two years after the incident. Organizations in a low data protection regulatory environment experienced 81 percent of costs in the first year, 14 percent in the second year and 5 percent of costs after more than two years.

Impact of security automation

This is the second year we examined the relationship between data breach cost and the state of security automation within companies that deploy, or do not deploy, automated security 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 incident response orchestration.

Key findings:

52%

52 percent of companies studied had security automation partially or fully deployed

95%

The average total cost of data breach was 95 percent higher in organizations without security automation deployed
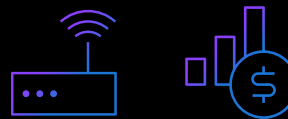
Technology and financial services organizations studied had the highest percentage of full deployment of automation

Figure 34:

State of security automation

Percentage of businesses with automation deployed

FY 2018   FY 2019
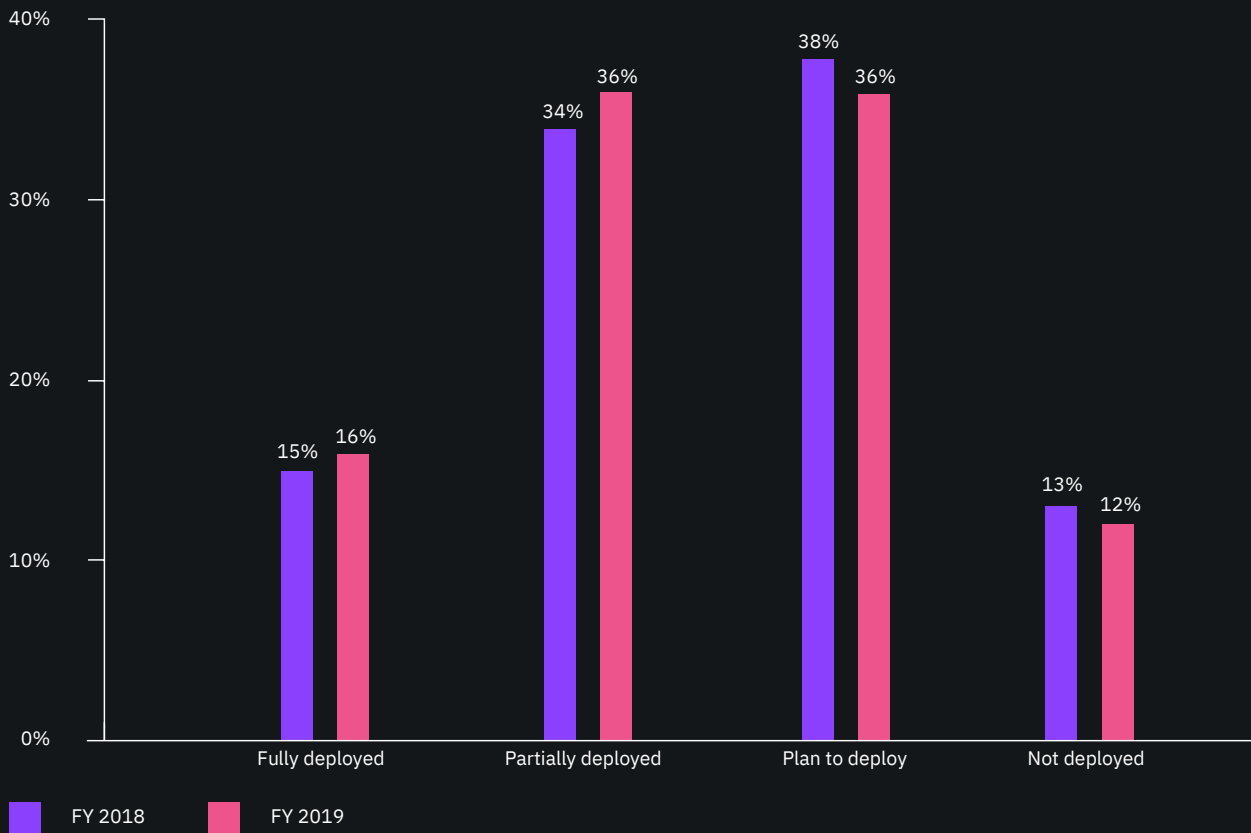
The state of security automation did not significantly change from the 2018 report.

Figure 34, shows that only 16 percent of companies reported full deployment and 36 percent reported partial deployment. Another 36 percent do not deploy security automation today but they do plan to deploy automation technologies within the next 24 months. Finally, 12 percent did not deploy, and had no plan to deploy security automation.

