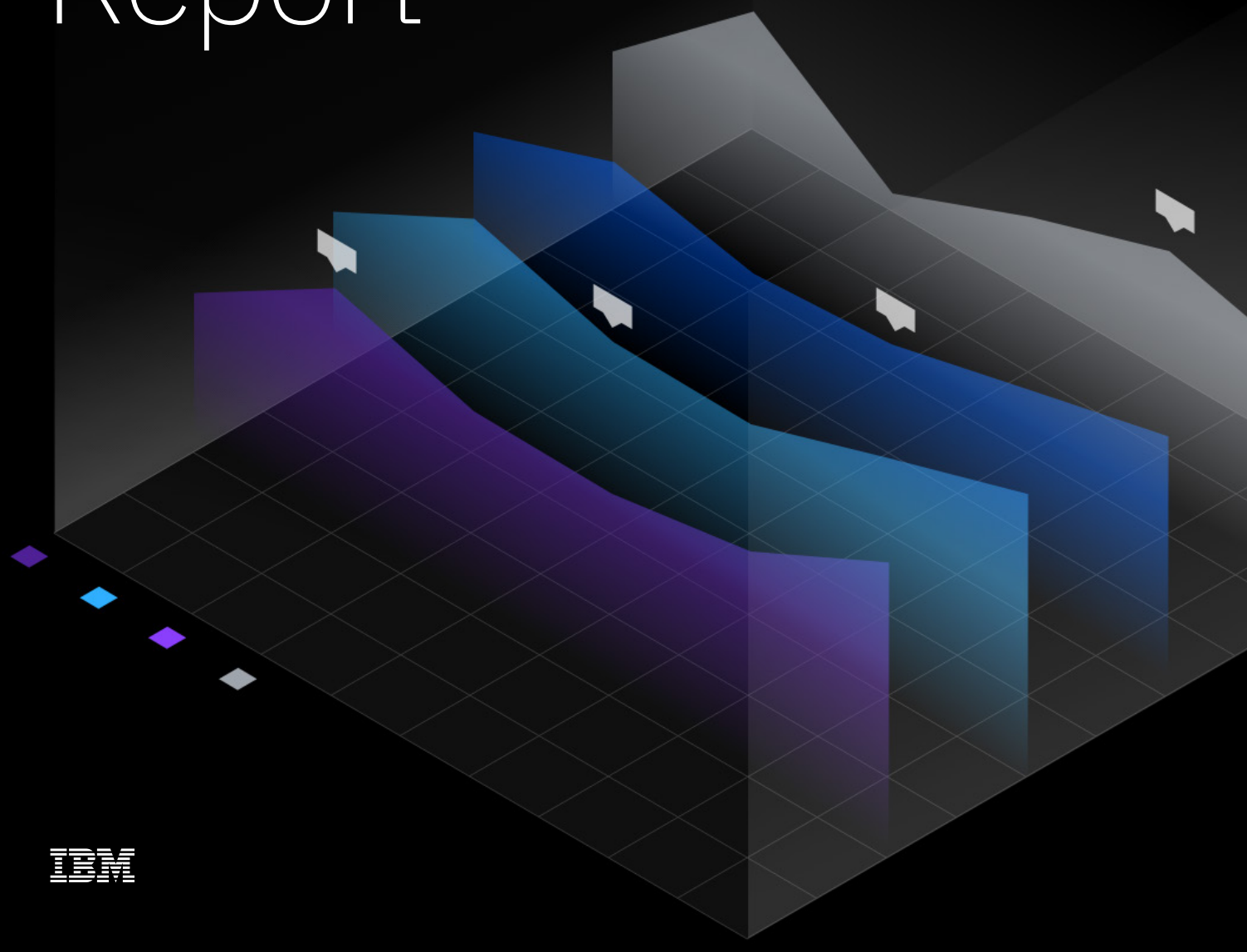
IBM Security

# Cost of a Data Breach Report 2020



IBM

# Contents

# Executive summary

This is the 15th year the Ponemon Institute has conducted the research to produce the annual *Cost of a Data Breach Report*, including the past five years this report has been sponsored and published by IBM Security. Our hope is that businesses can use this research to drive forward with innovation while maintaining customer trust at a time when data breaches and cybersecurity incidents are risks for organizations of all types and sizes.

The report has become one of the leading benchmark tools in the cybersecurity industry, offering IT, risk management and security leaders a point-in-time view of the factors that either mitigate or exacerbate the cost of data breaches. This report also offers a view of data breach trends, demonstrating both consistencies and fluctuations in the costs we have analyzed over time.

For the 2020 *Cost of Data Breach Report**, Ponemon Institute recruited 524 organizations that experienced data breaches between August 2019 and April 2020. To ensure the research is relevant to a broad set of companies, the organizations in the study comprise of various sizes, spanning 17 countries and regions as well as 17 industries. Our researchers interviewed more than 3,200 individuals who are knowledgeable about the data breach incidents in their organizations.

**Cost of a Data Breach Report facts**

524
Breached organizations

3,200
Individuals interviewed

17
Countries and regions

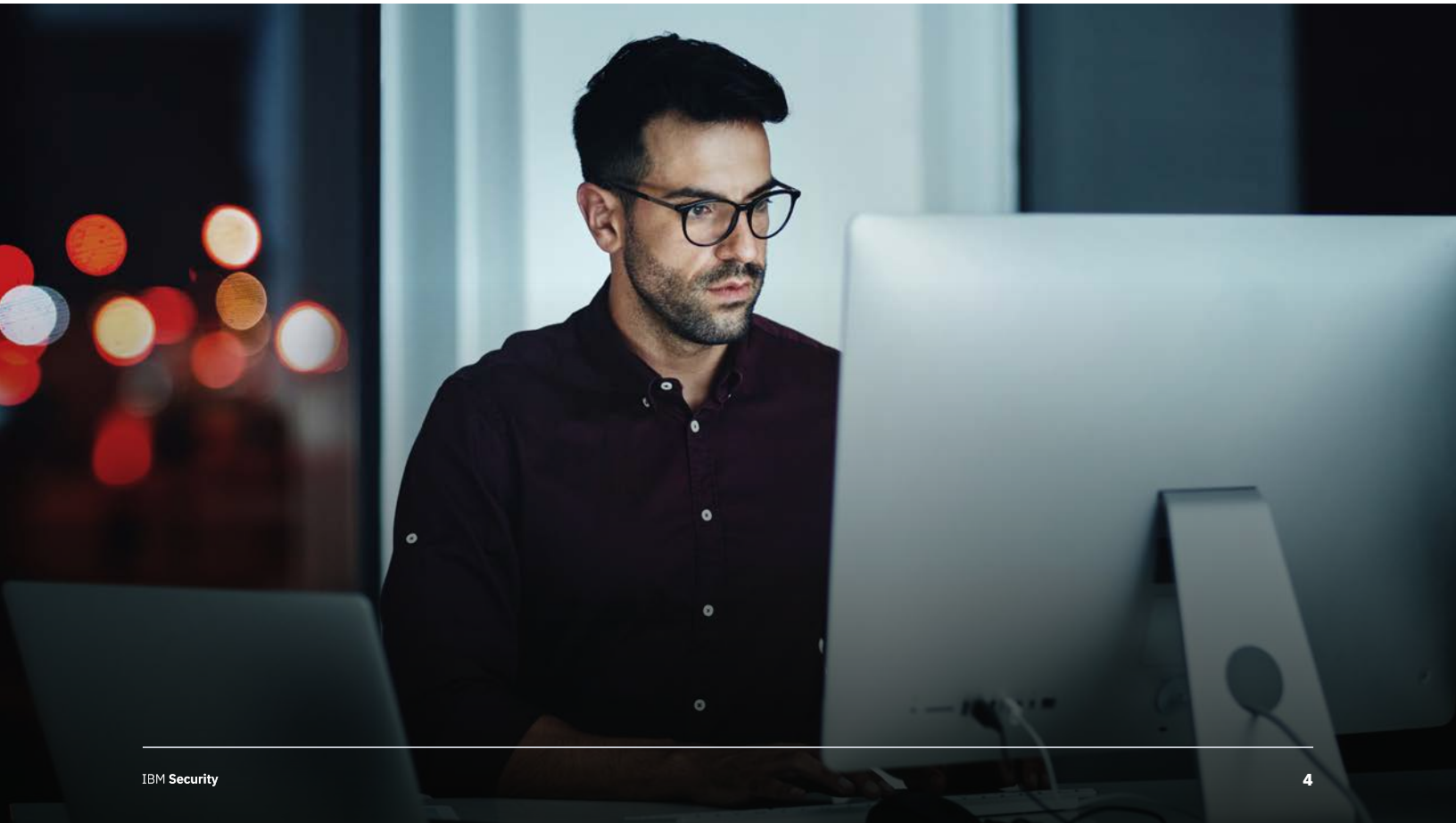
17
Industries

*Years in this report refer to the year of publication, not necessarily the year the breaches occurred. The data breaches analyzed in the 2020 report occurred between August 2019 and April 2020.

In the course of our interviews, we asked dozens of questions to determine what organizations spent on activities for the discovery of and the immediate response to the data breach. Other issues covered that may have influenced the cost were the root causes of the data breach, length of time it took the organizations to detect and contain the incident and estimated cost of business disruption and lost customers as a result of the breach. We examined many other cost factors, including security measures implemented before the breach and characteristics of the organization and its IT environment.

The result is a report with a vast data set, extensive analysis and trend insights. In the following pages of this executive summary, you will find a brief explanation of how data breach costs are calculated and the key findings of this research. For a deeper dive into the data, the complete findings section offers 49 analytical and demographics charts.

For IT leaders, cybersecurity strategists and risk management officers, we offer recommendations for security measures that may reduce the potential financial and brand damages from a data breach, based on what the research found were most effective for organizations in the study. We close the report with a detailed explanation of our research methodology.



# What's new in the 2020 report

We aim to renew the report each year to offer analyses that build upon past reports and break new ground to keep up with changing technology and trends to form a more complete picture of risks and standards for securing data.

What a momentous year 2020 has turned out to be. On top of the cyclical changes in technology and threats, a global pandemic has turned life upside down for businesses and consumers around the world.

Although this research began months before the COVID-19 pandemic had widespread impact, and after most of the breach incidents studied had occurred, we asked participants to answer supplemental research questions about potential impact of remote workforces due to the pandemic. We found that a majority of organizations (76%) predicted that remote work would make responding to a potential data breach a much more difficult ordeal.

Fresh research introduced with this year's report provides a deeper dive into the types of data we have long explored — including the per record cost of a data breach and the root causes of data breaches. In this study, for the first time, we segmented the cost per compromised record to discover those costs based on the type of records breached, including customer personally identifiable information (PII), employee PII and intellectual property (IP). On the data breach root causes analysis, we added a layer of depth to look at more specific types of malicious breaches, from stolen credentials to insider threats.

For the first time, we asked participants to identify the type of threat actor presumed to be responsible for the breach, including nation state and financially motivated attackers, with our cost analysis demonstrating that the most common type of malicious breach — those caused by financially motivated cybercriminals — was not the most expensive.

And as ransomware and destructive malware attacks have grown more common, we added new cost analyses to this year's report that found those pernicious attacks had a greater average cost of a breach than the overall average cost of a data breach.

**Data breach stats**

## $3.86 million

Average total cost

## United States

Highest country cost

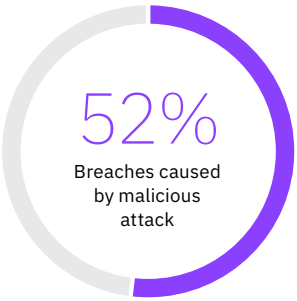
## Healthcare

Highest industry cost

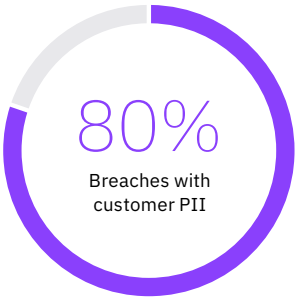
## 280 days

Average time to identify and contain

Several new cost factors were added to this year's research, including the impact of vulnerability and red team testing, which uses an adversarial approach to penetration testing, as well as the influence of a remote workforce and security skills shortage on those costs. Perhaps unsurprisingly, skills shortage was among the top three factors that increased the average cost of a data breach out of 25 analyzed, while red team testing made an entry in the top five cost factors shown to mitigate the average cost of a breach.




Other new questions examined included a deeper dive into the role played by the chief information security officer (CISO) and the types of costs covered by cybersecurity insurance.

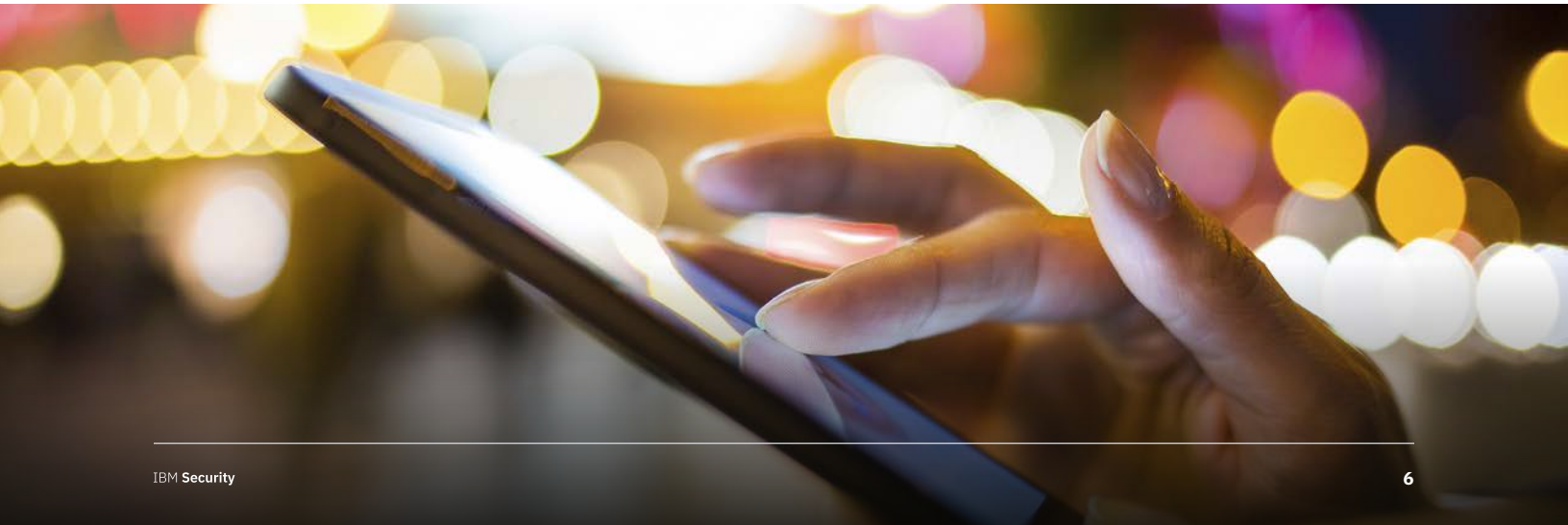



It's worth noting that the average total cost of a data breach declined slightly in this year's report, from $3.92 million last year to $3.86 million this year, which may lead some to believe that data breach costs have plateaued.

On the contrary, our study appears to show a growing divide in data breach costs between organizations with more advanced security processes, like automation and formal incident response teams, and those with less advanced security postures in these areas.

As this is a global report, the vastness of the research collected means we cannot highlight every nuance in the data breach costs for all countries and industries in this study. That's why we developed an online calculator and data explorer tool at ibm.com/databreach for you to customize and make your own discoveries.

We hope you will find insights that are meaningful to your organization and draw conclusions that can help you better protect the data that your business' success depends upon.



# How we calculate the cost of a data breach

To calculate the average cost of a data breach, this research excludes very small and very large breaches. Data breaches examined in the 2020 study ranged in size between 3,400 and 99,730 compromised records. We use a separate analysis to examine the costs of very large "mega breaches," which we explore in further detail in the complete findings section of the report.

This research uses an accounting method called activity-based costing, which identifies activities and assigns a cost according to actual use. Four process-related activities drive a range of expenditures associated with an organization's data breach: detection and escalation, notification, post data breach response and lost business.

*For a more in-depth explanation of the methods used for this report, see the section on research methodology.*

**The four cost centers are described below.**

## Detection and escalation

Activities that enable a company to reasonably detect the breach.

- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards

## Lost business

Activities that attempt to minimize the loss of customers, business disruption and revenue losses.

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

## Notification

Activities that enable the company to notify data subjects, data protection regulators and other third parties.

- Emails, letters, outbound calls or general notice to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement of outside experts

## Ex-post response

Activities to help victims of a breach communicate with the company and redress activities to victims and regulators.

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fines

# Key findings

*The key findings described here are based on IBM Security analysis of the research data compiled by the Ponemon Institute.*

-1.5%

Avg. total cost net change, 2019-2020

## The average total cost of a data breach declined slightly year-over-year, but costs increased for many organizations.

Despite a nominal decline from $3.92 million in the 2019 study to $3.86 million in the 2020 study, costs were much lower for some of the most mature companies and industries and much higher for organizations that lagged behind in areas such as security automation and incident response processes. Similarly, deeper analysis of the average cost of a single lost or stolen record (cost per record) showed wide variability, depending on the types of data lost or stolen in a breach.

$150

Customer PII avg. cost per record

## Customers' personally identifiable information (PII) was the most frequently compromised type of record, and the costliest, in the data breaches studied.

Eighty percent of breached organizations stated that customer PII was compromised during the breach, far more than any other type of record. While the average cost per lost or stolen record was $146 across all data breaches, those containing customer PII cost businesses $150 per compromised record.

The cost per record of customer PII increased to $175 in breaches caused by a malicious attack. Anonymized customer data was involved in 24% of breaches in the study, at an average cost of $143 per record, which increased to $171 per record in breaches caused by malicious attacks.

+$137,000

Remote work impact on avg. total cost

## Remote work during COVID-19 was expected to increase data breach costs and incident response times.

Of organizations that required remote work as a result of COVID-19, 70% said remote work would increase the cost of a data breach and 76% said it would increase the time to identify and contain a potential data breach. Having a remote workforce was found to increase the average total cost of a data breach of $3.86 million by nearly $137,000, for an adjusted average total cost of $4 million.


## Stolen or compromised credentials were the most expensive cause of malicious data breaches.

One in five companies (19%) that suffered a malicious data breach was infiltrated due to stolen or compromised credentials, increasing the average total cost of a breach for these companies by nearly $1 million to $4.77 million. Overall, malicious attacks registered as the most frequent root cause (52% of breaches in the study), versus human error (23%) or system glitches (25%), at an average total cost of $4.27 million.

+14%

Cloud misconfiguration impact on avg. total cost

## Misconfigured clouds were a leading cause of breaches.

Alongside stolen or compromised credentials, misconfigured cloud servers tied for the most frequent initial threat vector in breaches caused by malicious attacks, at 19%. Breaches due to cloud misconfigurations resulted in the average cost of a breach increasing by more than half a million dollars to $4.41 million.

## $1.52 million

Lost business avg. total cost

### Lost business continued to be the largest contributing cost factor.

Lost business costs accounted for nearly 40% of the average total cost of a data breach, increasing from $1.42 million in the 2019 study to $1.52 million in the 2020 study. Lost business costs included increased customer turnover, lost revenue due to system downtime and the increasing cost of acquiring new business due to diminished reputation.

## $3.58 million

Average cost savings of fully deployed security automation vs. no security automation

### The impact of security automation on data breach costs has grown over the past three years.

The share of businesses with fully deployed security automation, defined as the use of artificial intelligence platforms and automated breach orchestration, grew from just 15% in 2018 to 21% in the 2020 study.

Meanwhile, the effectiveness of security automation in reducing the average cost of a data breach continued to grow. Businesses that had not deployed security automation saw an average total cost of $6.03 million, more than double the average cost of a data breach of $2.45 million for businesses that had fully deployed security automation. The $3.58 million savings in average breach costs for companies with fully deployed security automation versus those without deployed security automation grew from a savings of $1.55 million in the 2018 study.

## 100x

Cost multiplier of > 50 million records vs. average breach

### Mega breach costs soared by the millions.

Companies that experienced breaches of more than 1 million records continued to see costs that were many times the overall average, in a sample of very large data breaches. Breaches of 1 million to 10 million records cost an average of $50 million, more than 25 times the average cost of $3.86 million for breaches of less than 100,000 records. In breaches of more than 50 million records, the average cost was $392 million, more than 100 times the average.


## Breaches caused by nation state actors were most expensive.

While the majority of malicious breaches were caused by financially motivated cyberattackers, those caused by nation state actors were the costliest. Fifty-three percent of malicious breaches in the 2020 study were believed to be carried out by financially motivated cybercriminals, compared to 13% by nation state threat actors, 13% by hacktivists and 21% remaining unknown. However, the presumed state-sponsored breaches cost an average of $4.43 million, compared to $4.23 million in financially motivated breaches.

+$292,000

Security system complexity impact on avg. total cost

## Security complexity and cloud migration cost companies most.

Security system complexity was the most expensive of 25 cost factors, increasing the average total cost of a breach by $292,000, for an adjusted average total cost of $4.15 million. Undergoing an extensive cloud migration at the time of the breach increased the average cost of a breach by more than $267,000, to an adjusted average cost of $4.13 million.

+96 days

Healthcare vs. financial industry breach lifecycle

## The average time to identify and contain a breach varied widely depending on industry, geography and security maturity.

On average, companies in the 2020 study required 207 days to identify and 73 days to contain a breach in 2019, combining for an average “lifecycle” of 280 days.