Figure 35:

Security automation decreases the total cost of a data breach

Measured in US$ millions

FY 2018   FY 2019
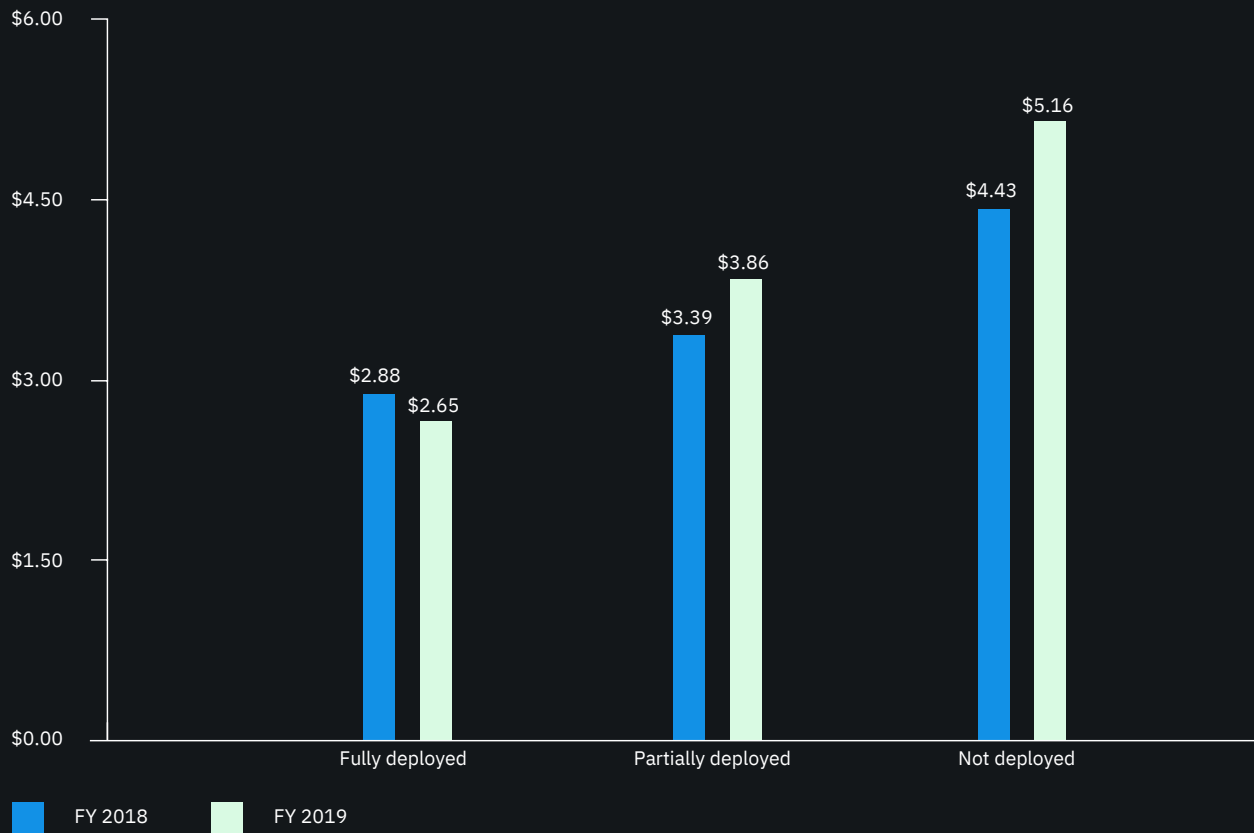
Organizations that do not deploy automation realized a much higher total cost of data breach.

As shown in **Figure 35**, results show the average total cost of data breach was $2.65 million for organizations that fully deployed security automation. Organizations that did not deploy automation realized a total cost of $5.16 million – for a net total cost difference of $2.51 million, or 95 percent higher than organizations with fully-deployed automation.

Figure 36:

State of security automation by country or region

Mean fully deployed = 16%; Mean partially deployed = 36%; Mean not deployed = 48%

	Fully deployed	Partially deployed	Not deployed
Germany	19%	51%	30%
Canada	16%	53%	31%
Middle East	20%	48%	32%
South Korea	23%	41%	36%
United States	16%	42%	42%
ASEAN	16%	39%	44%
United Kingdom	15%	39%	46%
Australia	16%	36%	48%
India	13%	37%	50%
Japan	18%	31%	51%
Italy	16%	33%	51%
Scandinavia	15%	31%	54%
France	13%	30%	57%
South Africa	16%	22%	62%
Brazil	12%	24%	64%
Turkey	14%	12%	74%