While the lifecycle of a breach averaged 329 days in the healthcare sector, the average lifecycle was 96 days shorter in the financial sector (233 days). Fully deployed security automation helped companies reduce the lifecycle of a breach by 74 days compared to companies with no security automation deployment, from 308 to 234 days.

# $2 million

Average cost savings with incident response teams and IR testing vs. no IR teams or testing

## Incident response (IR) preparedness was the highest cost saver for businesses.

The average total cost of a data breach for companies with an IR team that also tested an IR plan using tabletop exercises or simulations was $3.29 million, compared to $5.29 million for companies with neither an IR team nor tests of the IR plan — a difference of $2 million. The cost difference between these groups was $1.23 million in the 2019 study.

# 12 of 16

Countries with increased avg. total cost since 2019 study

## Regional and industry differences showed some big swings from 2019.

The United States continued to experience the highest data breach costs in the world, at $8.64 million on average, followed by the Middle East at $6.52 million. The average total cost increased in 12 of 16 countries or regions that were studied in both 2019 and 2020, with the biggest increase in Scandinavia, at 12.8%.

For the tenth year in a row, healthcare continued to incur the highest average breach costs at $7.13 million — a 10.5% increase over the 2019 study. Similarly, the energy sector saw a 14.1% increase from 2019, to an average of $6.39 million in the 2020 study. Overall, 13 of 17 industries experienced an average total cost decline year over year, with the steepest drops coming in media, education, public sector and hospitality.

# Complete findings

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

1. Global findings and highlights
2. Root causes of a data breach
3. Factors that influence the cost of a data breach
4. Security automation trends and effectiveness
5. Time to identify and contain a data breach
6. Longtail costs of a data breach
7. Potential impacts of COVID-19
8. Cost of a mega breach

# Global findings and highlights

The *Cost of a Data Breach Report* is a global report, combining results from 524 organizations across 17 countries and regions, and 17 industries to provide global averages. However, in some cases, the report breaks out the results by country/region or industry for comparative purposes. Although sample sizes in some countries/regions and industries are quite small, the organizations in the study have been selected in an attempt to be representative.

## Key findings

**$7.13 million**

The average cost of a data breach in the healthcare industry, an increase of 10% compared to the 2019 study

**80%**

Share of breaches that included records containing customer PII, at an average cost of $150 per record

**$5.52 million**

Average total cost of a breach at enterprises of more than 25,000 employees, compared to $2.64 million for organizations under 500 employees

**Figure 1**

# Global study at a glance

| Country/region | 2020 sample | Percentage of sample | Currency | Years of study |
|---|---|---|---|---|
| United States | 63 | 12% | USD | 15 |
| India | 47 | 9% | INR | 9 |
| United Kingdom | 44 | 8% | GBP | 13 |
| Germany | 37 | 7% | Euro | 12 |
| France | 36 | 7% | Euro | 7 |
| Brazil | 35 | 7% | BRL | 9 |
| Japan | 33 | 6% | Yen | 11 |
| Middle East* | 29 | 6% | Riyal | 7 |
| Canada | 26 | 5% | CA Dollar | 6 |
| South Korea | 24 | 5% | Won (KRW) | 3 |
| ASEAN# | 23 | 4% | Singapore Dollar | 2 |
| Australia | 23 | 4% | AU Dollar | 11 |
| Scandinavia+ | 23 | 4% | Krone | 2 |
| Italy | 21 | 4% | Euro | 9 |
| Latin America** | 21 | 4% | Peso | 1 |
| Turkey | 20 | 4% | Turkish Lira | 3 |
| South Africa | 19 | 4% | Rand (SAR) | 5 |
| Total | 524 | | | |

## This year's study examined breaches at companies in 17 countries or regional samples.

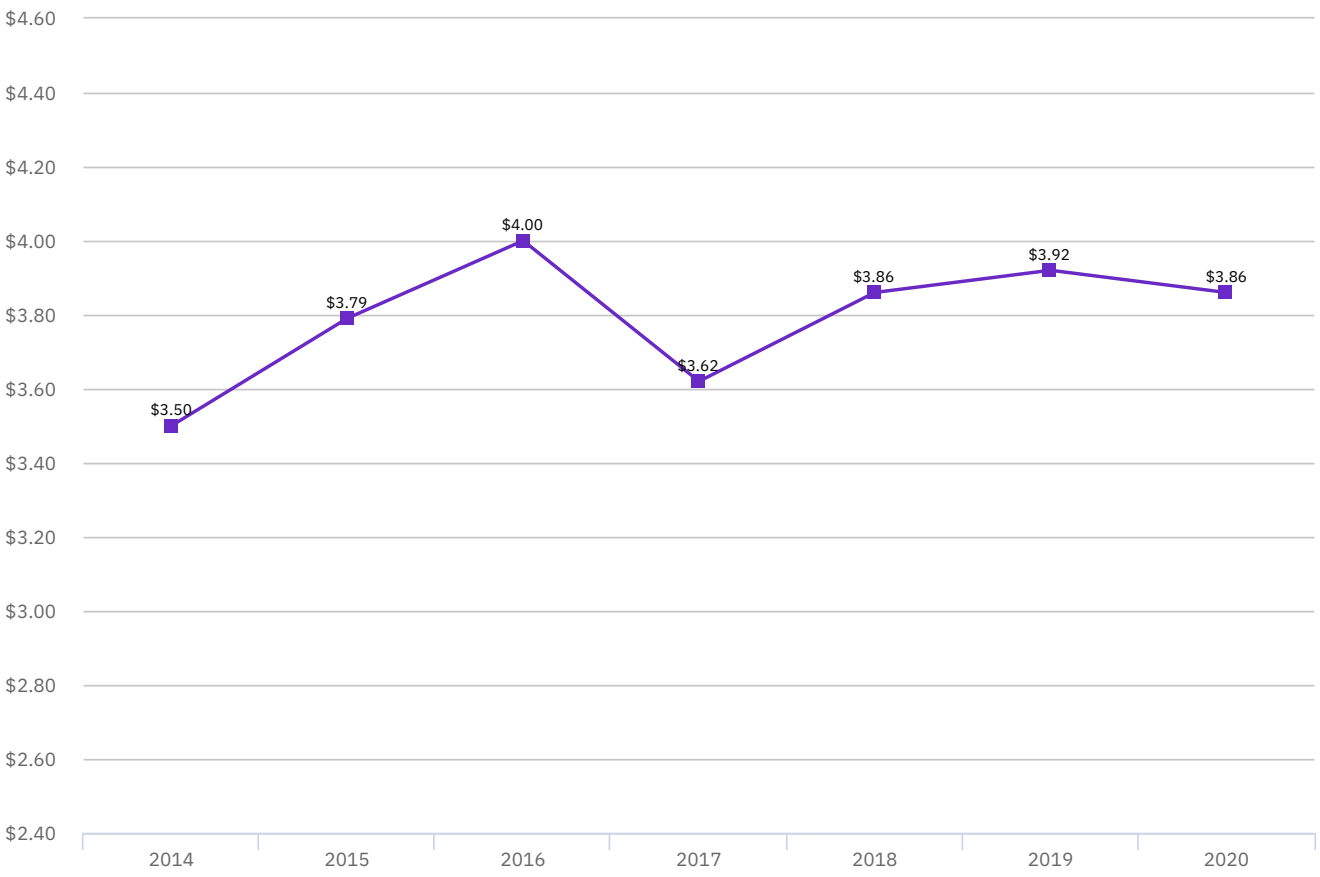
Countries and regions included the United States, India, the United Kingdom, Germany, Brazil, Japan, France, the Middle East, Canada, Italy, South Korea, Australia, Turkey, ASEAN, South Africa, Scandinavia and, for the first time, Latin America — a region that includes Mexico, Argentina, Chile and Colombia. **Figure 1** presents sample size, currency for each country/region and the number of years the country/region has been included in the research.

*Middle East is a cluster of companies located in Saudi Arabia and the United Arab Emirates
#ASEAN is a cluster of companies located in Singapore, Indonesia, Philippines, Malaysia, Thailand and Vietnam
+Scandinavia is a cluster of companies located in Denmark, Sweden, Norway and Finland
** Latin America is a cluster of companies in Mexico, Argentina, Chile and Colombia

**Figure 2**

## Average total cost of a data breach

Measured in US$ millions



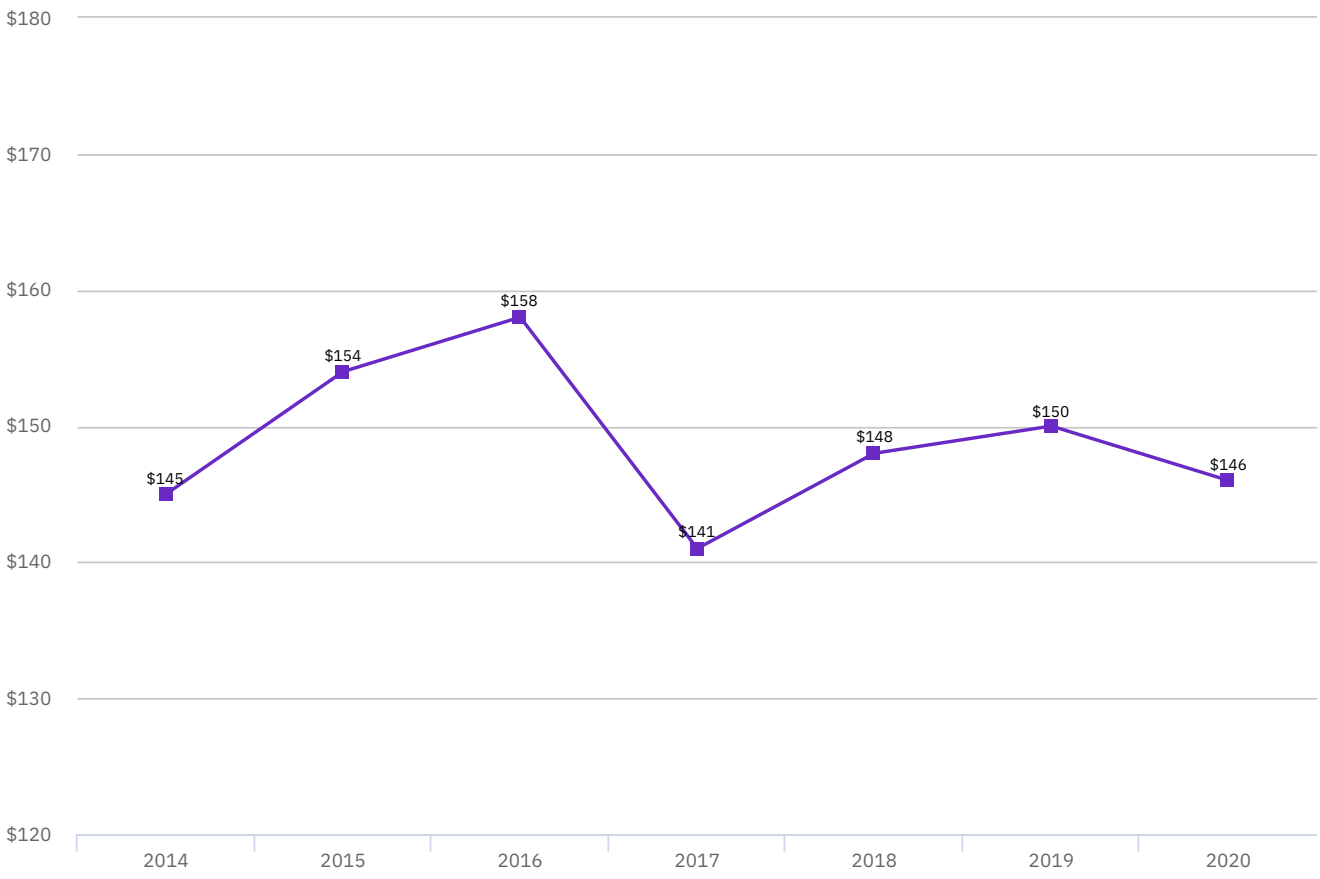

### The average total cost of a data breach has increased by 10% since 2014.

**Figure 2** presents the global average total cost of a data breach over seven years. The consolidated average total cost in the 2020 study was $3.86 million, a slight decrease from $3.92 in 2019. The weighted average is $3.79 million over seven years.

**Figure 3**

## Average per record cost of a data breach

Measured in US$



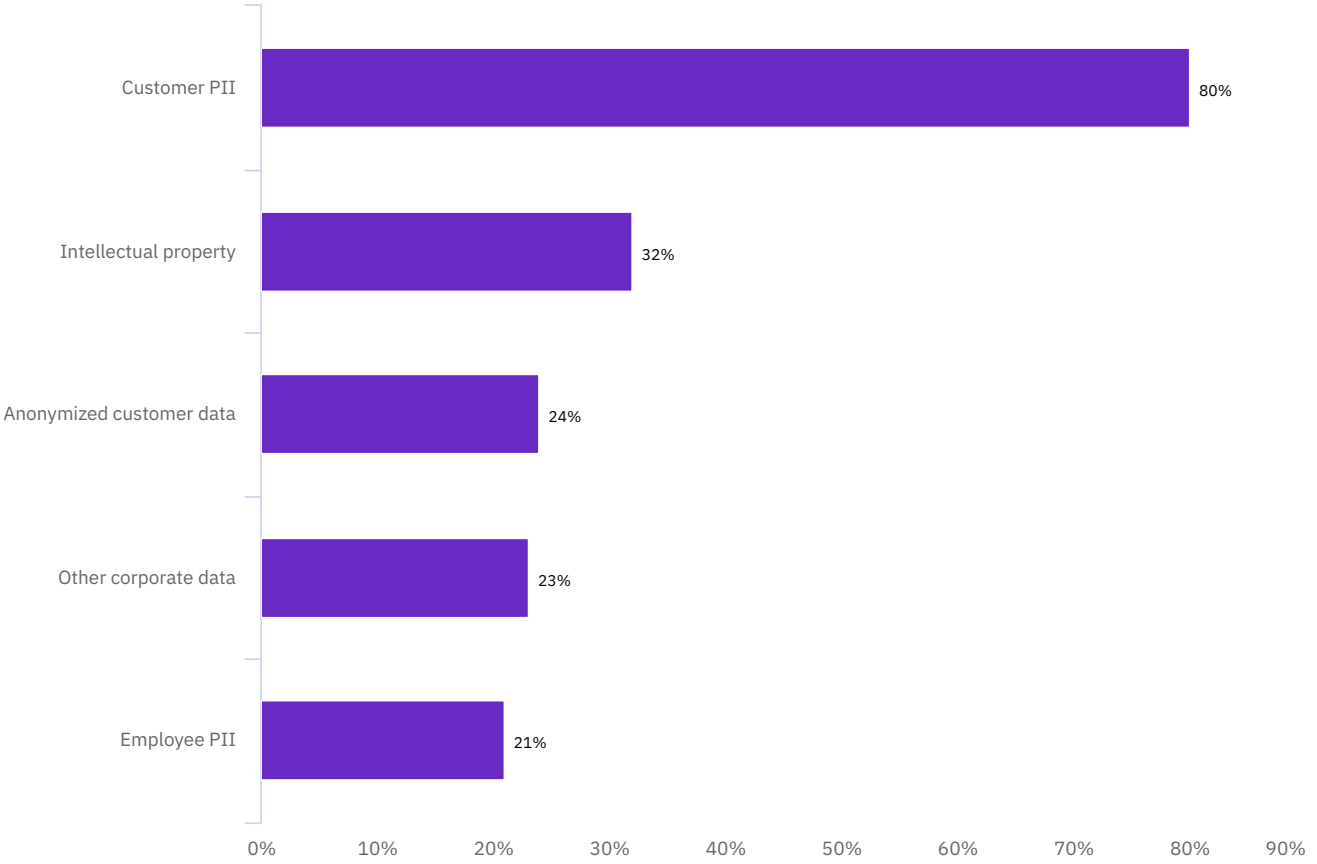

### The per record cost of a data breach decreased slightly to $146.

**Figure 3** shows the average data breach cost per compromised record over the past seven years. The weighted average over seven years is $149 per record.

**Figure 4**

## Types of records compromised

Percentage of breaches involving data in each category



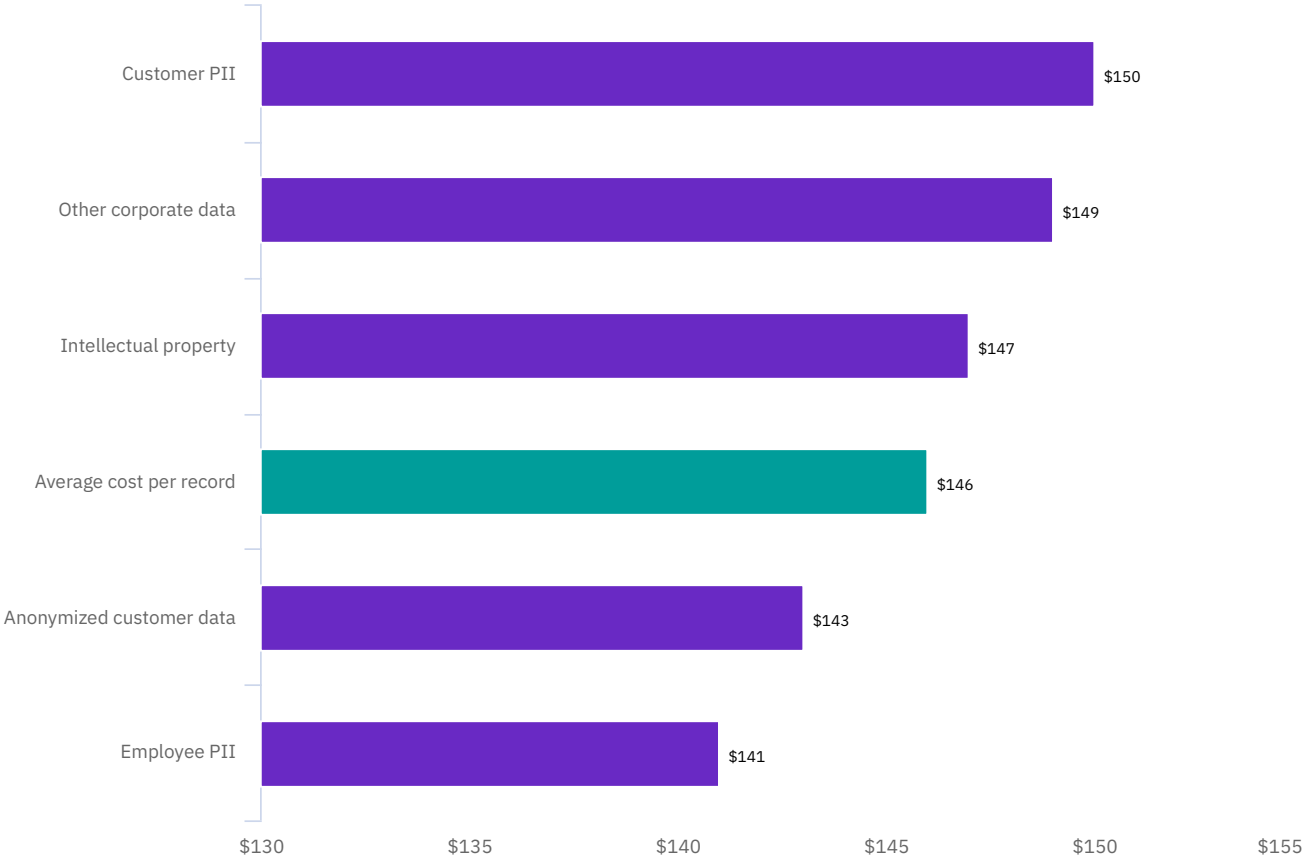

### Customer PII was the type of data most often lost or stolen in breaches.

**Figure 4** shows that 80% of data breaches included customer PII. Intellectual property was compromised in 32% of breaches, while anonymized customer data was compromised in 24% of breaches.

**Figure 5**

## Average cost per record by type of data compromised

Measured in US$



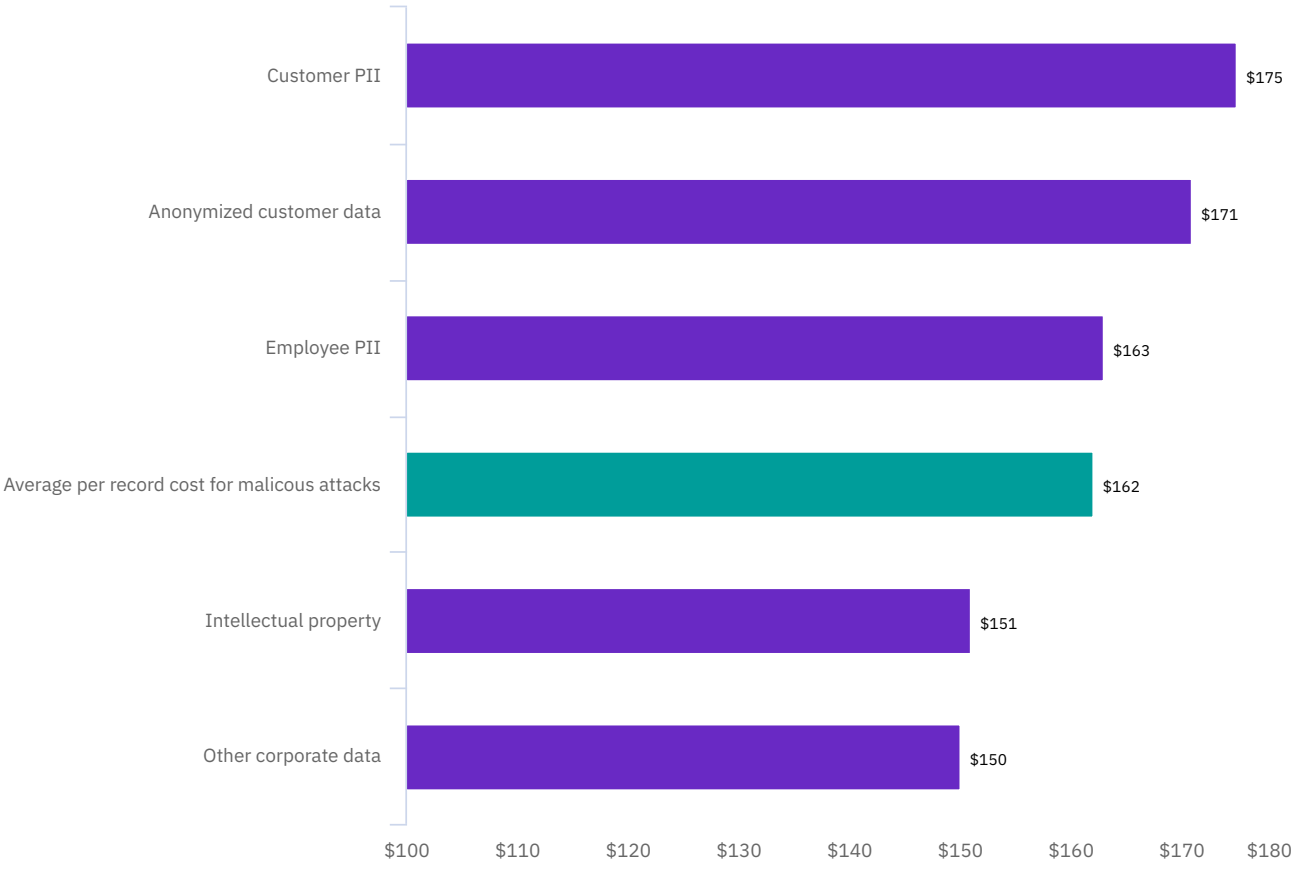

### Customer PII was the costliest type of data compromised in breaches.

Customer PII cost an average of $150 per lost or stolen record, as shown in **figure 5**. Intellectual property cost $147 per record, anonymized customer data (non PII) cost $143 per record and employee PII cost $141 per record.

**Figure 6**

## Average cost per record by type of data compromised in a malicious attack

Measured in US$



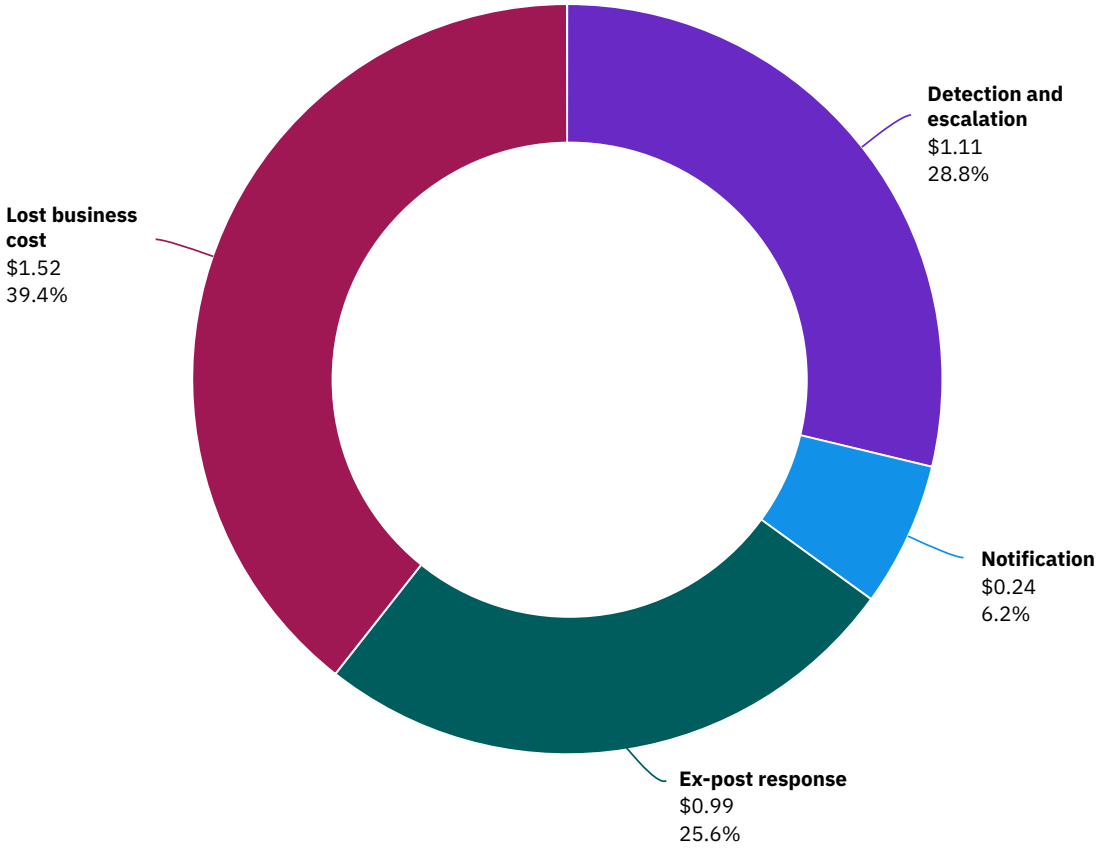

## Per record costs were higher in breaches resulting from malicious attacks.

As shown in **figure 6**, the per record cost of customer PII was $175 in malicious attacks, nearly 17% more than the overall average per record cost of customer PII ($150 per record) compromised in any type of breach.

**Figure 7**

## Data breach average total cost divided into four categories

Measured in US$ millions



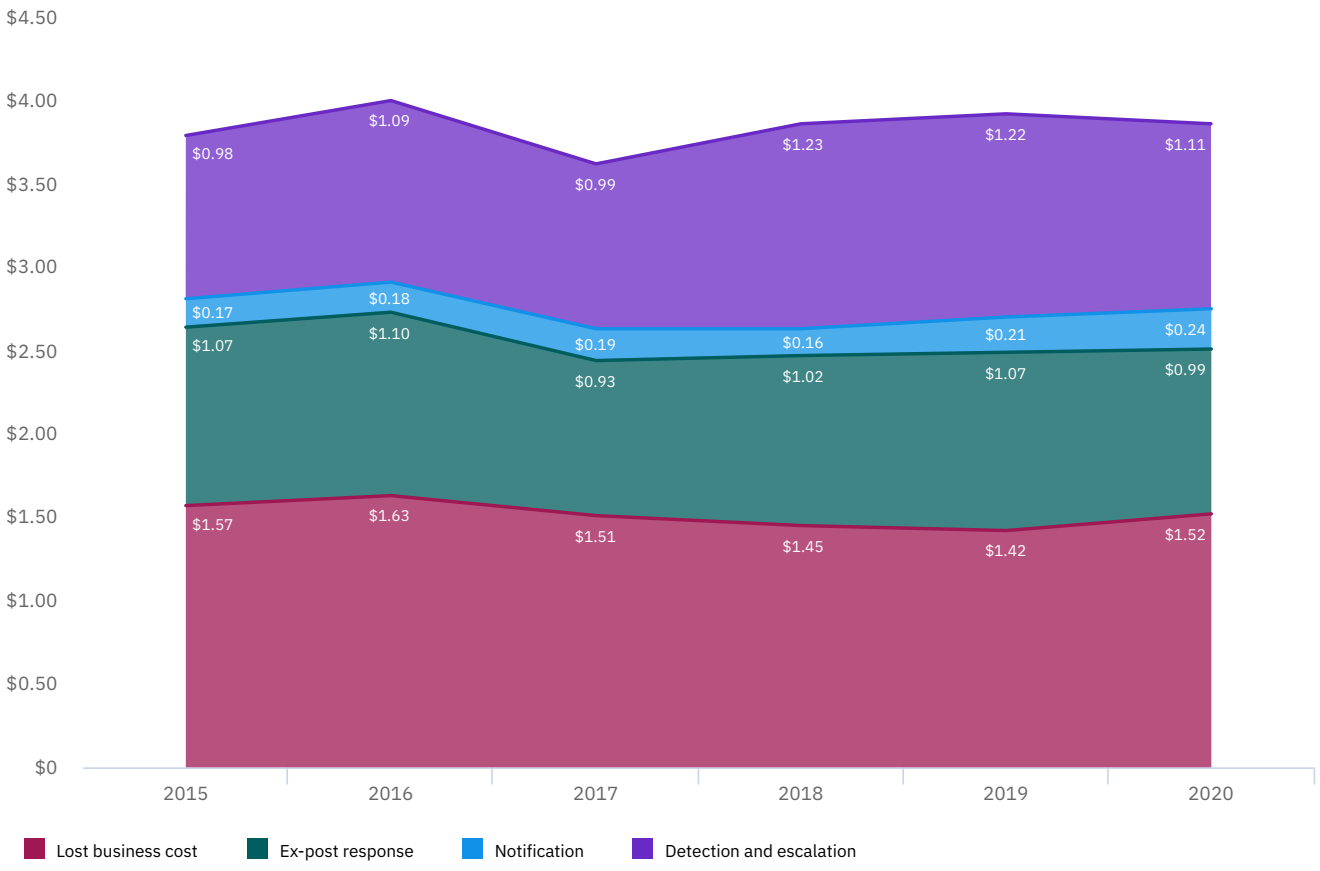

### Lost business costs comprised the largest share of the average cost of a data breach.

**Figure 7** presents the four cost segments in US dollars and percentage of the total cost of a data breach. Lost business cost an average of $1.52 million or 39% of total cost. The lowest cost was for notification of the data breach, at $240,000 or 6% of total cost.

**Figure 8**

## Trend in average data breach cost in four categories

Measured in US$ millions



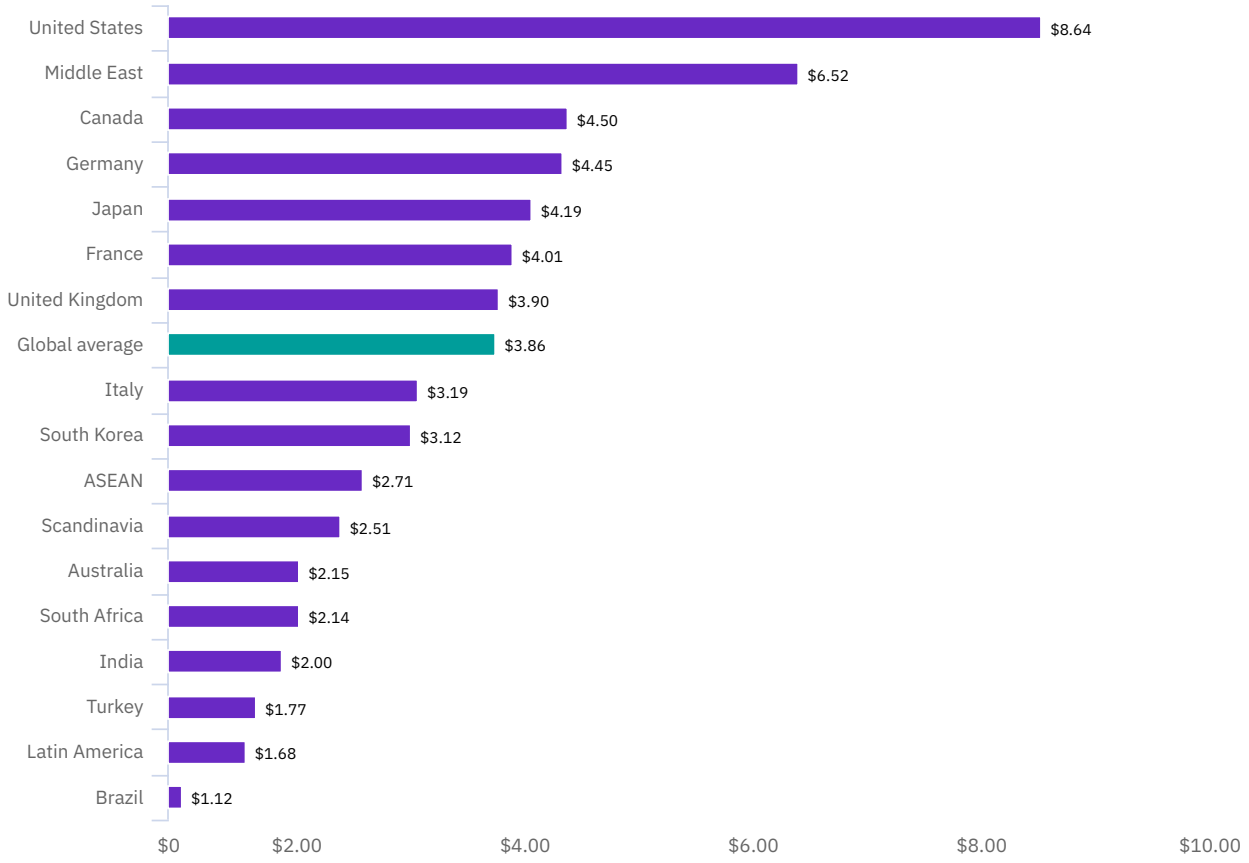

## Lost business costs increased slightly year over year.

**Figure 8** shows trends in the cost of lost business, ex-post response, notification and detection and escalation over the past six years. The pattern shows consistency in these costs. Notification continues to be the lowest and lost business is the highest cost component.

**Figure 9**

## Average total cost of a data breach by country or region

Measured in US$ millions



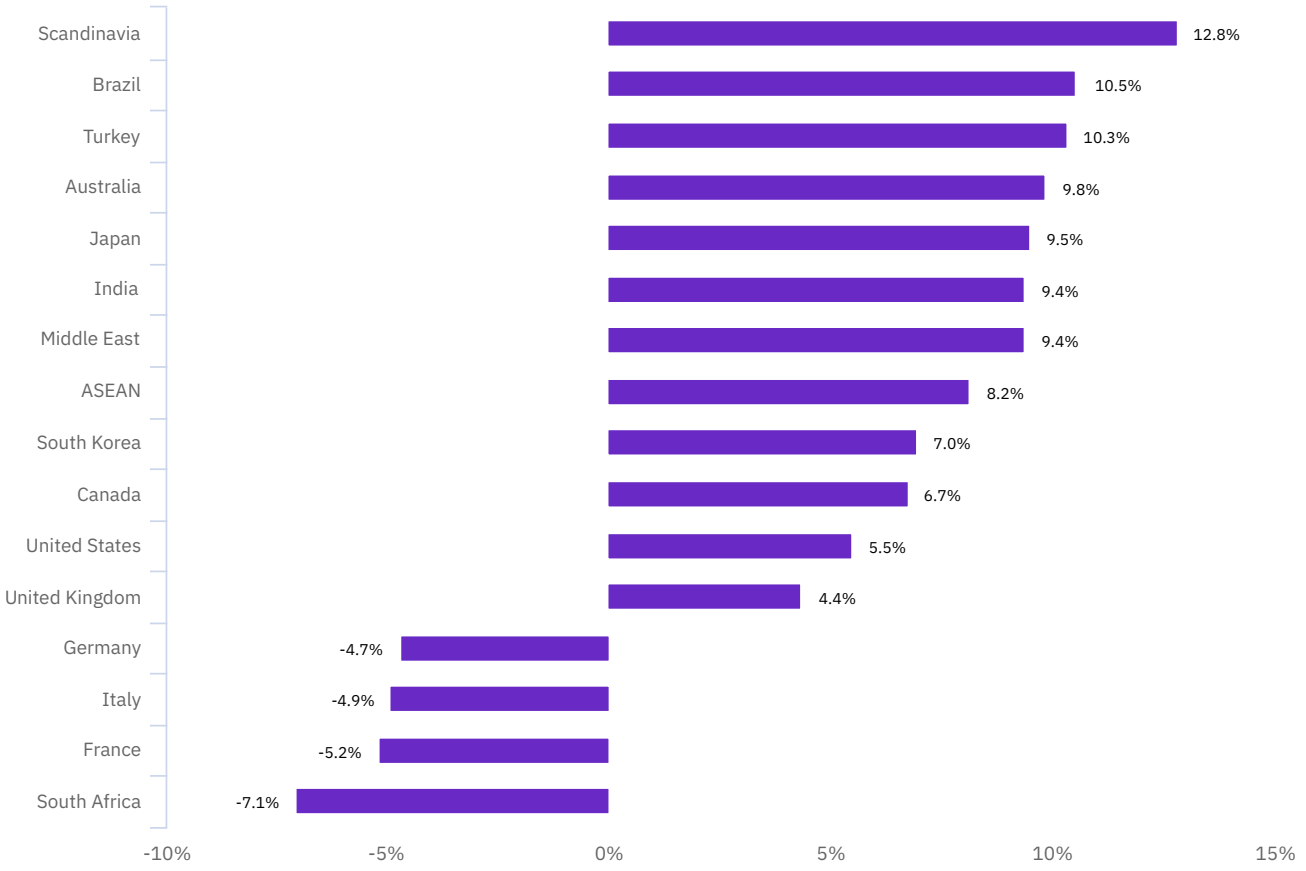

### The average total cost of a data breach varied by country.

**Figure 9** shows the average total cost of a data breach by country. Organizations in the United States had the highest average total cost at $8.64 million, followed by the Middle East at $6.52 million. In contrast, Latin American and Brazilian organizations had the lowest average total cost at $1.68 million and $1.12 million, respectively.

**Figure 10**

## Percent change in average total cost by country or region, 2019-2020

Calculated using local currency



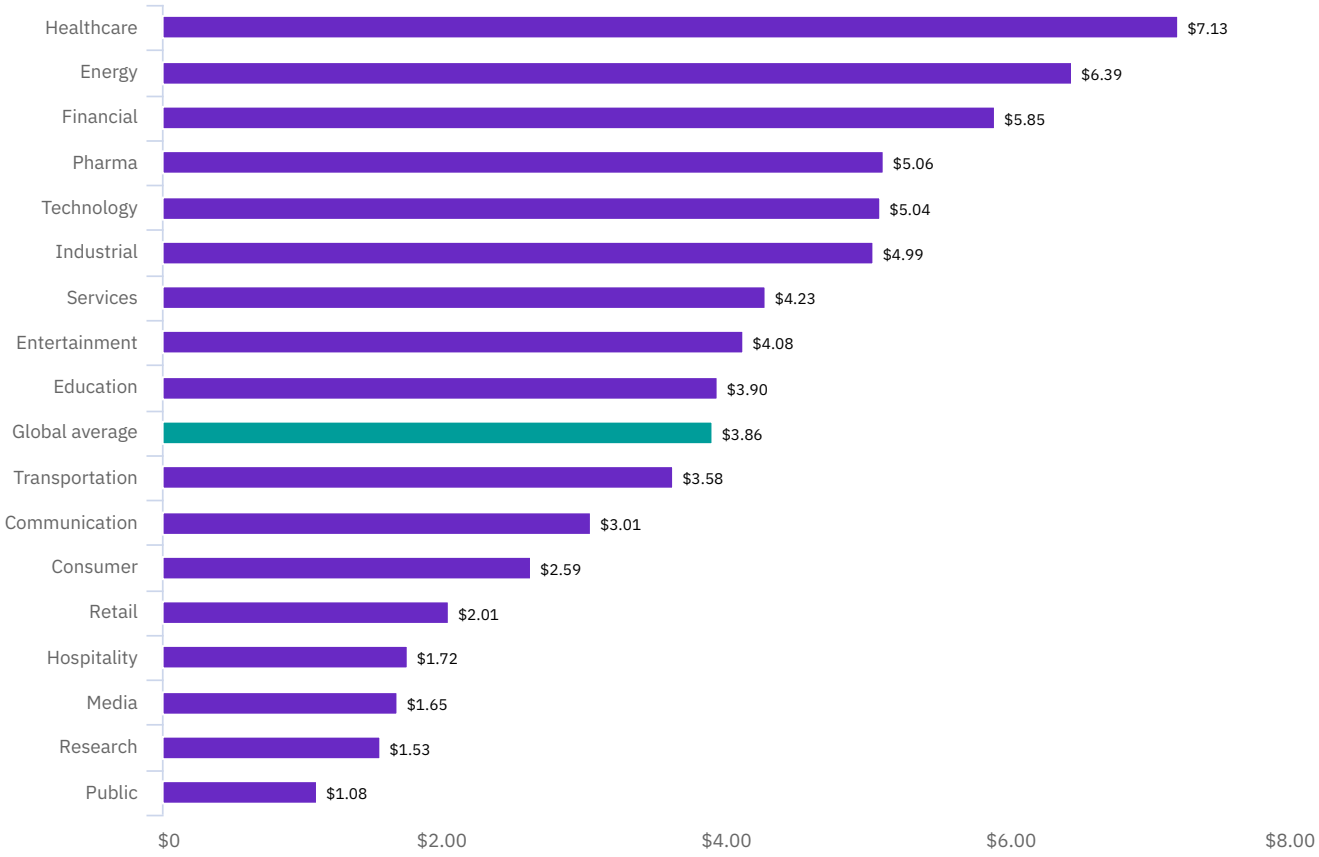

### The average total cost of a data breach increased in 12 of 16 countries.

As shown in **figure 10**, Scandinavia had the greatest increase in the total cost of a data breach and France and South Africa had the greatest decrease, from 2019 to the 2020 study.