0%   25%   50%   75%   100%

■ Fully deployed   ■ Partially deployed   ■ Not deployed
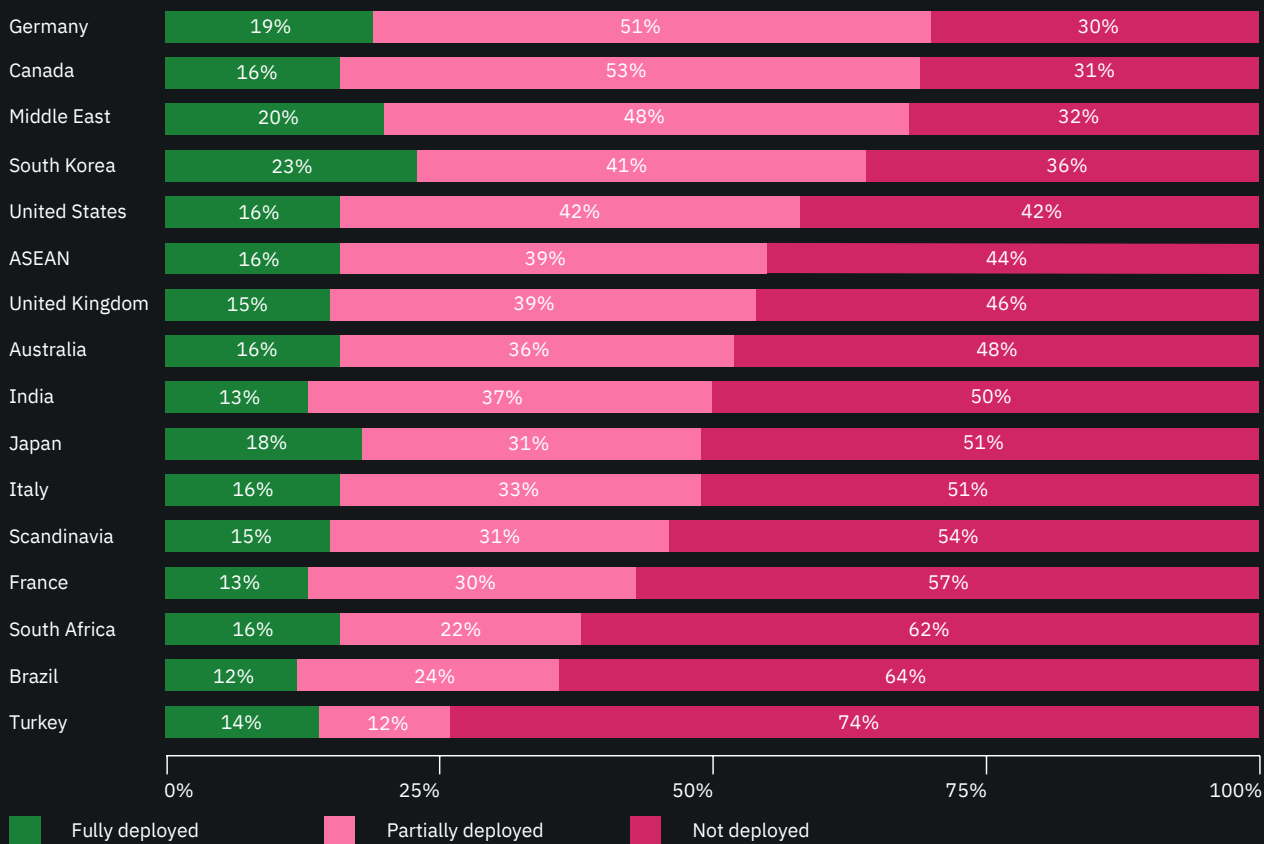
The state of deployment varies significantly among countries and regions.

Figure 36, shows South Korea and the Middle East had more organizations that have fully deployed automation. Turkey, Brazil and South Africa had the highest percentage of organizations that had not deployed automation.

Figure 37:

State of security automation by industry

Mean fully deployed = 16%; Mean partially deployed = 36%; Mean not deployed = 48%

Industry	Fully deployed	Partially deployed	Not deployed
Technology	25%	50%	25%
Financial	23%	48%	29%
Research	18%	42%	40%
Retail	15%	41%	44%
Transportation	19%	36%	45%
Communication	21%	34%	45%
Hospitality	12%	38%	50%
Health	15%	35%	50%
Entertainment	13%	36%	51%
Education	16%	33%	51%
Services	15%	32%	53%
Media	11%	36%	53%
Pharmaceuticals	13%	33%	54%
Consumer	14%	32%	54%
Energy	17%	29%	54%
Public	15%	29%	56%
Industrial	16%	27%	57%