**Figure 11**

## Average total cost of a data breach by industry

Measured in US$ millions

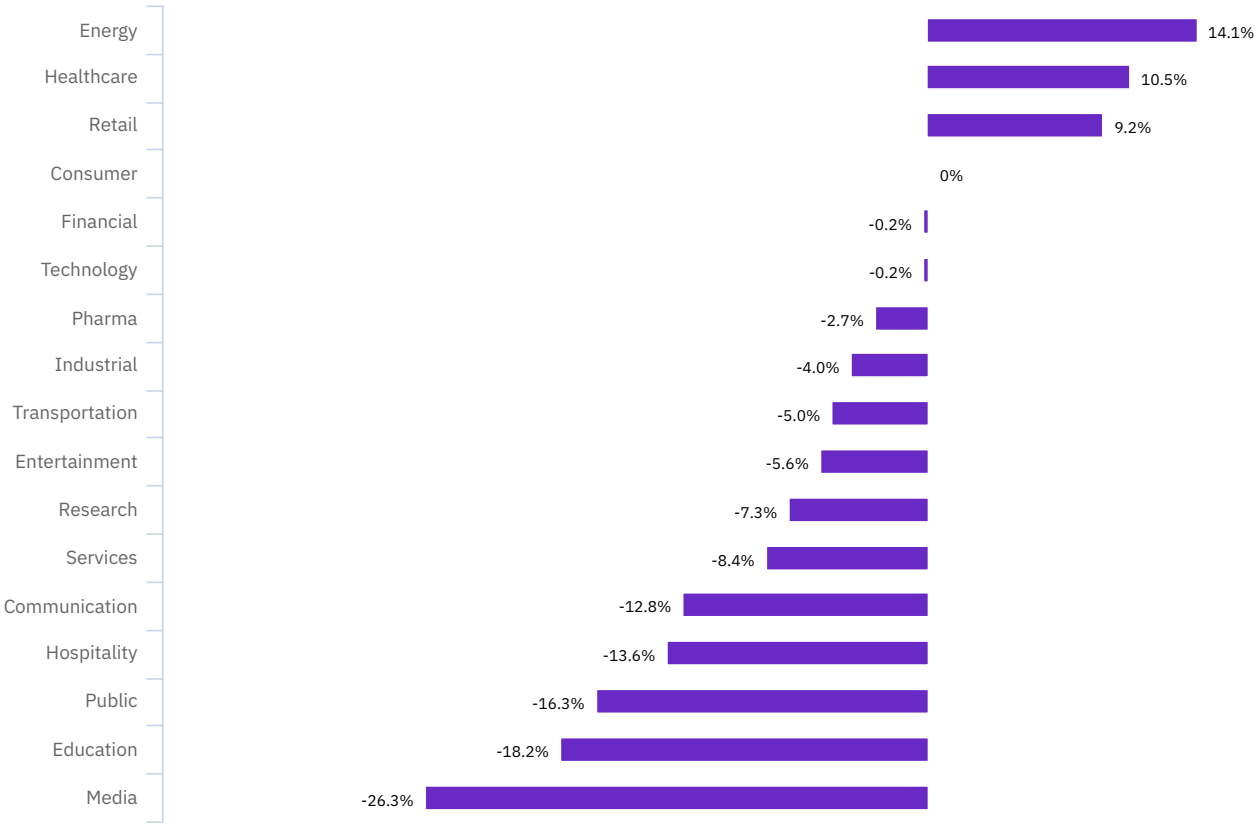



### Organizations subject to more rigorous regulatory requirements had higher average data breach costs.

As shown in **figure 11**, healthcare, energy, financial services and pharmaceuticals experienced an average total cost of a data breach significantly higher than less regulated industries such as hospitality, media and research. Public sector organizations traditionally have the lowest cost of a data breach in this research, because they are unlikely to experience a significant loss of customers as a result of the data breach.

**Figure 12**

## Percent change in average total cost by industry, 2019-2020



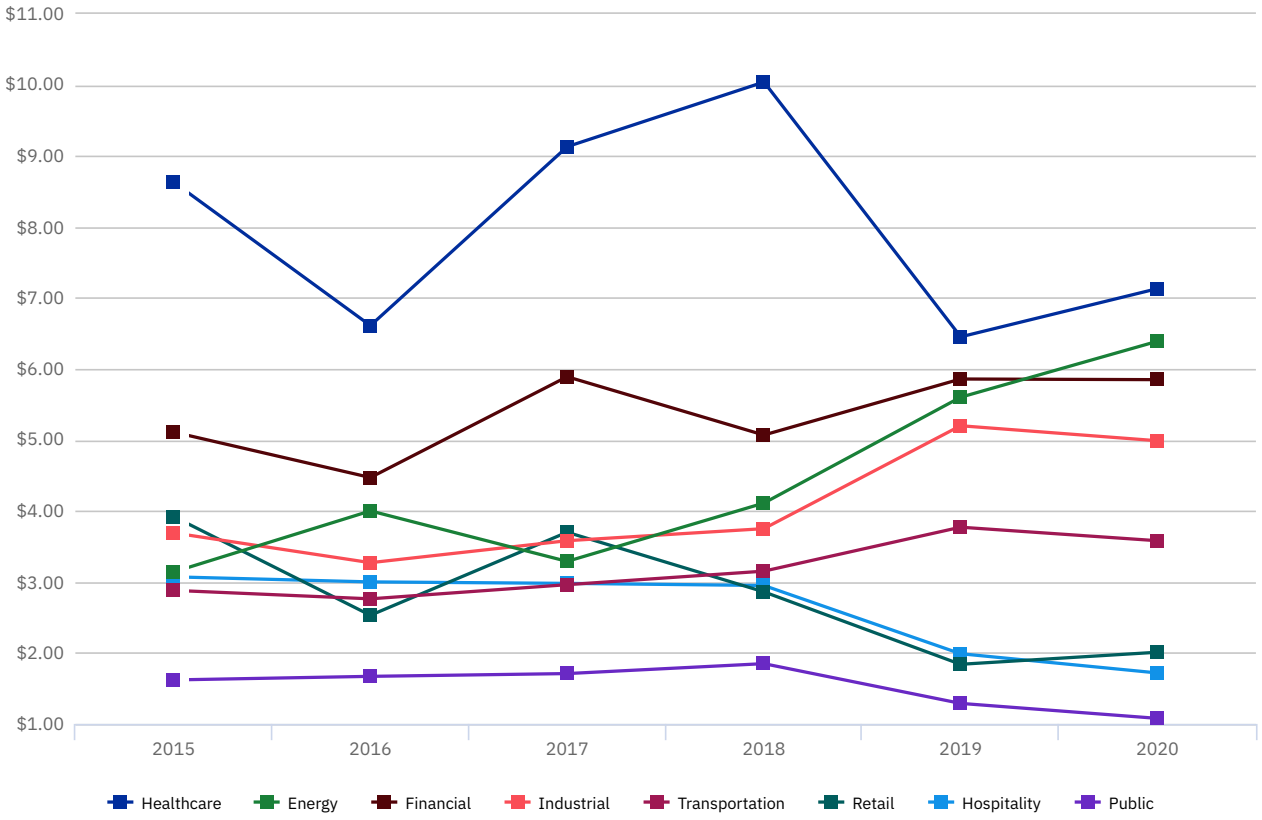

### Energy, healthcare and retail industries experienced the greatest increase in data breach costs.

**Figure 12** reveals that an increase in data breach costs occurred in only three of 17 industries between the 2019 study and the 2020 study. Energy, healthcare and retail experienced the highest increases in the average total cost, while public sector, education and media had the greatest decreases.

**Figure 13**

## Trend in average total cost of a data breach in eight industries

Measured in US$ millions



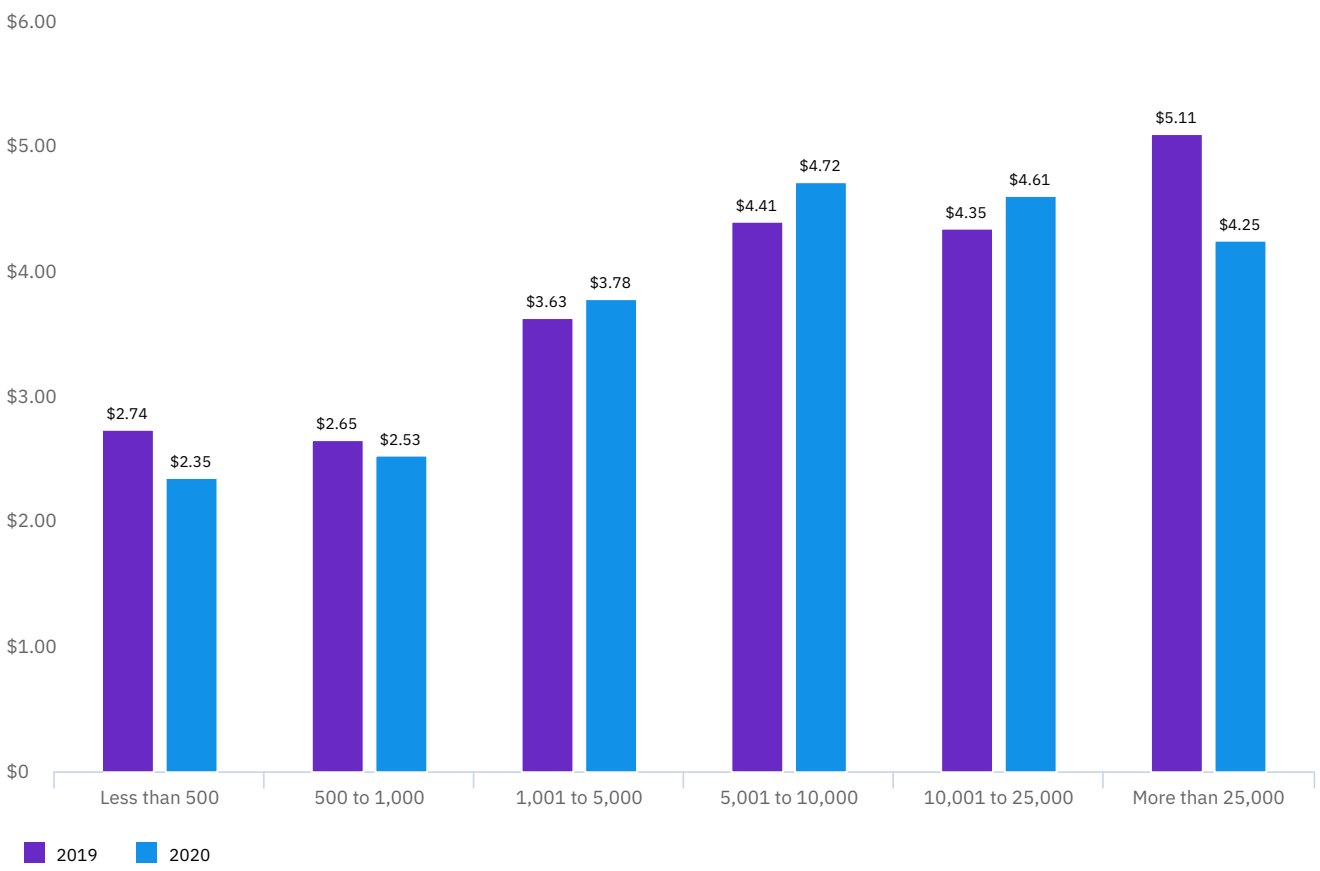

## Healthcare and financial industries have consistently had the highest data breach costs.

**Figure 13** presents a line graph for each of eight industry sectors over the past six years. Healthcare has consistently had the highest cost and public sector consistently the lowest cost.

**Figure 14**

## Average total cost of a data breach by organizational size

Measured in US$ millions




## The average cost of a data breach increased for mid-sized organizations.

**Figure 14** shows the average total cost of a data breach decreased between the 2019 and 2020 studies for the smallest organizations (1,000 or fewer employees) and for the largest organizations (more than 25,000 employees). Organizations with more than 25,000 employees experienced a drop in average total costs from $5.11 million in 2019 to $4.25 million in 2020, which is a 16.8% decrease. For mid-sized organizations, however, total breach costs increased on average. In the 5,001 to 10,000 employee range, breach costs increased from an average of $4.41 million in 2019 to $4.72 million in 2020, a 7% increase. Proportionately, smaller organizations had higher average costs per employee.

# Root causes of a data breach

For several years this research study has asked participants what caused the data breach. In prior years, these root causes were grouped in three categories: system glitches, including both IT and business process failures; human error, including negligent employees or contractors who unintentionally cause a data breach; and malicious attacks, which can be caused by hackers or criminal insiders.

This year's study continues to report on the breaches in these three categories. However, in a deeper analysis, we asked participants to provide more detailed information about the cause of malicious attacks, including initial threat vector and type of attacker. In this section we report the results of both these analyses.

## Key findings

52%

Share of breaches caused by malicious attacks, at an average cost of $4.27 million

19%

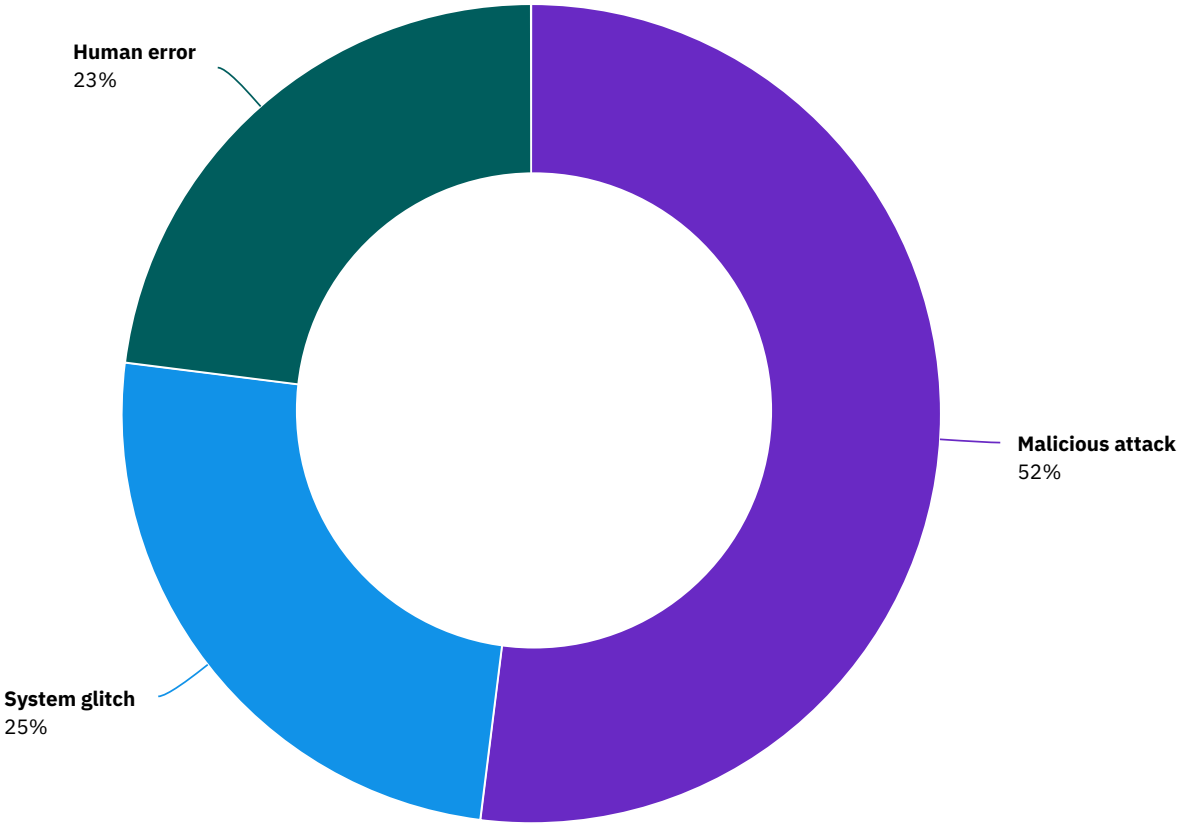
Share of malicious breaches caused by compromised credentials (19%) and cloud misconfiguration (19%)

$4.43 million

Average cost of breaches caused by nation state attackers, responsible for 13% of malicious breaches

**Figure 15**

## Data breach root cause breakdown in three categories



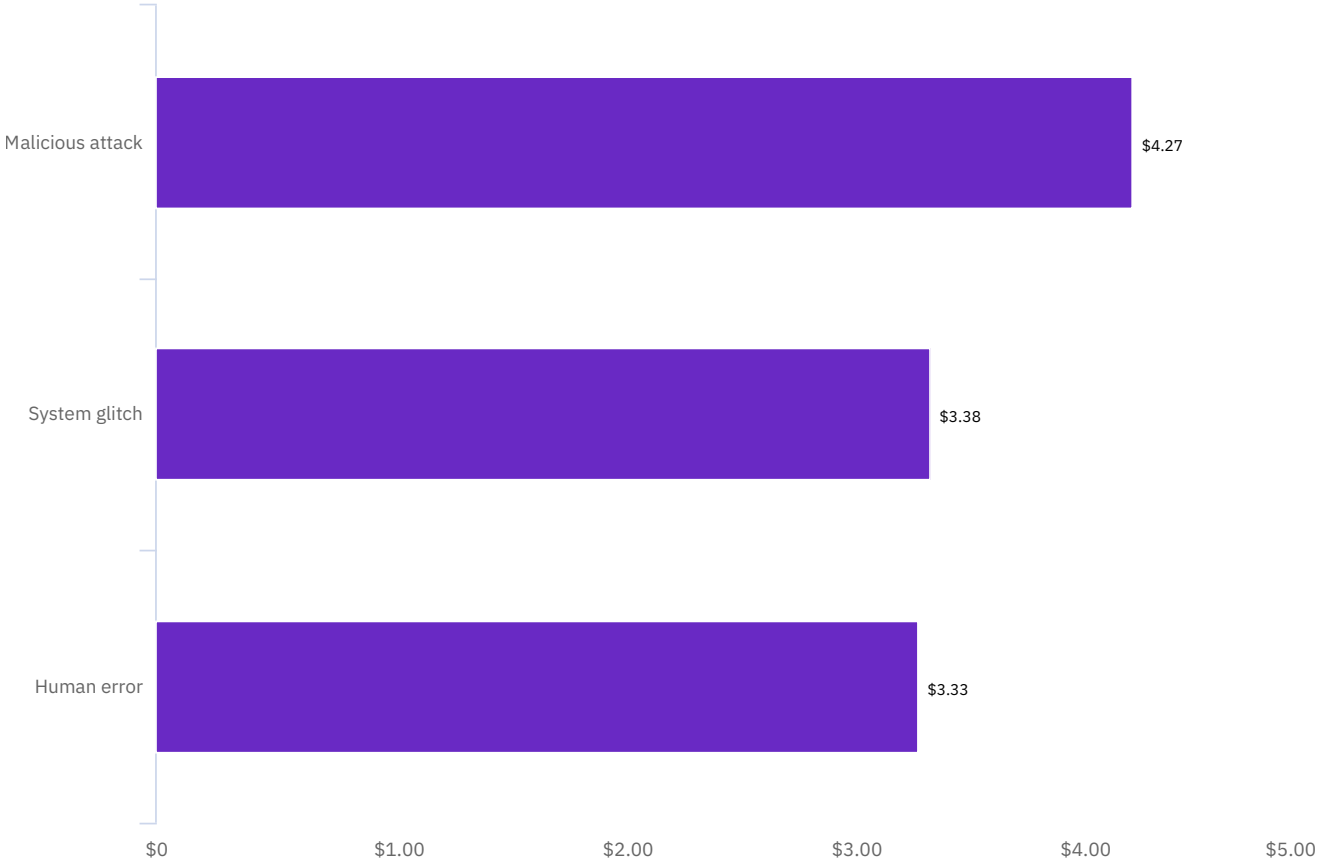

### Malicious attacks caused a majority of data breaches.

**Figure 15** provides a summary of the three major categories for root causes of data breach. Fifty-two percent of incidents involved a malicious attack, compared to 25% caused by system glitches and 23% caused by human error.

**Figure 16**

## Average total cost for three data breach root causes

Measured in US$ millions



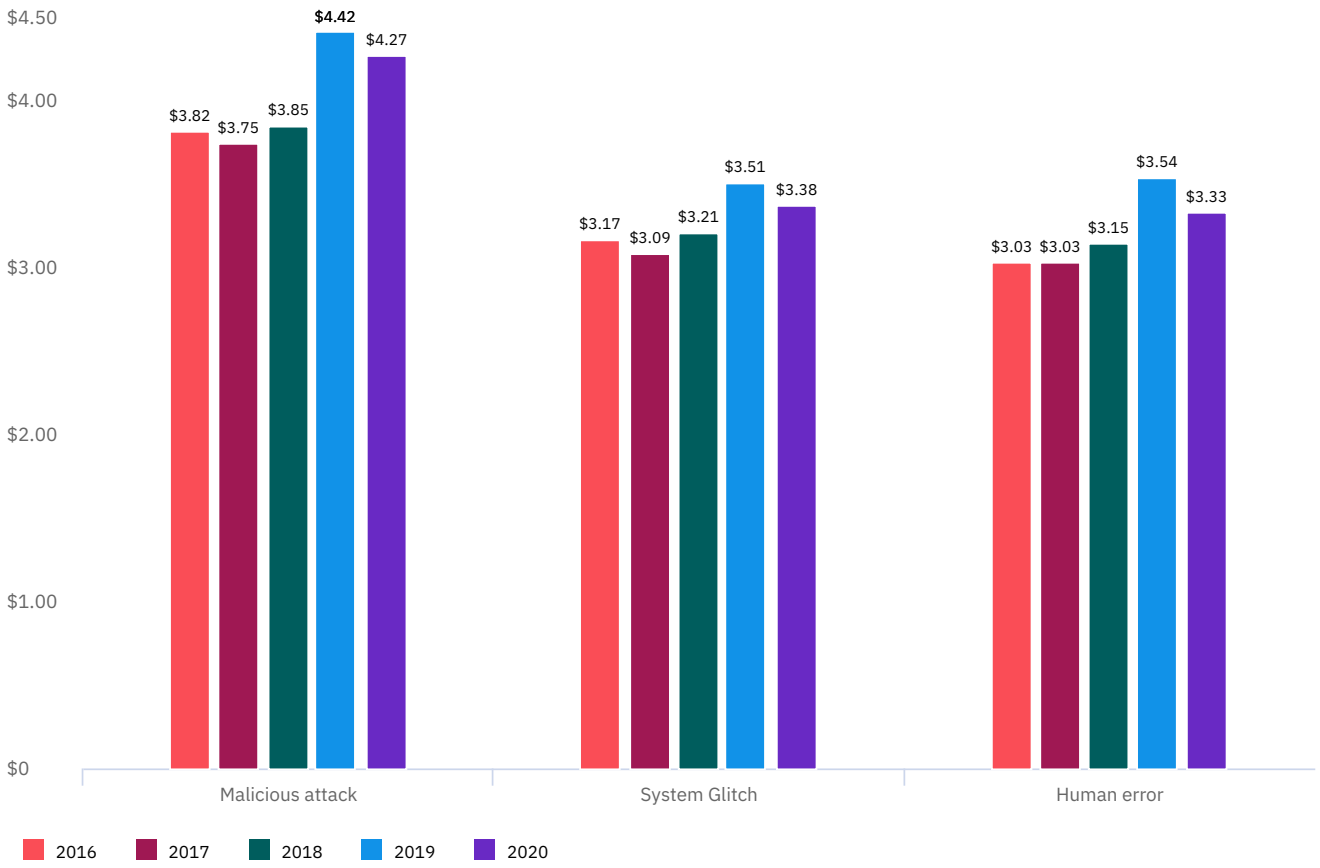

### Malicious attack was the most expensive root cause.

Malicious attack breaches in the 2020 study cost an average of $4.27 million, nearly $1 million more than breaches caused by a system glitch or human error, as shown in **figure 16**.

**Figure 17**

## Trend in average total cost by root cause of the data breach

Measured in US$ millions

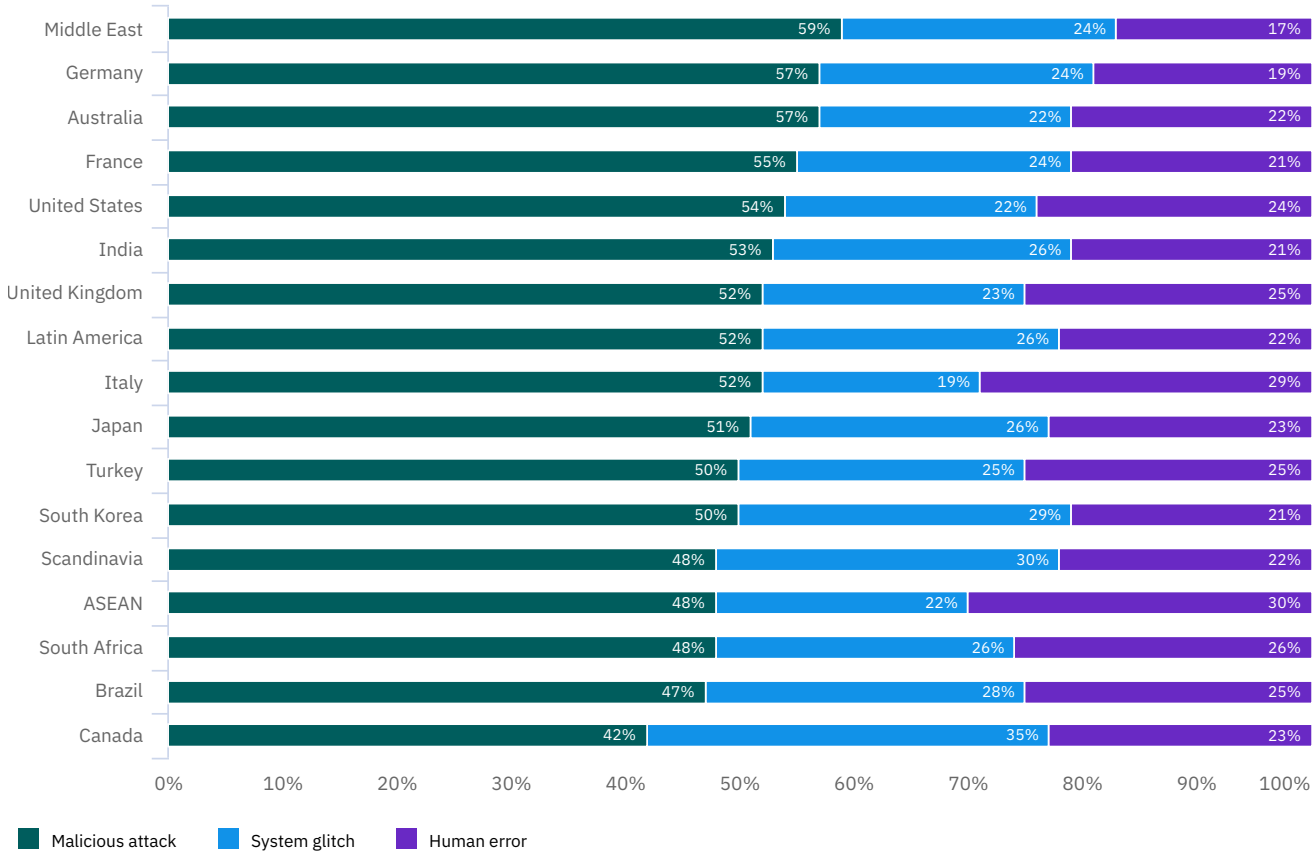



## Malicious breaches have remained the costliest over the past five years.

**Figure 17** shows the average total cost for the three data breach root causes over the past five years. Since the 2016 study, the pattern of root causes has stayed fairly constant, with a slight decrease in costs in the 2020 study compared to 2019. The average total cost of a malicious breach has increased by nearly 12% since the 2016 study.

**Figure 18**

## Breakdown of data breach root causes by country or region

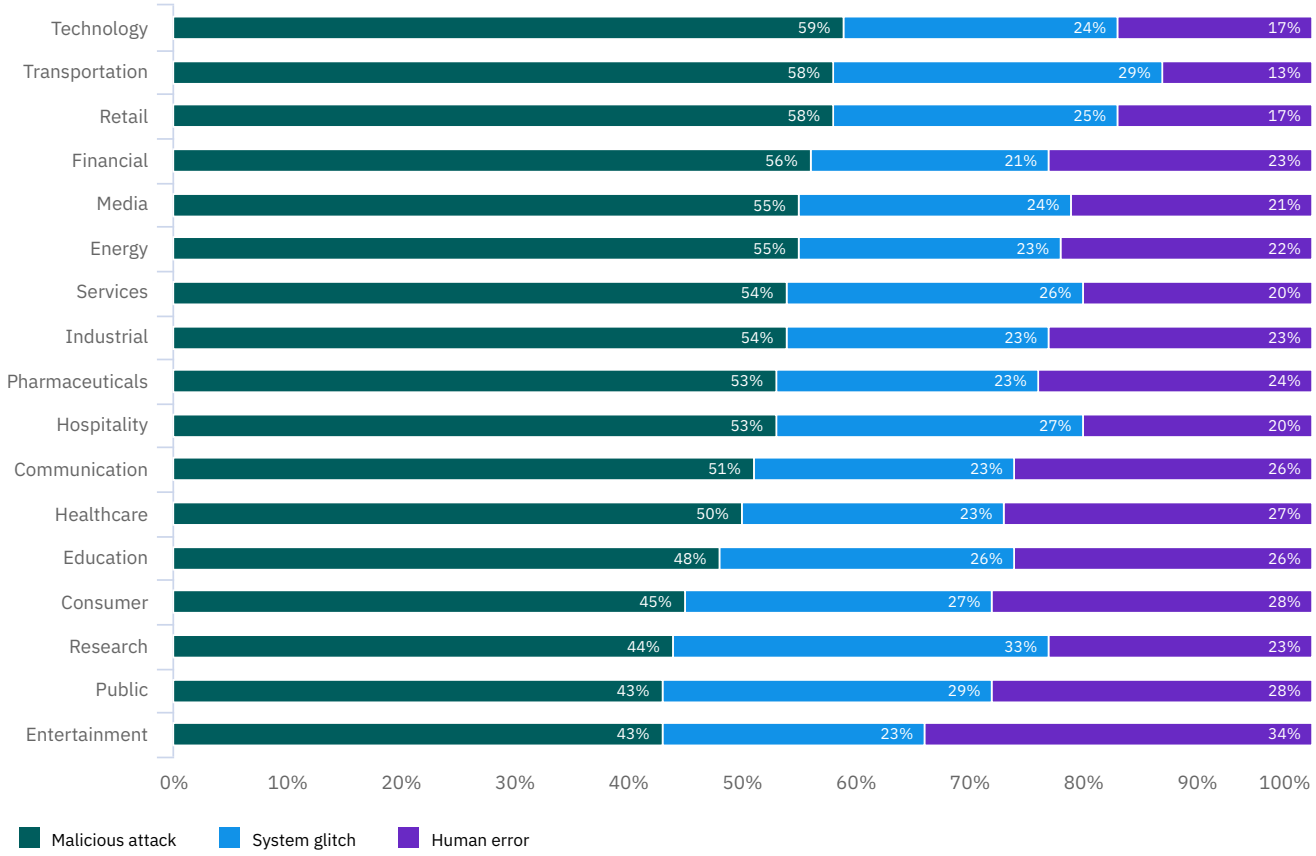



### Root causes of breaches varied by geography.

The Middle East, Germany and Australia had the highest percentage of breaches caused by malicious attacks, while South Africa, Brazil and Canada had the lowest percentage of malicious attacks, according to **figure 18**. Data breaches caused by system glitches are highest in Canada. ASEAN and Italy had the highest percentage of data breaches caused by human error.

**Figure 19**

# Breakdown of data breach root causes by industry



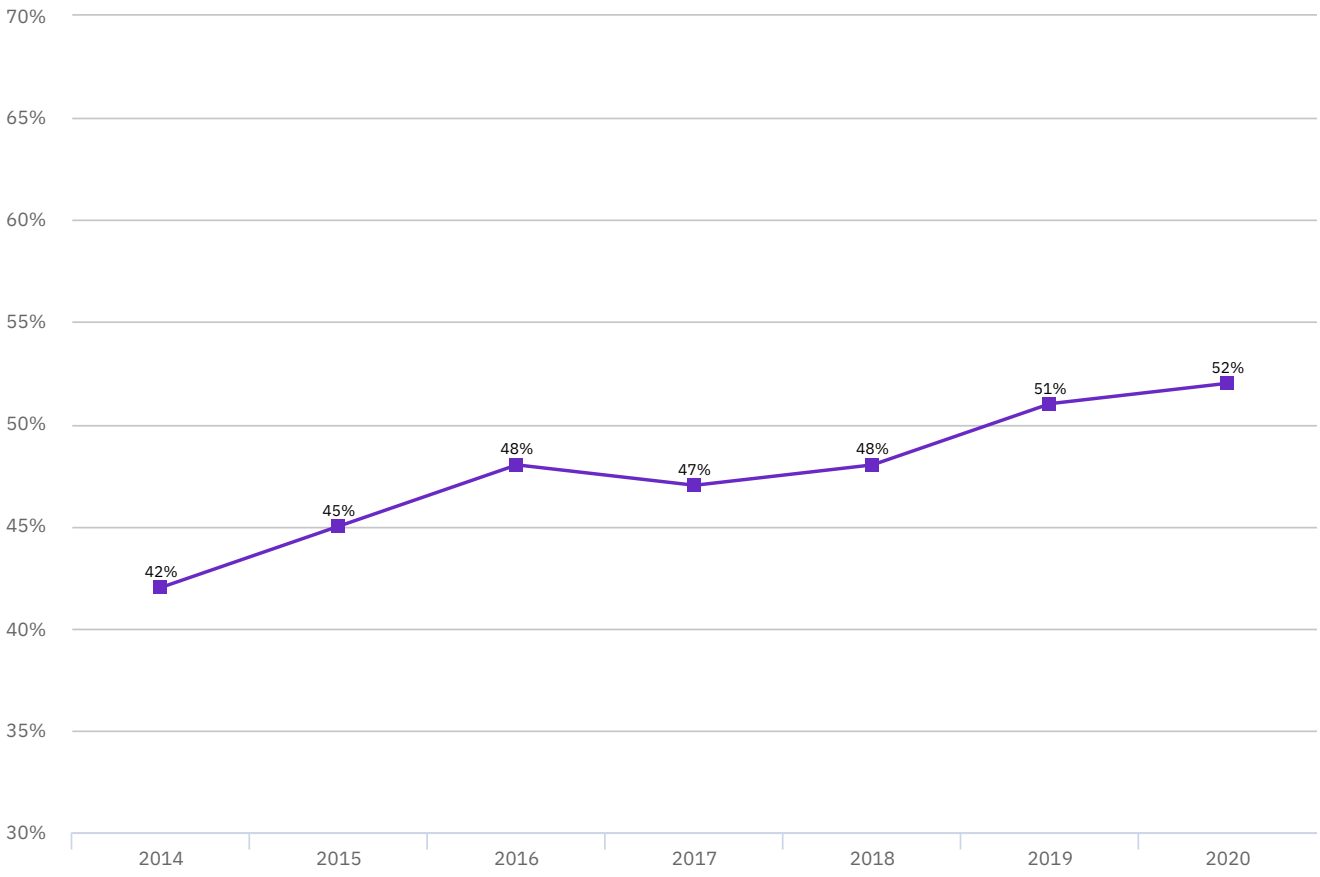

## Industries varied in breakdown of data breach root causes.

As shown in **figure 19**, technology, transportation, retail and financial had the highest percentage of malicious attacks. Entertainment, public sector and consumer industries had the highest percentage of data breaches caused by human error. System glitches were more frequently the root causes of a breach in research, public sector and transportation.

**Figure 20**

## Trend in data breaches caused by a malicious attack

Percentage of all breaches



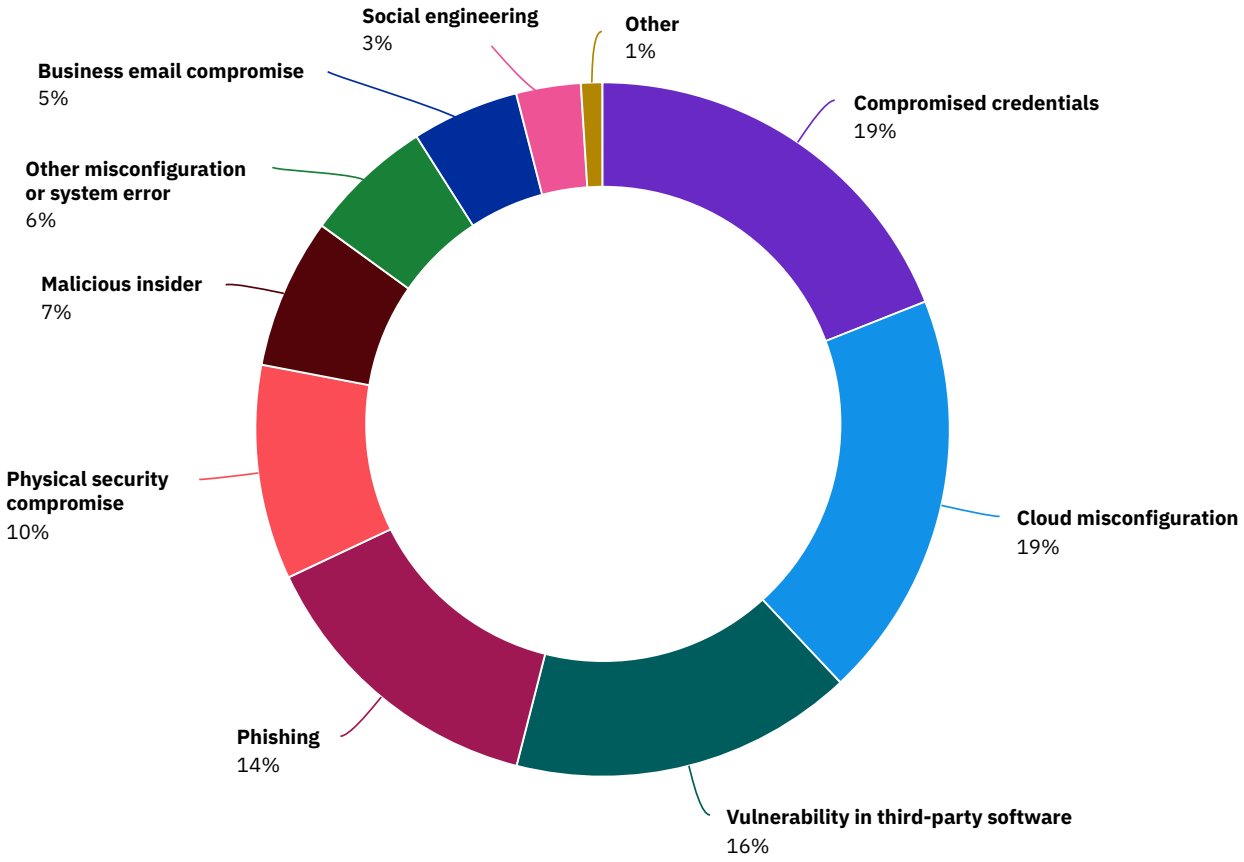

### The share of breaches caused by malicious attacks steadily increased over time.

**Figure 20** shows the share of breaches caused by malicious attacks increased from 42% in the 2014 report to 52% in the 2020 report. This 10 percentage point increase represents a nearly 24% increase (growth rate) in the share of breaches caused by malicious attacks.

**Figure 21**

## Breakdown of malicious data breach root causes by threat vector

Percentage of breaches caused by malicious attack

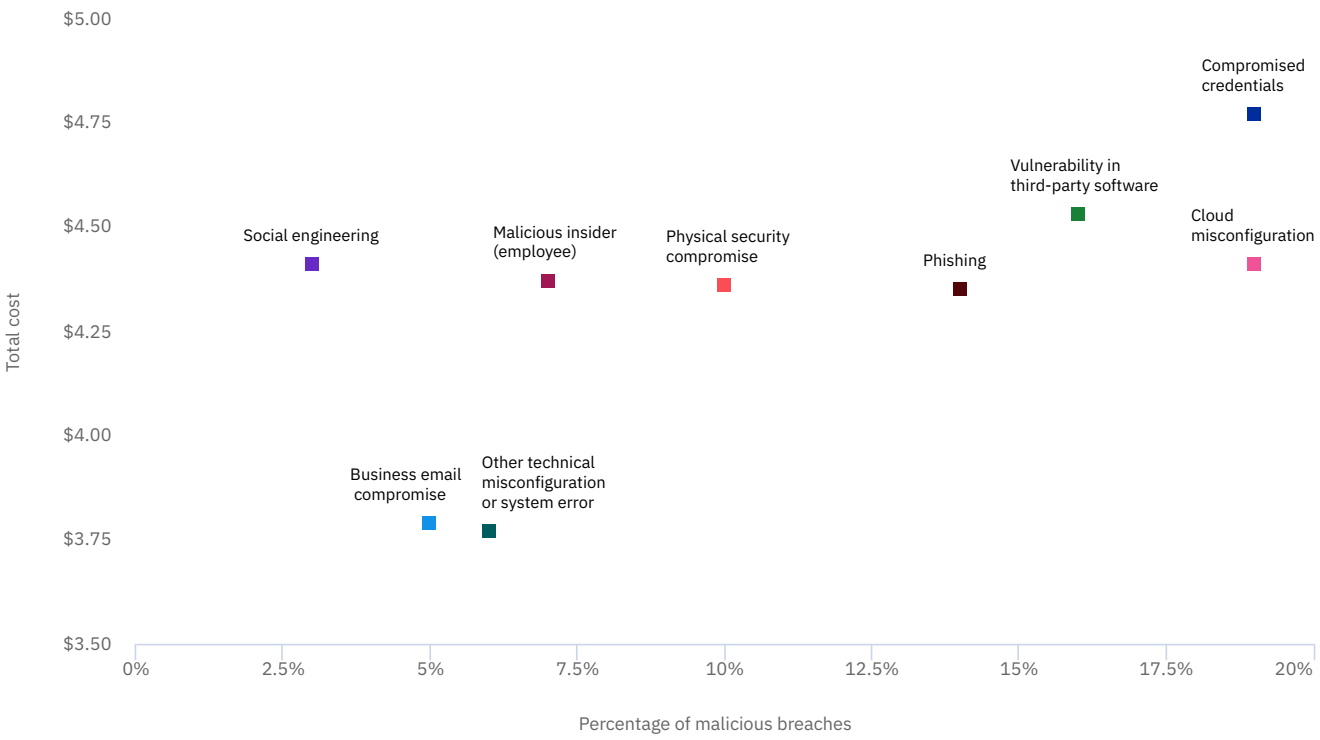



### A majority of malicious breaches were caused by compromised credentials, cloud misconfiguration or a third-party software vulnerability.

Stolen or compromised credentials and cloud misconfiguration were the leading initial threat vectors, each responsible for 19% of malicious breaches. Third-party software vulnerability was the initial threat vector in 16% of malicious breaches, according to **figure 21**.