■ Fully deployed   ■ Partially deployed   ■ Not deployed
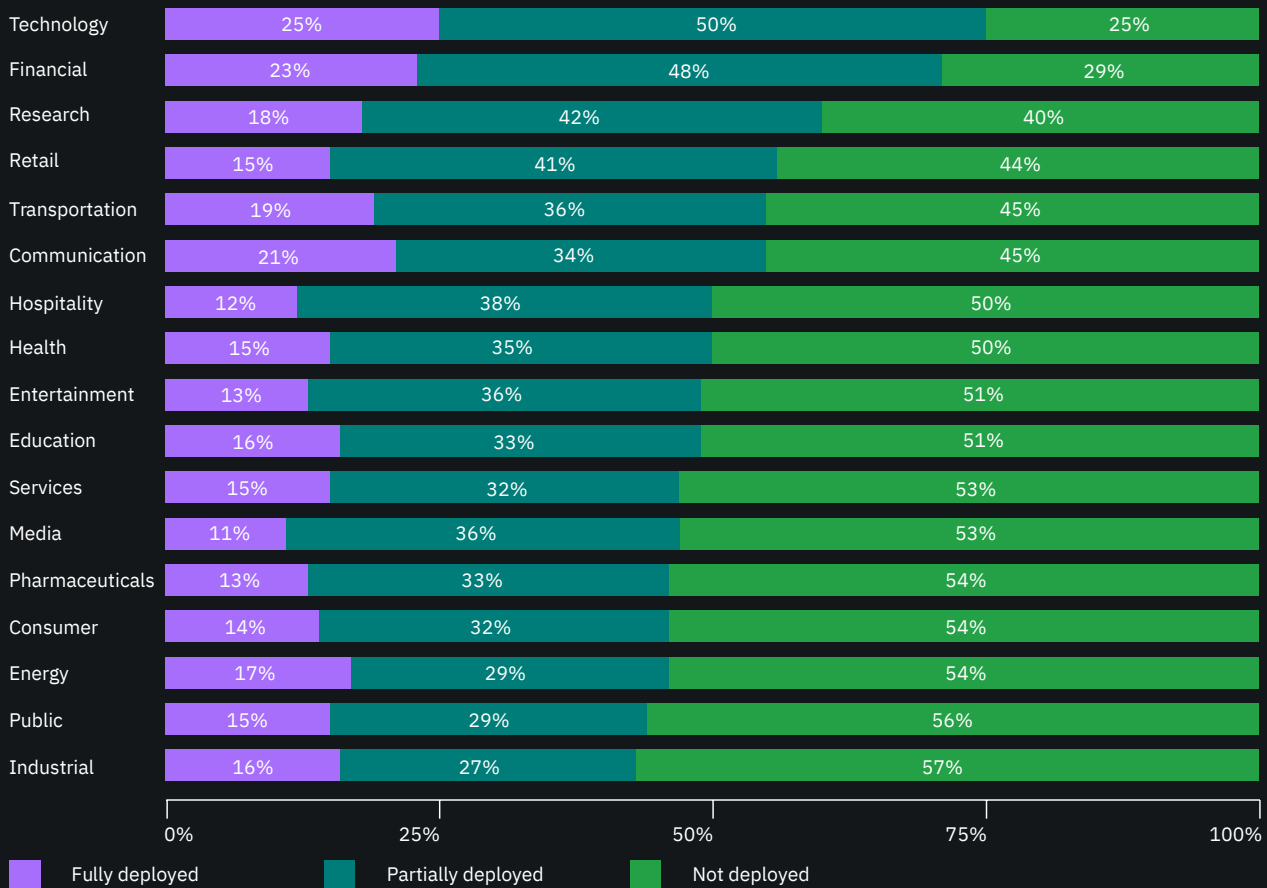
The state of deployment varied significantly among industries.

Figure 37, shows technology and financial services had the highest percentage of full deployment of automation. Industrial and public sectors had the highest percentage of organizations that had not deployed automation.

Cost of a mega breach

For the second reporting year we measured the cost of a data breach involving more than one million compromised records, or what we refer to as a mega breach. We recruited 14 companies that experienced such a data breach within the past three years. These companies are not included in the overall sample for calculation of the average cost of a data breach.

Key findings:

The cost of a mega breach of more than 1 million records was estimated at $42 million in the 2019 report, an increase of nearly 8 percent over the 2018 report

$42^M

8%

Estimated at $42 million in the 2019 report

An increase of nearly 8 percent over the 2018 report

A mega breach of more than 50 million records increased from an estimated $350 million in the 2018 report to an estimated $388 million in the 2019 report, a growth of almost 11 percent

$350^M

$388^M

11%

$350 million in the 2018 report

An estimated $388 million in the 2019 report

A growth of almost 11 percent

Figure 38:

Average total cost of a mega breach by number of records lost

Measured in US$ millions

2018 Total Cost (US$ Millions)   2019 Total Cost (US$ Millions)

Cost of a mega breach grows.

Figure 38, shows the estimated total cost at six size-levels
of a data breach, ranging from 1 million to 50 million lost
or stolen records. Drawing from our mega cost simulations,
a data breach involving 1 million compromised records
yields a total cost of $42 million dollars. At 50 million
records, we estimate a total cost of $388 million dollars.

Steps to Help Minimize Financial Consequences of a Data Breach

The cost of a data breach research underscores the importance of being prepared for a cyber incident. In this section, based on the results of our research, we outline steps organizations have taken to help reduce the damages and financial impact of a data breach. Observations regarding security practices that seem to mitigate data breaches are for educational purposes and do not guarantee results.

Have an incident response team and put incident response plans to the test.

To help mitigate the costs of a potential data breach, form of an incident response team and test the incident response plan. Organizations can help strengthen their ability to respond quickly to contain the fallout from a breach by establishing a detailed cyber incident playbook and routinely testing that plan through tabletop exercises or by running through a breach scenario in a simulated environment such as a cyber range.

Programs that preserve customer trust can help reduce the unexpected loss of customers following a data breach.

Organizations we surveyed worldwide continued to lose customers as a result of their data breaches. However, organizations with a senior-level leader, such as a chief privacy officer or chief information security officer, directing initiatives to help improve customer trust in the guardianship of their personal information, reduced turnover and, therefore, reduce the cost of the breach. Organizations that offered data breach victims identity protection in the aftermath were also more successful in reducing customer turnover.

Discover, classify and encrypt sensitive data and identify database misconfigurations.

Data classification schema and retention programs can help bring visibility into the sensitive and confidential information that is vulnerable to a breach and reduce the volume of such information. Vulnerability scanning can help you identify database vulnerability exposures and misconfigurations. The most sensitive data should be obscured and encrypted on premise, at the endpoint, in transit, and in the cloud.

Invest in technologies that help improve the ability to rapidly detect and contain a data breach.

The faster the data breach was identified and contained, the lower the costs. This year, the increasing time to resolve a breach was potentially due to the increasing severity of criminal and malicious attacks experienced by a majority of companies in our sample. Security automation and intelligent orchestration capabilities that provide visibility across the security operations center can help improve an organization's ability to contain the damage from a breach.

Invest in governance, risk management and compliance programs.

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. An internal framework for satisfying governance requirements, evaluating risk across the enterprise and tracking compliance with governance requirements can help improve an organization's ability to detect and escalate a data breach.

Minimize complexity of IT and security environments.

In this year's study, we showed that data breaches caused by a third party, compliance failures, extensive cloud migration, system complexity, and extensive IoT, mobile and OT environments, increased the cost of a data breach for the companies studied.

How We Calculate the Cost of a Data Breach

To calculate the cost of a 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

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

Categorizing the costs

Once the company estimated a cost range for these activities, we categorized the costs as direct or indirect 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.

Figure 39:
Direct and indirect costs by country or region
Measured in US$

Country/Region	Direct per record cost	Indirect per record cost
United States	$88	$154
Germany	$85	$108
Canada	$78	$109
Middle East	$88	$85
France	$73	$90
Italy	$80	$77
South Africa	$73	$83
United Kingdom	$70	$84
Japan	$75	$66
South Korea	$62	$78
ASEAN	$59	$71
Australia	$50	$60
Turkey	$48	$46
Scandinavia	$43	$42
Brazil	$31	$45
India	$31	$42