**Figure 22**

## Average cost and frequency of malicious data breaches by root cause vector

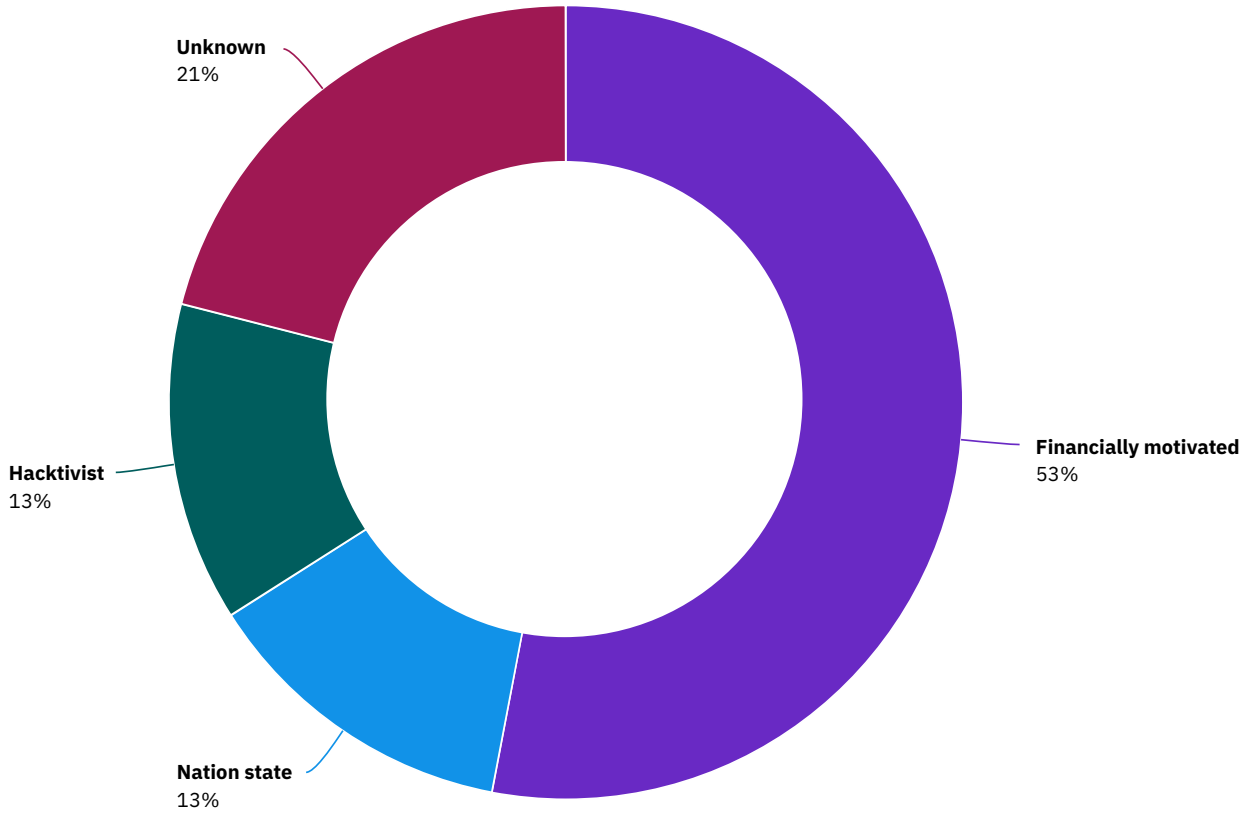



### Compromised credentials were the costliest and most frequent threat vector.

**Figure 22** shows nine initial threat vectors in malicious breaches on a scatter plot, with the percentage of breaches represented on the X-axis and the average total cost on the Y-axis. Compromised credentials is the threat vector furthest to the upper right of the graph, showing its potent combination of frequency and cost in malicious data breaches.

**Figure 23**

## Malicious data breaches organized by threat actor type



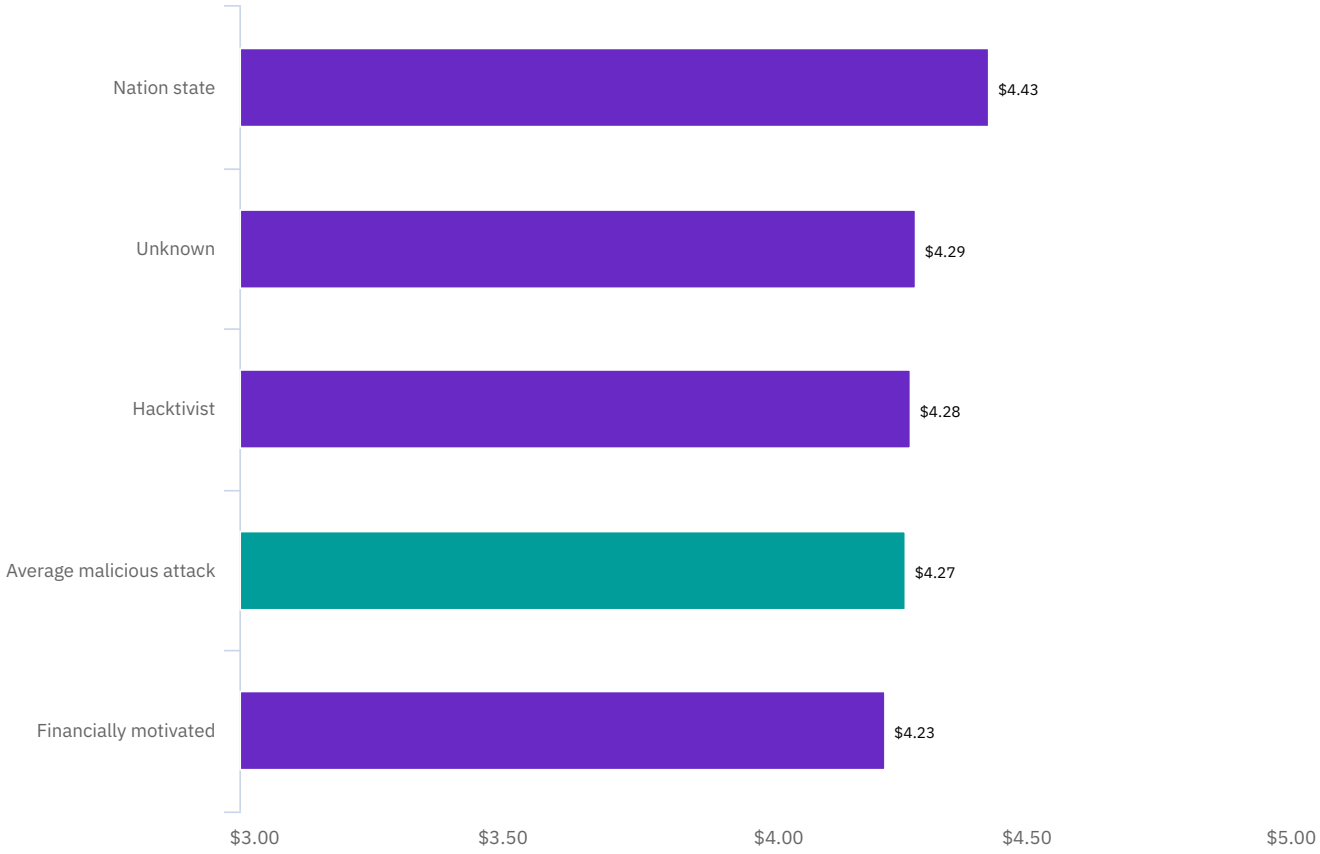

### Financially motivated attackers caused the majority of malicious data breaches.

According to **figure 23**, a majority of malicious breaches, 53%, were caused by financially motivated attackers. Nation state threat actors were involved in 13% of malicious breaches, hacktivists in 13%, and 21% of this type of data breach was caused by attackers of unknown motivation.

**Figure 24**

## Average cost of a malicious data breach by threat actor type

Measured in US$ millions



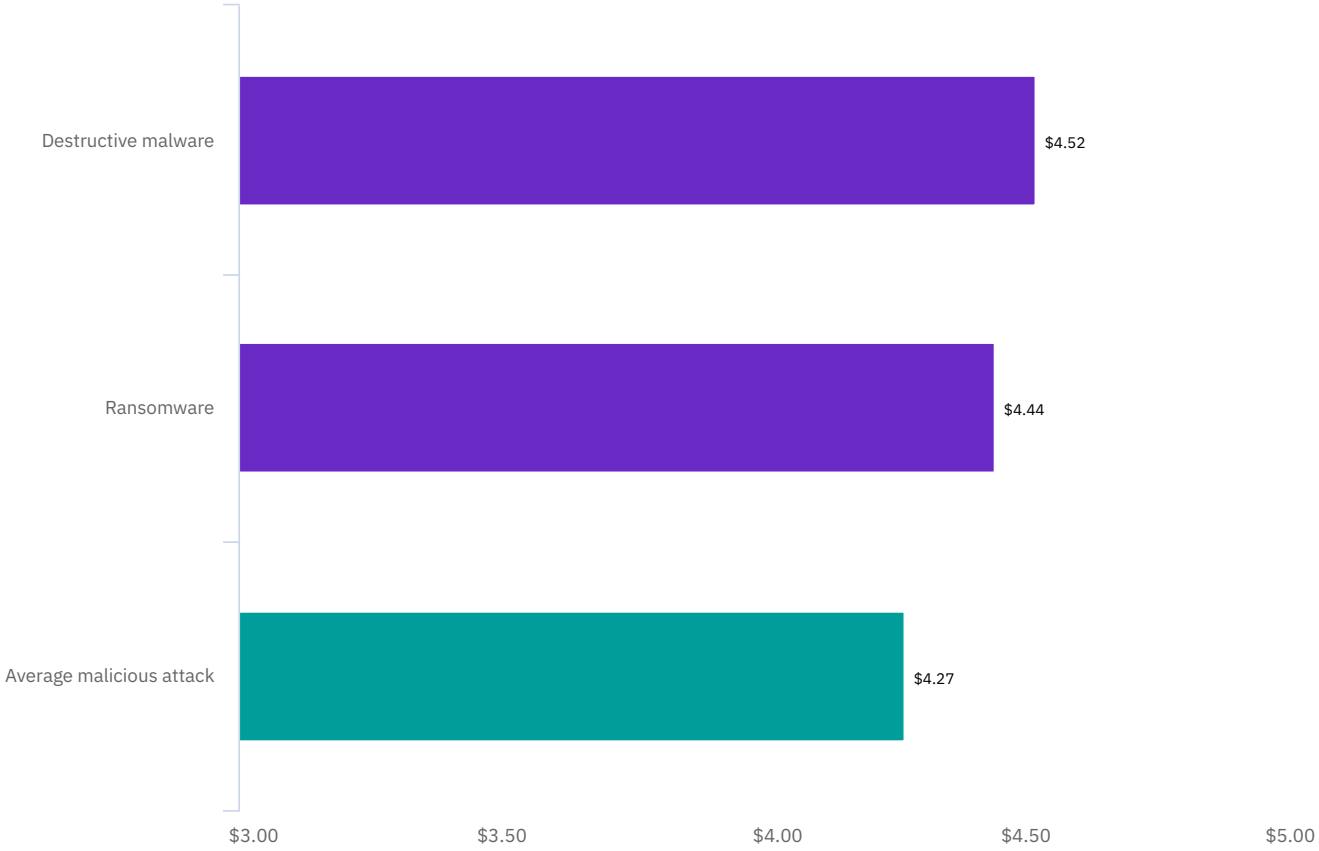

### Nation state attackers caused the most expensive malicious breaches.

**Figure 24** presents the cost of a data breach by type of threat actor. The costliest malicious breaches were caused by nation state actors, at an average of $4.43 million. Hacktivists were responsible for malicious breaches that cost an average of $4.28 million, while breaches caused by financially motivated cybercriminals cost an average of $4.23 million.

**Figure 25**

## Average cost of a ransomware or destructive malware breach

Measured in US$ millions




### Ransomware and destructive malware breaches cost more than the average malicious attack.

Malicious attacks that destroyed data in destructive/wiper-style attacks (average cost of $4.52 million) and ransomware attacks ($4.44 million) were more expensive than the average malicious breach ($4.27 million) or the average data breach ($3.86 million), as shown in **figure 25**.

# Factors that influence the cost of a data breach

This section looks deeper at a multitude of factors that influence the costs of a data breach, including various types of security technologies and practices, IT environments and involvement by third parties. This year's study includes an analysis of 25 unique cost factors that had either a mitigating influence (decreasing the average total cost of a breach) or an amplifying influence (increasing the average total cost of a breach).

Several factors are new to the report this year: red team testing, vulnerability testing and managed security services (which were mitigating cost factors) and security skills shortage and remote workforce (which were amplifying cost factors).

This section also looks deeper at three areas that were shown to have a mitigating influence on data breach costs: the role of the CISO, cyber insurance and incident response teams.

## Key findings

**$291,870**

Increase to the average total cost of a data breach associated with complex security systems

**51%**

Share of organizations with cyber insurance that used claims to cover the cost of consulting and legal services

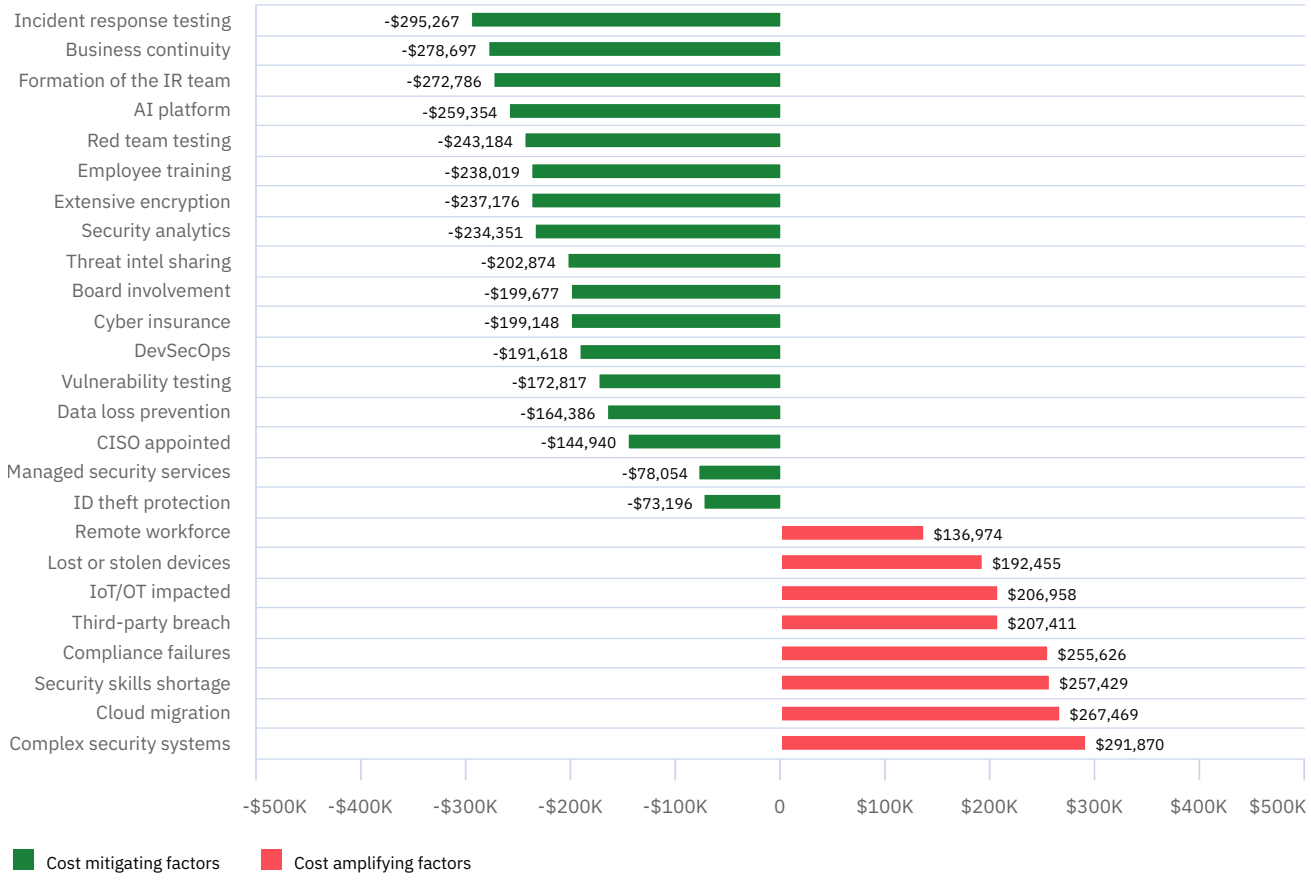
**46%**

Share of respondents who said the CISO is most responsible for the data breach

**Figure 26**

# Impact of 25 key factors on the average total cost of a data breach

Change in US$ from average total cost of $3.86 million




## Security system complexity and incident response plan testing had the biggest impact on the total cost of a data breach.

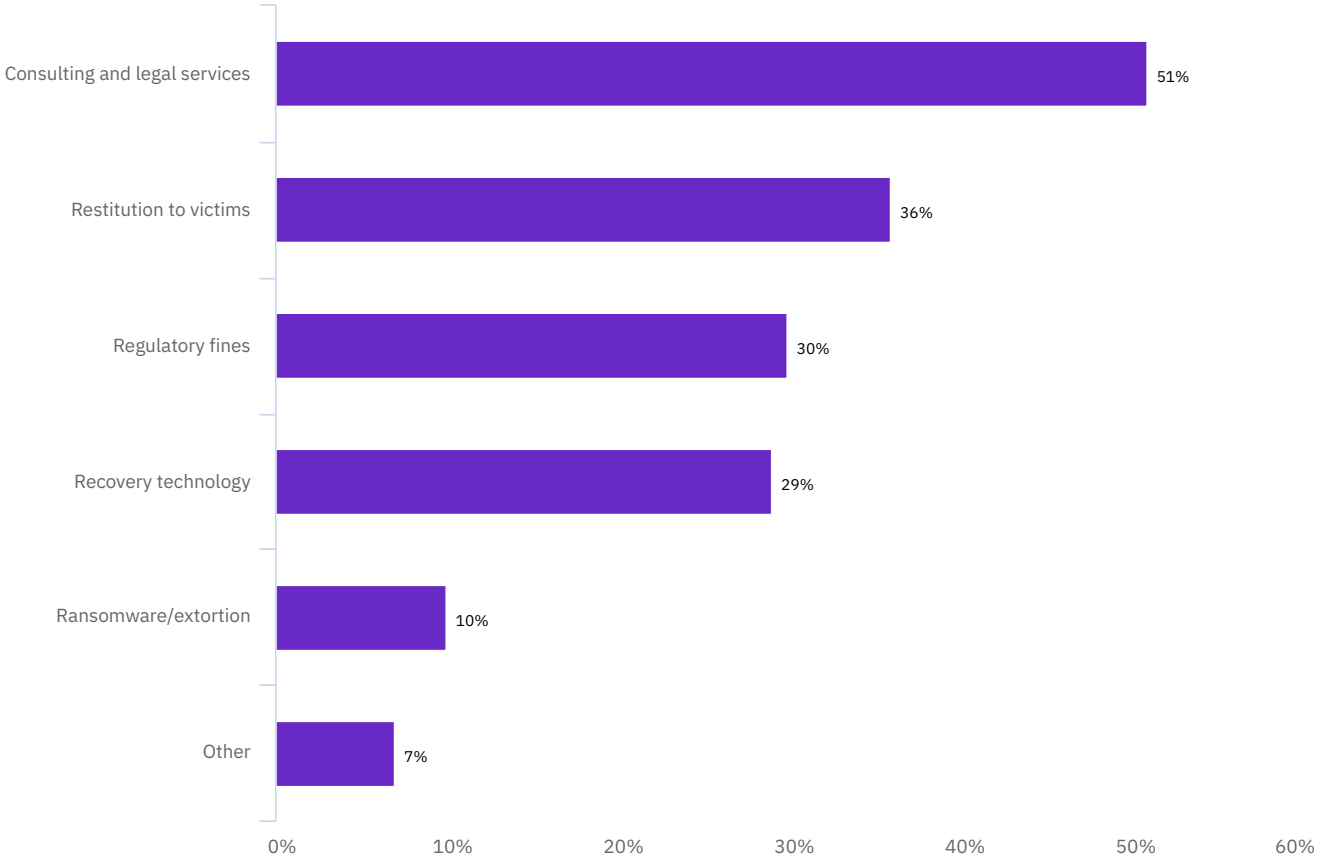
**Figure 26** shows the average cost impact of 25 factors on the average total cost of a data breach of $3.86 million. Security system complexity, created by the number of enabling technologies and the lack of in-house expertise, amplified the average total cost of a data breach by an average of $291,870. Migration to the cloud was associated with higher than average data breach costs, increasing the average cost by an average of $267,469.

Factors that mitigated the average total cost of a data breach included extensive testing of the incident response plan and business continuity management, decreasing the average cost by an average of $295,267 and $278,697, respectively.

**Figure 27**

## Types of costs recovered using cybersecurity insurance claims

Percentage of responses, more than one response allowed



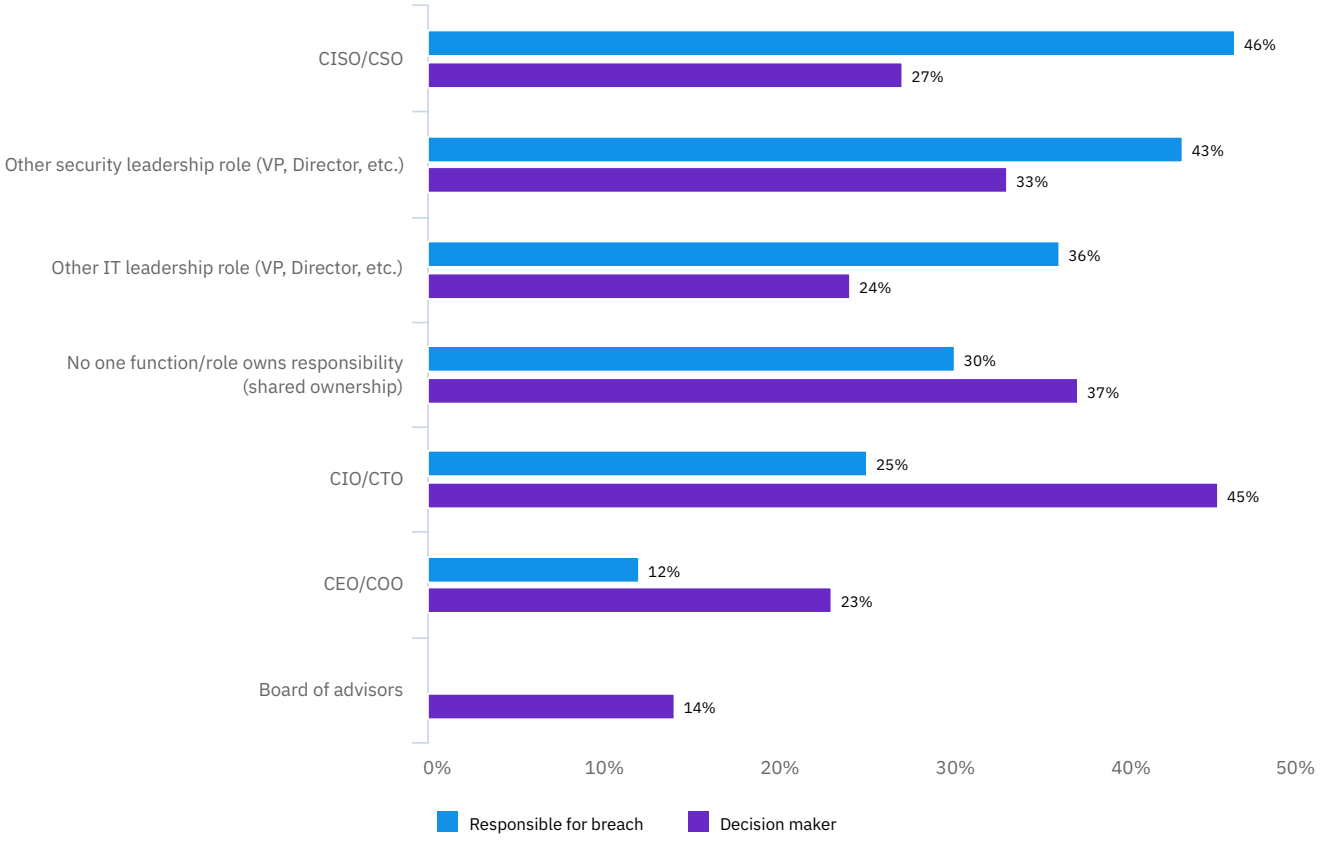

### Cyber insurance most often covered the cost of third-party services and victim restitution.

According to **figure 27**, 51% of organizations with cyber insurance used claims to cover the cost of third-party consulting and legal services. The cost of restitution to victims was covered by cyber insurance for 36% of organizations. Only 10% of organizations with cyber insurance used claims to cover the cost of ransomware or extortion.

**Figure 28**

## Who is most responsible for the breach and cybersecurity policy and technology decisions?

Percentage of responses, more than one response allowed



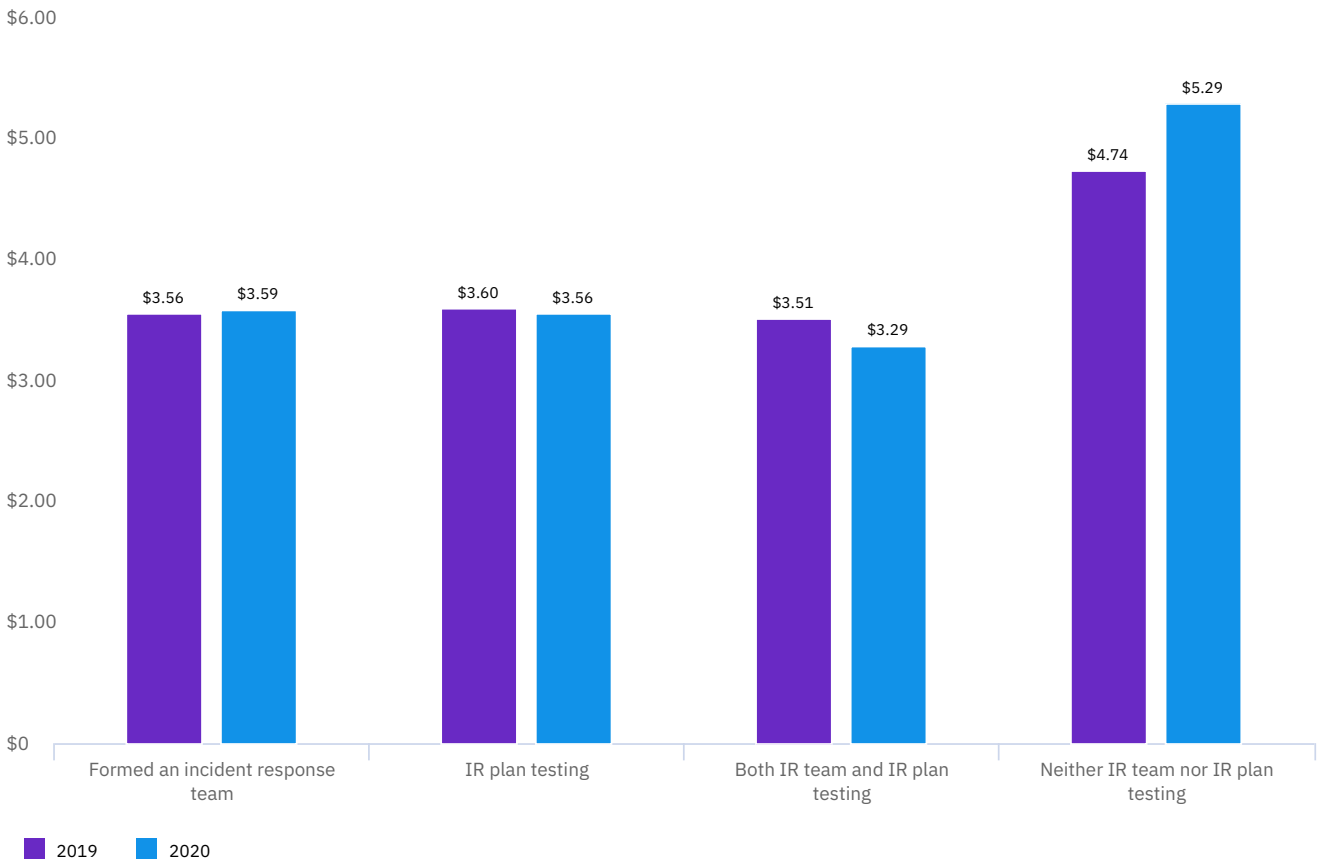

### CISOs were most likely to be held ultimately responsible for the data breach.

As shown in **figure 28**, 46% of respondents said the CISO/CSO would be held responsible for a data breach, but only 27% said the CISO/CSO was most responsible for cybersecurity policy and technology decision-making. CEOs and COOs were least likely to be held responsible for a data breach, while the CIO/CTO role was most often considered the ultimate decision maker of cybersecurity policy and technology.

**Figure 29**

## Average total cost of a data breach with incident response team and IR plan testing

Measured in US$ millions




### Incident response teams combined with incident response plan testing greatly reduced the cost of a data breach.

As shown in **figure 29,** organizations that both formed an incident response team and extensively tested their incident response plan had an average cost of a data breach of $3.29 million. In contrast, organizations that took neither of these steps experienced an average total cost of $5.29 million, a $2 million difference.

# Security automation trends and effectiveness

This was the third year we examined the relationship between data breach cost and security automation. 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 automated orchestration.

## Key findings

**21%**

Share of organizations in 2020 with fully deployed security automation, up from 15% in 2018

**$3.58 million**

Difference in the average total cost of a data breach for organizations without security automation deployed vs. organizations with automation fully deployed

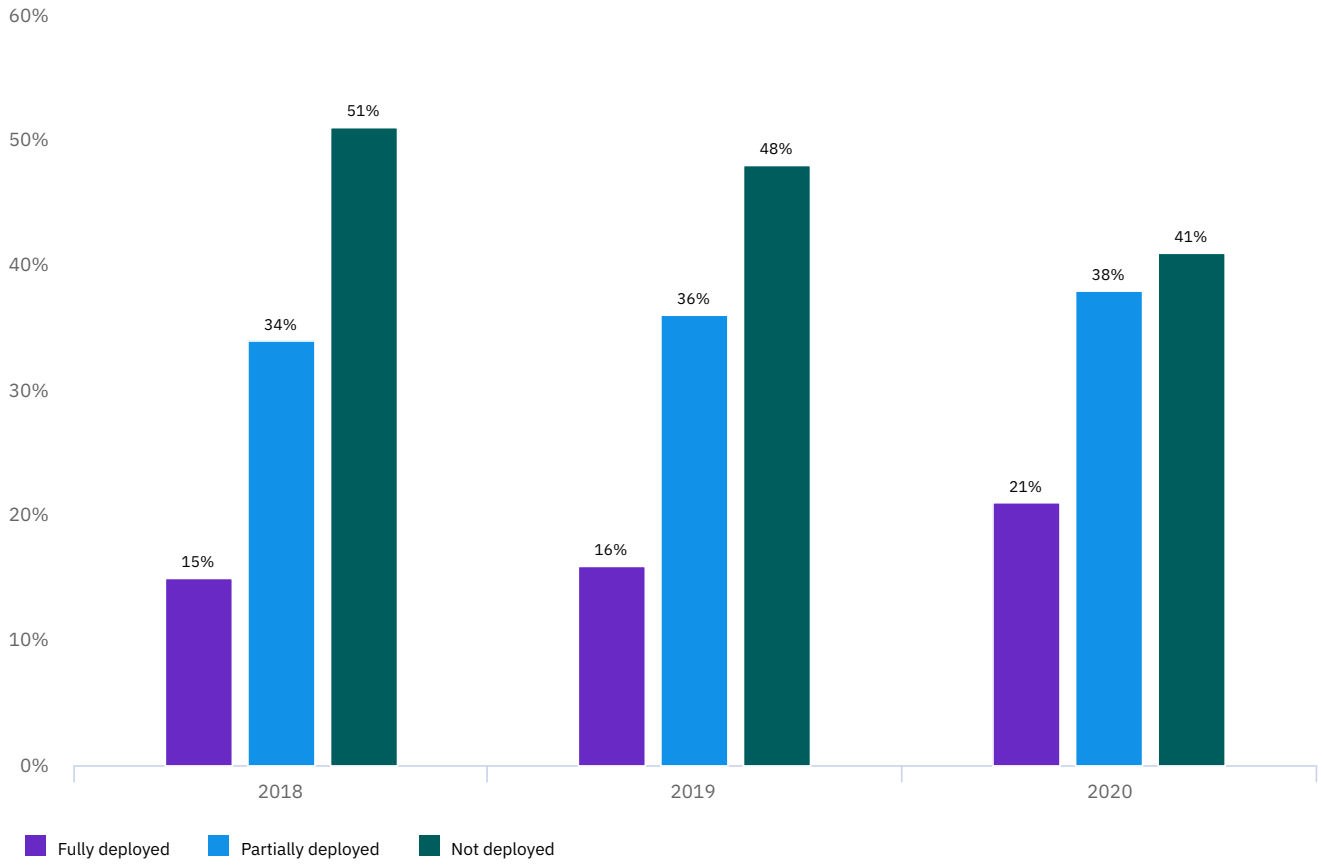
**30%**

Share of organizations in Germany with fully deployed security automation, highest of any nation

**Figure 30**

## State of security automation comparing three levels of deployment

Percentage of organizations per automation level



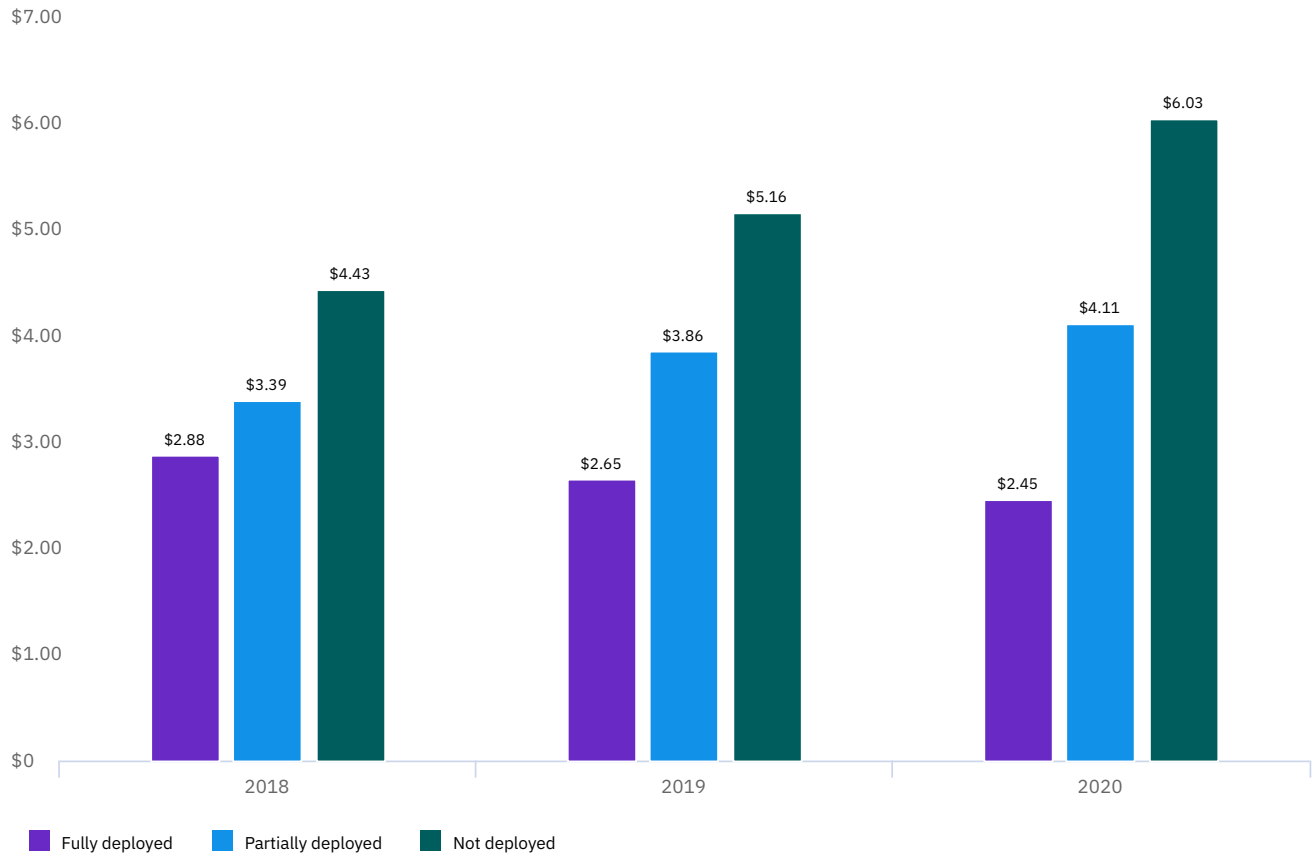

### Full deployment of automation increased over the last three years.

As shown in **figure 30**, only 21% of companies reported full deployment of security automation in the 2020 study, but that was an increase from 15% in 2018 and 16% in 2019. Another 38% reported partial deployment of automation and 41% reported automation was not deployed in the 2020 study.

**Figure 31**

# Average total cost of a data breach by security automation deployment level

Measured in US$ millions



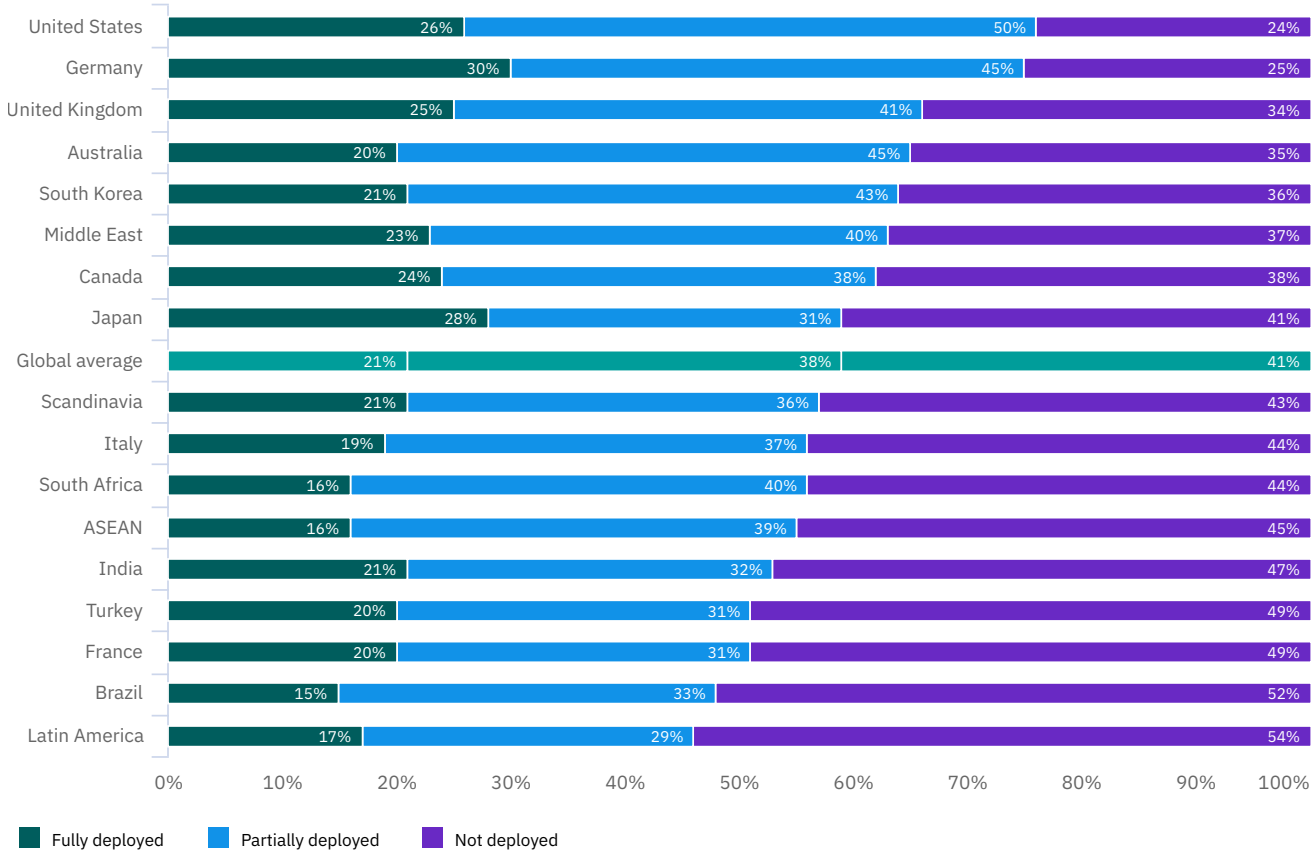

## Security automation's impact on data breach costs increased over the last three years.

As shown in **figure 31**, the average total cost of data breach was $2.45 million for organizations in the 2020 study that fully deployed security automation, which was $3.58 million less than the average cost for organizations without security automation deployed. In the 2018 study, the gap between the average cost of a breach at organizations with fully deployed automation and no automation deployed was $1.55 million, and in 2019, that gap was $2.51 million.

**Figure 32**

## Average security automation deployment by country

Percentage of organizations in three automation levels



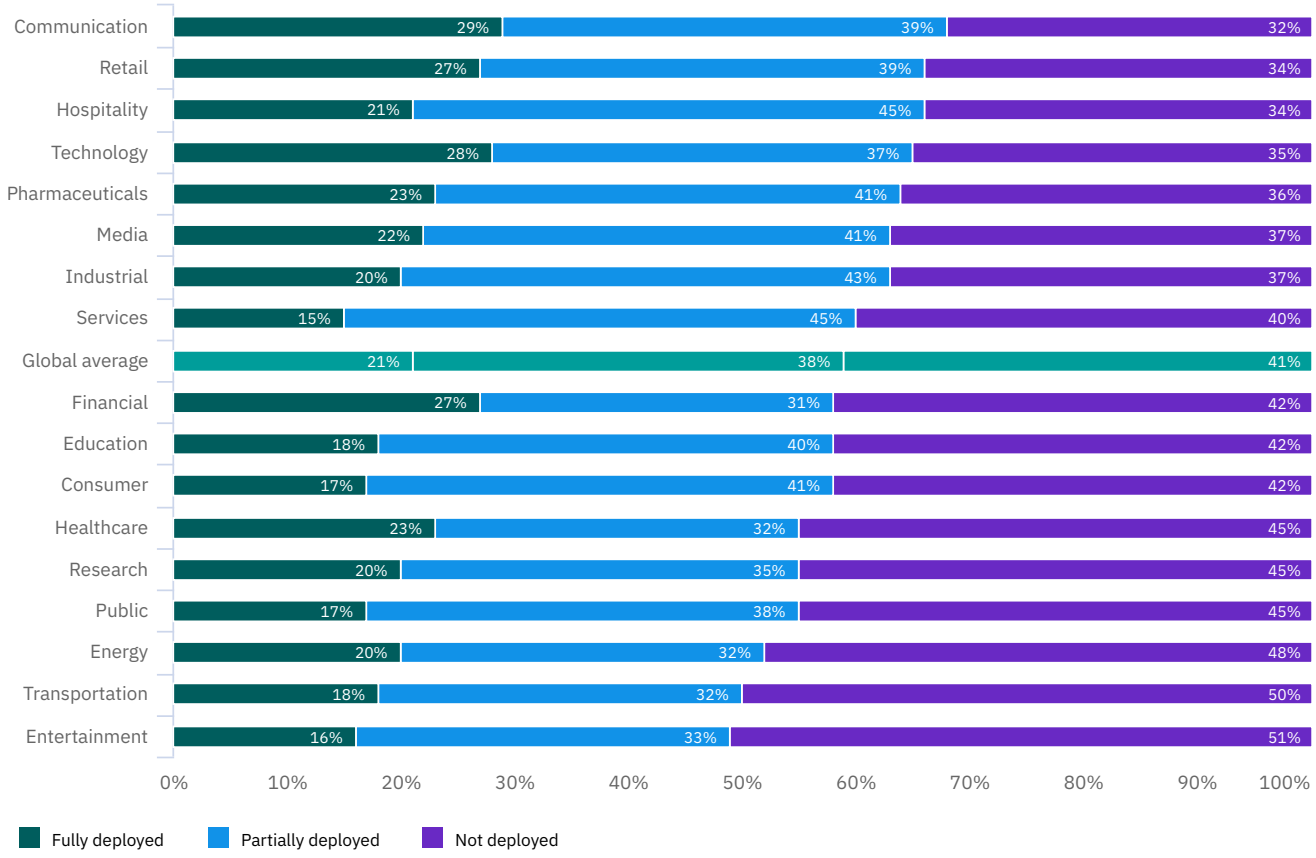

## The level of security automation varied among countries and regions.

According to **figure 32**, the United States and Germany had higher percentages of organizations with either fully deployed or partially deployed automation (76% in the United States and 75% in Germany). Fully deployed security automation was at 26% in the United States and 30% in Germany. Latin America and Brazil had the highest percentages of organizations without deployed automation (54% and 52% respectively).