$0 $63 $125 $188 $250

■ Direct per record cost   ■ Indirect per record cost
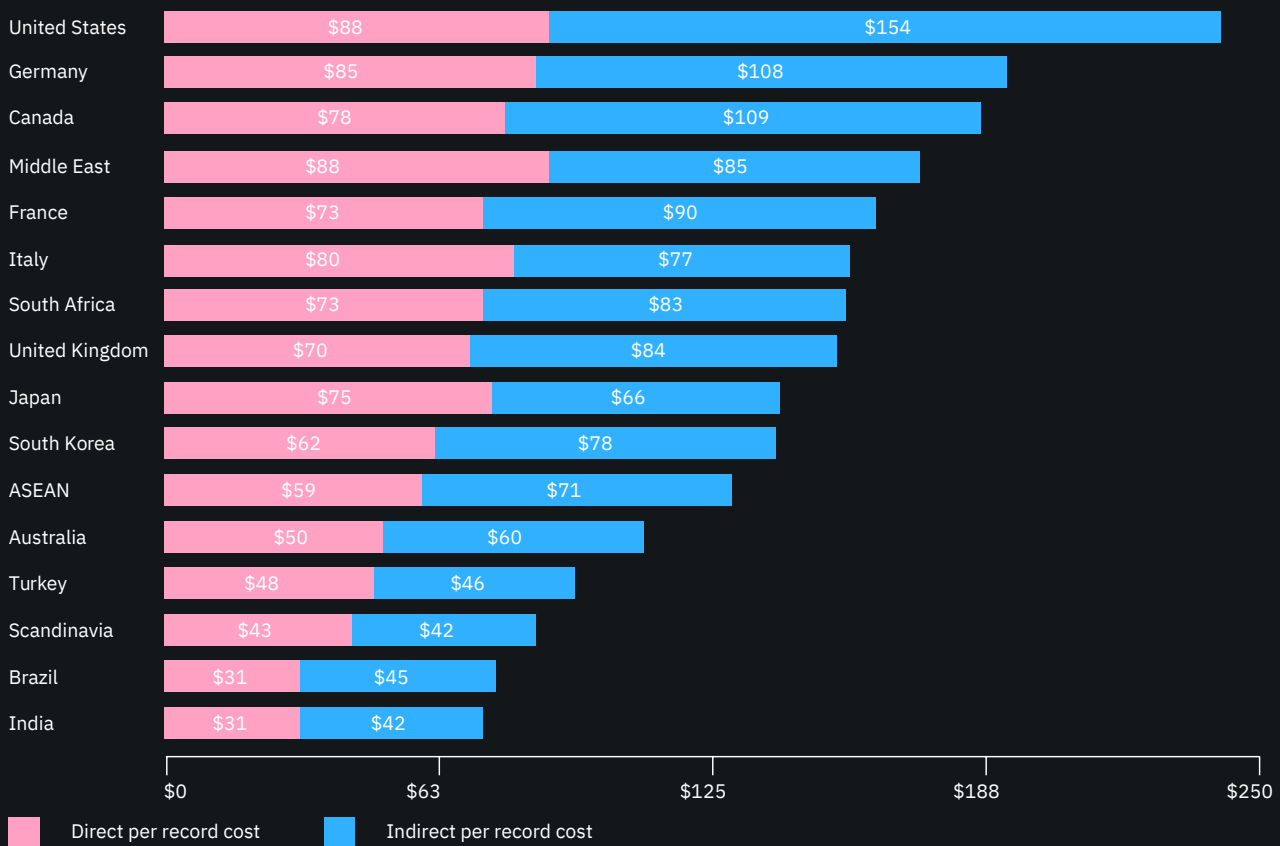
According to **Figure 39,** the U.S. had the highest indirect cost per lost record. The highest direct per record costs of a data breach were in the U.S. and Middle East.

Data collection methods

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.

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 infor-mation. 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.

How research participants estimated data breach costs

To preserve confidentiality, organizations did not provide actual accounting information on breach costs. Instead, research participants estimated costs incurred by their organization using a number line. Participants were instructed to mark a number line in one spot between the lower and upper limits of a range for each data breach cost category.

LL   UL

Organization Characteristics

This year's annual study was conducted in 507 organizations in 16 countries or regional samples: the United States, India, the United Kingdom, Germany, Brazil, Japan, France, the Middle East, Canada, Italy, South Korea, Australia, Turkey, ASEAN, South Africa, and, for the first time, Scandinavia.
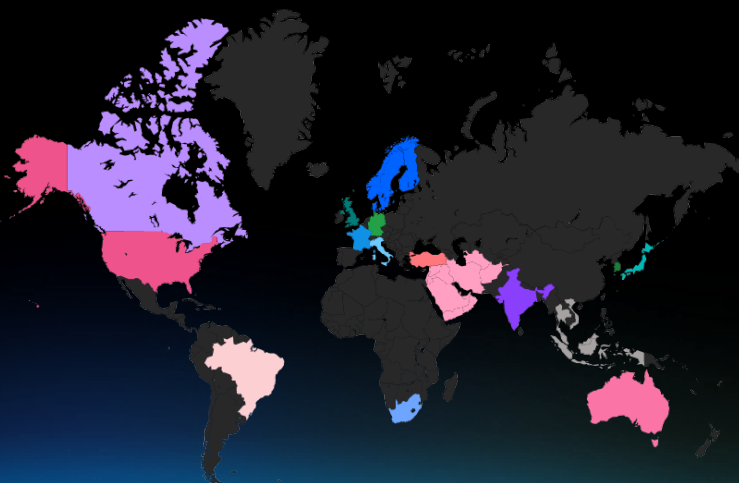
Represented industries

There were 17 industries represented in the sample.

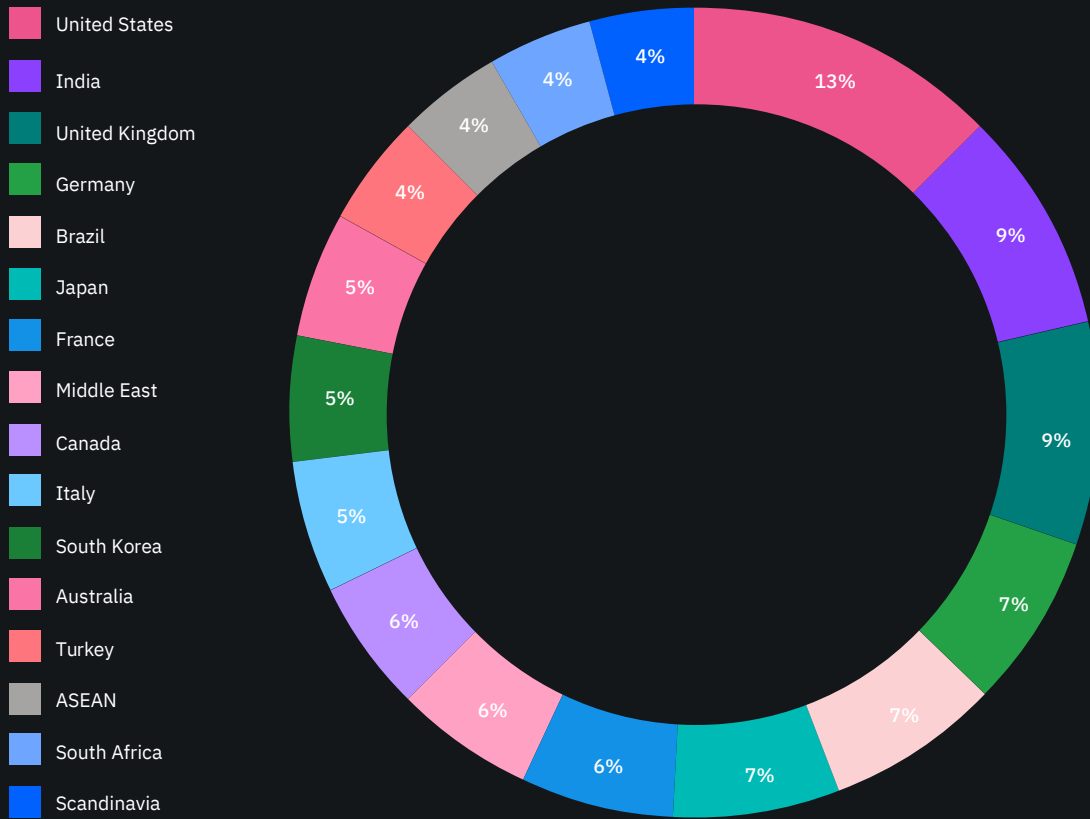|				
Healthcare Hospitals, clinics	**Financial** Banking, insurance, investment companies	**Energy** Oil and gas companies, utilities, alternative energy producers and suppliers	**Pharma** Pharmaceutical, including biomedical life sciences	**Industrial** Chemical process, engineering and manufacturing companies
Technology Software and hardware companies	**Education** Public and private universities and colleges, training and development companies	**Services** Professional services such as legal, accounting and consulting firms	**Entertainment** Movie production, sports, gaming and casinos	**Transportation** Airlines, railroad, trucking and delivery companies
Communication Newspapers, book publishers, public relations and advertising agencies	**Consumer** Manufacturers and distributors of consumer products	**Media** Television, satellite, social media, Internet	**Hospitality** Hotels, restaurant chains, cruise lines	**Retail** Brick and mortar and e-commerce
Research Market research, think tanks, R&D	**Public Sector** Federal, state and local government agencies and NGOs			

Figure 40:

Distribution of the sample by country or region

Sample size (n) = 507

Legend:
- United States
- India
- United Kingdom
- Germany
- Brazil
- Japan
- France
- Middle East
- Canada
- Italy
- South Korea
- Australia
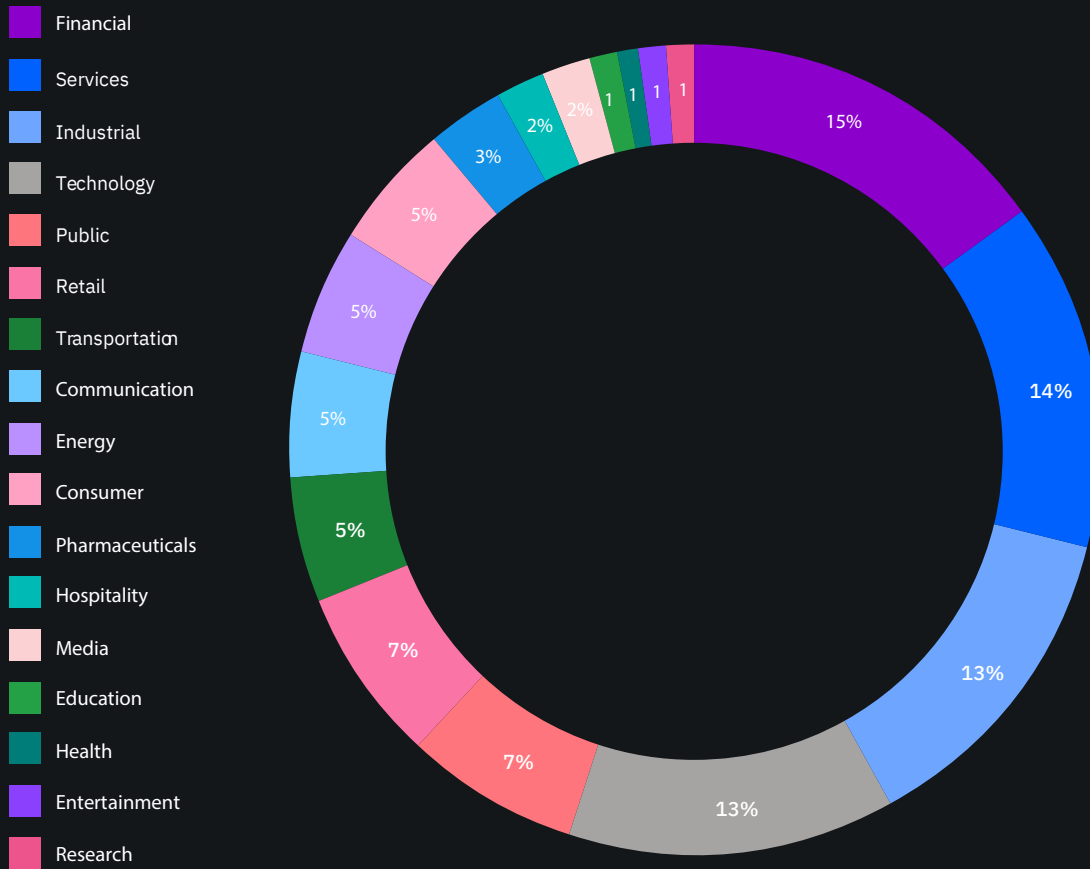- Turkey
- ASEAN
- South Africa
- Scandinavia

This year's study included organizations from 16 countries or regions.

Figure 40, shows the distribution of benchmark organizations by their country or region. The United States had the highest representation followed by India at 13 percent and 9 percent, respectively. The smallest representation was Scandinavia at 4 percent.

Figure 41:

Industry distribution of the sample

Sample size (n) = 507

- Financial
- Services
- Industrial
- Technology
- Public
- Retail
- Transportation
- Communication
- Energy
- Consumer
- Pharmaceuticals
- Hospitality
- Media
- Education
- Health
- Entertainment
- Research

Seventeen industries were represented in this year's study.

Figure 41, shows the distribution of benchmark organizations by industry. The largest sectors were financial, services, industrial and technology sector organizations.

Research 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 a period from July 2018 to April 2019. 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, 507 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 record 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.

Next steps

Protect assets →

Orchestrate your response →

Identify threats →

Remediate and recover →

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

The Cost of a Data Breach Report is sponsored, analyzed and reported by IBM Security. Previous years' Cost of a Data Breach Reports are available at 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.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security solutions to help organizations stop threats, prove compliance, and grow securely.

IBM operates one of the broadest and deepest security research, development and delivery organizations. It monitors more than two trillion events per month in more than 130 countries and holds more than 3,000 security patents. To learn more, visit ibm.com/security.

IBM **Security**