**Figure 33**

# Average security automation deployment by industry

Percentage of organizations in three automation levels




## The level of security automation deployed varied by industry.

As seen in **figure 33**, communication, technology and retail industries had the highest percentages of organizations with either fully or partially deployed automation. Financial organizations had a higher than average share of organizations with security automation fully deployed (27%). But its relatively low share of organizations with partial deployment of automation (31%) meant the financial industry's combined share of fully and partially deployed automation was below the global average (58% vs the global average of 59%). Entertainment and transportation had the highest percentages of organizations that had not deployed automation.

# Time to identify and contain a data breach

In previous years, this research has shown that the faster the data breach can be identified and contained, the lower the costs. The average time to identify describes the time it takes to detect that an incident has occurred. The time to contain refers to the time it takes for an organization to resolve a situation once it has been detected and ultimately restore service.

The time elapsed between the first detection of the breach and its containment is referred to as the data breach lifecycle. These metrics can be used to determine the effectiveness of an organization's incident response and containment processes. For the first time, this year's study examined the impact of security automation on the direction of the data breach lifecycle.

## Key findings

**280 days**

Average time to detect and contain a data breach

**315 days**

Average time to detect and contain a data breach caused by a malicious attack

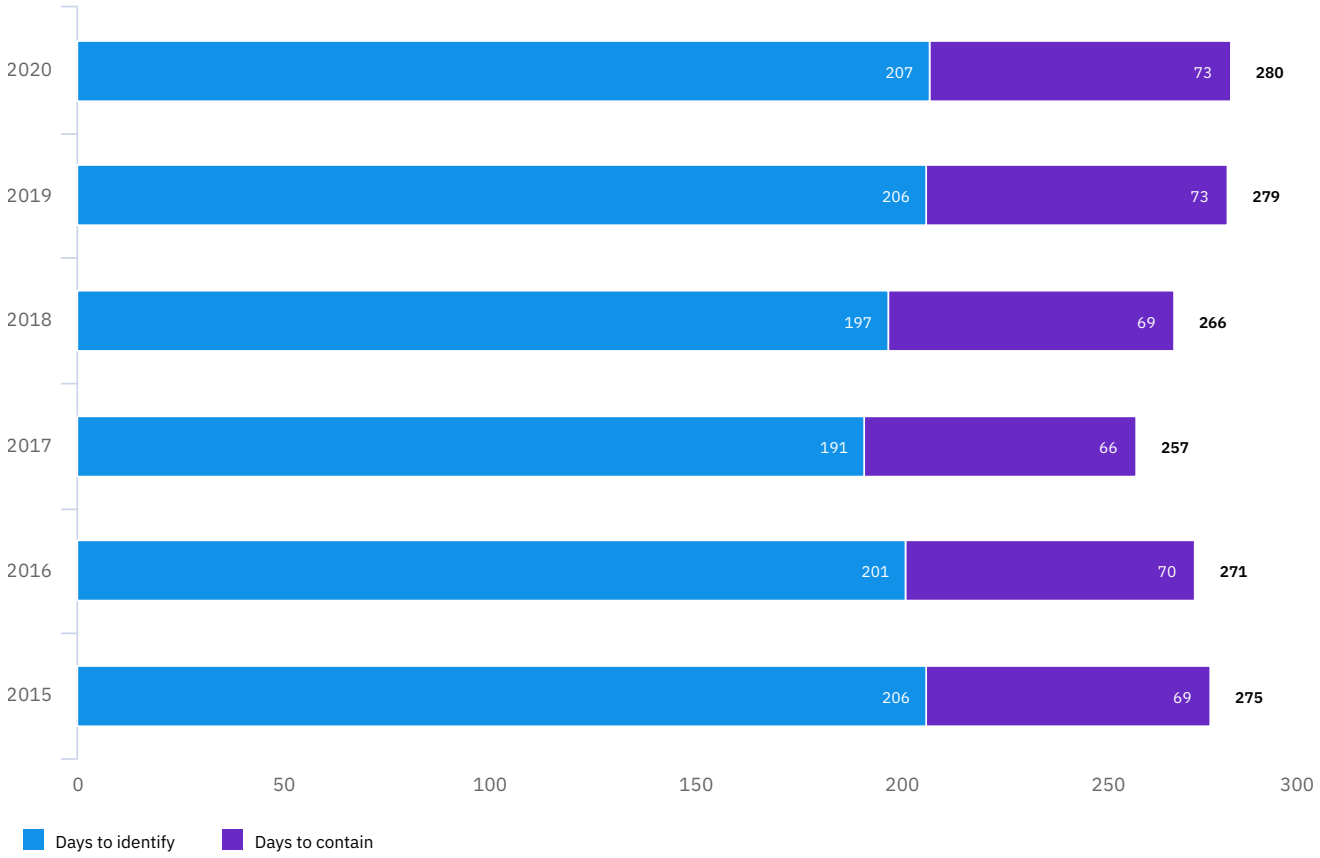
**$1.12 million**

Average cost savings of containing a breach in less than 200 days vs. more than 200 days

**Figure 34**

## Average time to identify and contain a data breach

Measured in days



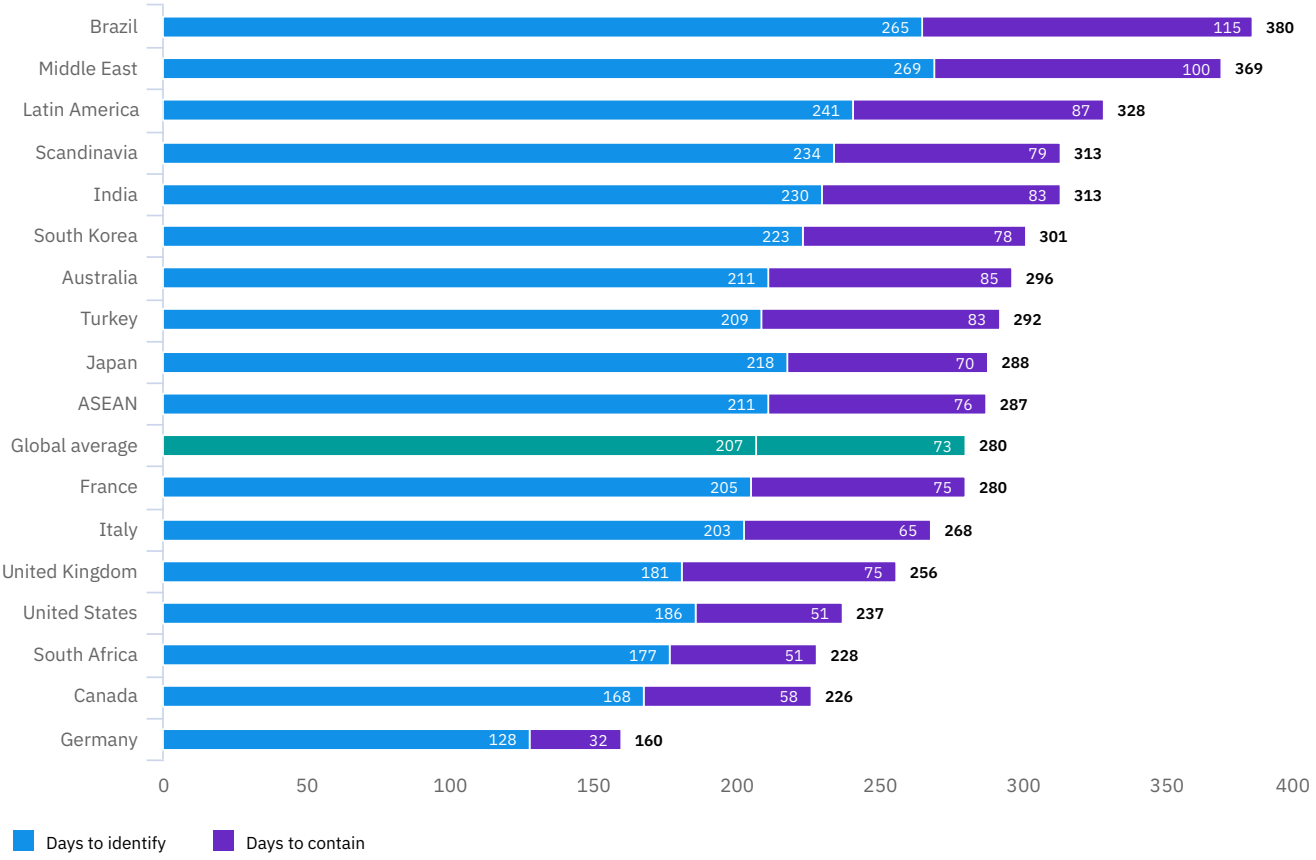

## The average time to identify and contain a breach has stayed consistent.

As shown in **figure 34**, the time to identify and time to contain a data breach have not varied much in the past few reports. In the 2020 study, the average time to identify was 207 days and the average time to contain was 73 days, for a combined 280 days. In 2019, the combined data breach lifecycle was 279 days.

**Figure 35**

## Average time to identify and contain a data breach by country or region

Measured in days



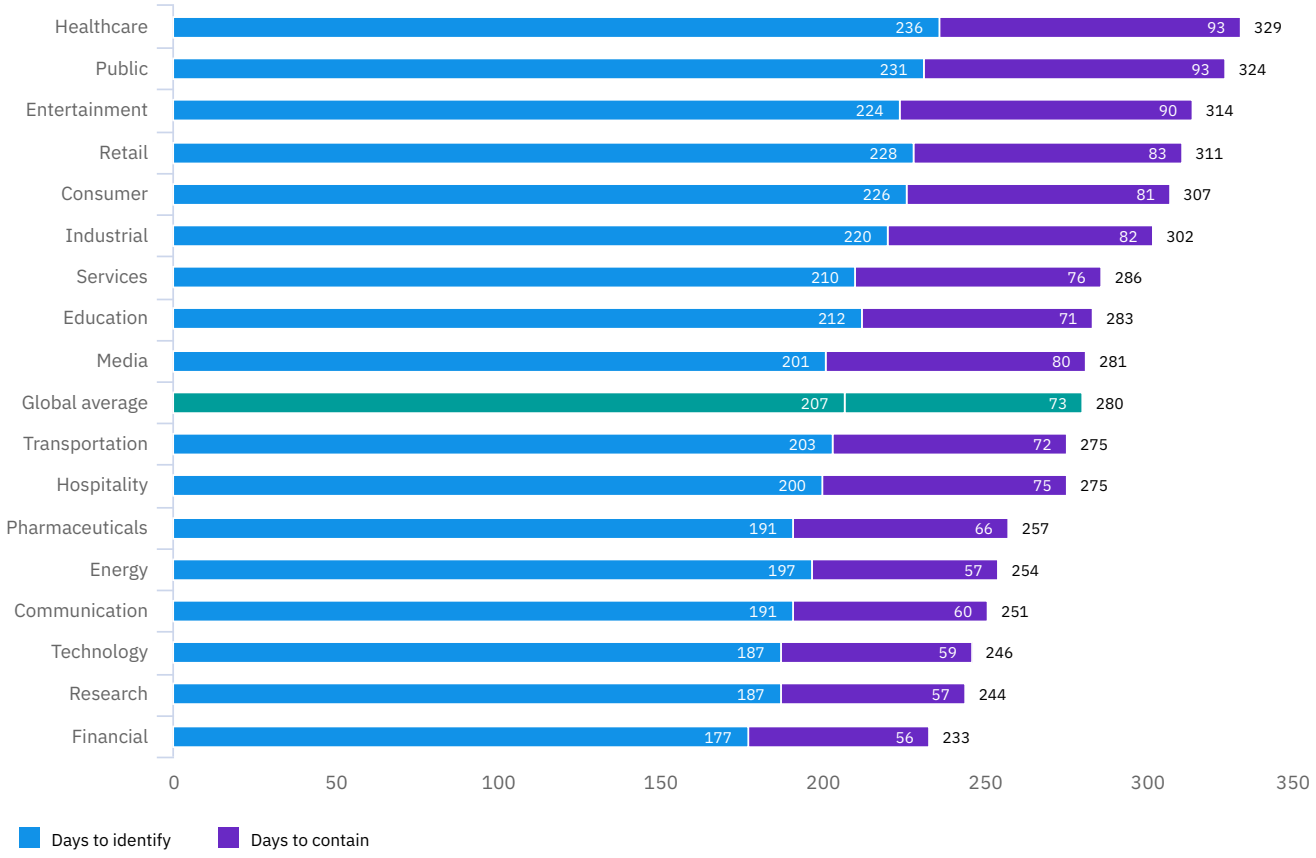

### The gaps between countries/regions in average breach lifecycle were significant.

According to **figure 35**, Brazil and the Middle East took far longer than average to identify and contain a data breach, averaging 380 days and 369 days, respectively. South Africa, Canada and Germany had much shorter data breach lifecycles, with organizations in Germany taking an average of just 160 days to contain the breach.

**Figure 36**

## Average time to identify and contain a data breach by industry

Measured in days



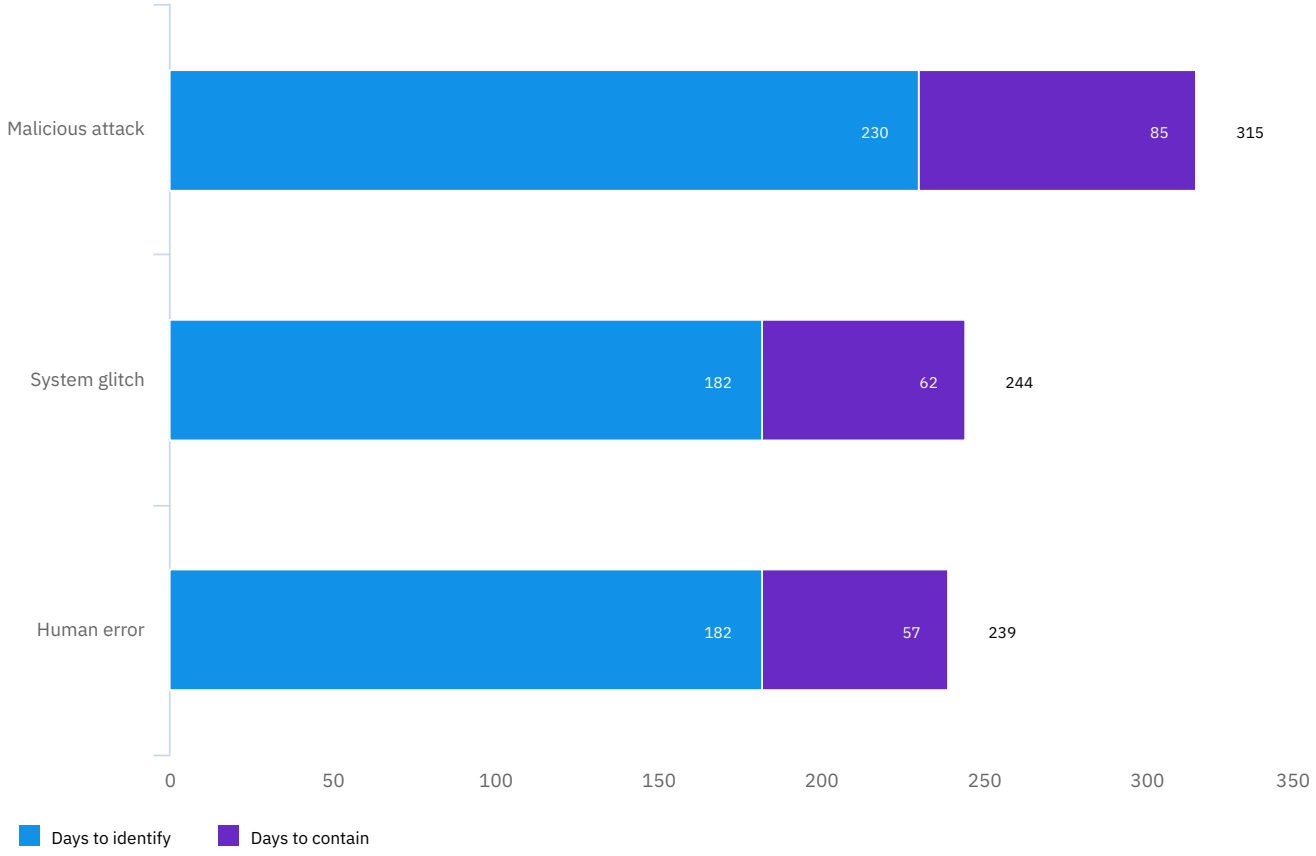

### Financial and healthcare industries were far apart in time to identify and contain a breach.

As shown in **figure 36**, healthcare had the highest average time to identify and contain a breach, at 329 days. The financial industry had the lowest average time to identify and contain a breach, at 233 days. Nine industries were above the average, and eight were below the global average breach lifecycle of 280 days.

**Figure 37**

## Average time to identify and contain a data breach by root cause

Measured in days



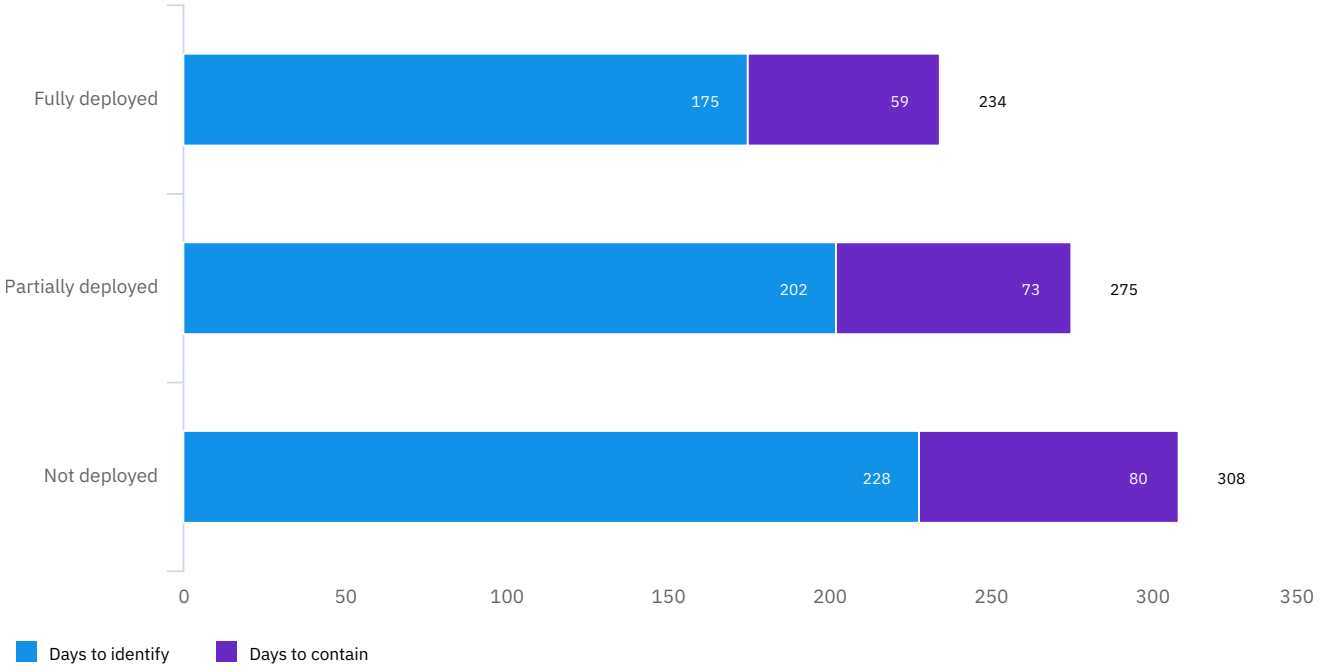

### Breaches caused by malicious attacks took the longest to identify and contain.

Malicious breaches in the 2020 study took an average of 315 days to identify and contain, compared to breaches with other root causes, as shown in **figure 37**. It took an average of 244 days to identify and contain a system glitch breach and 239 days to identify and contain a breach caused by human error. Malicious breaches took 23 days longer to identify than an average data breach. An average of 230 days was necessary to identify a malicious breach, compared to the overall average of 207 days.

**Figure 38**

## Average time to identify and contain a data breach by level of security automation

Measured in days



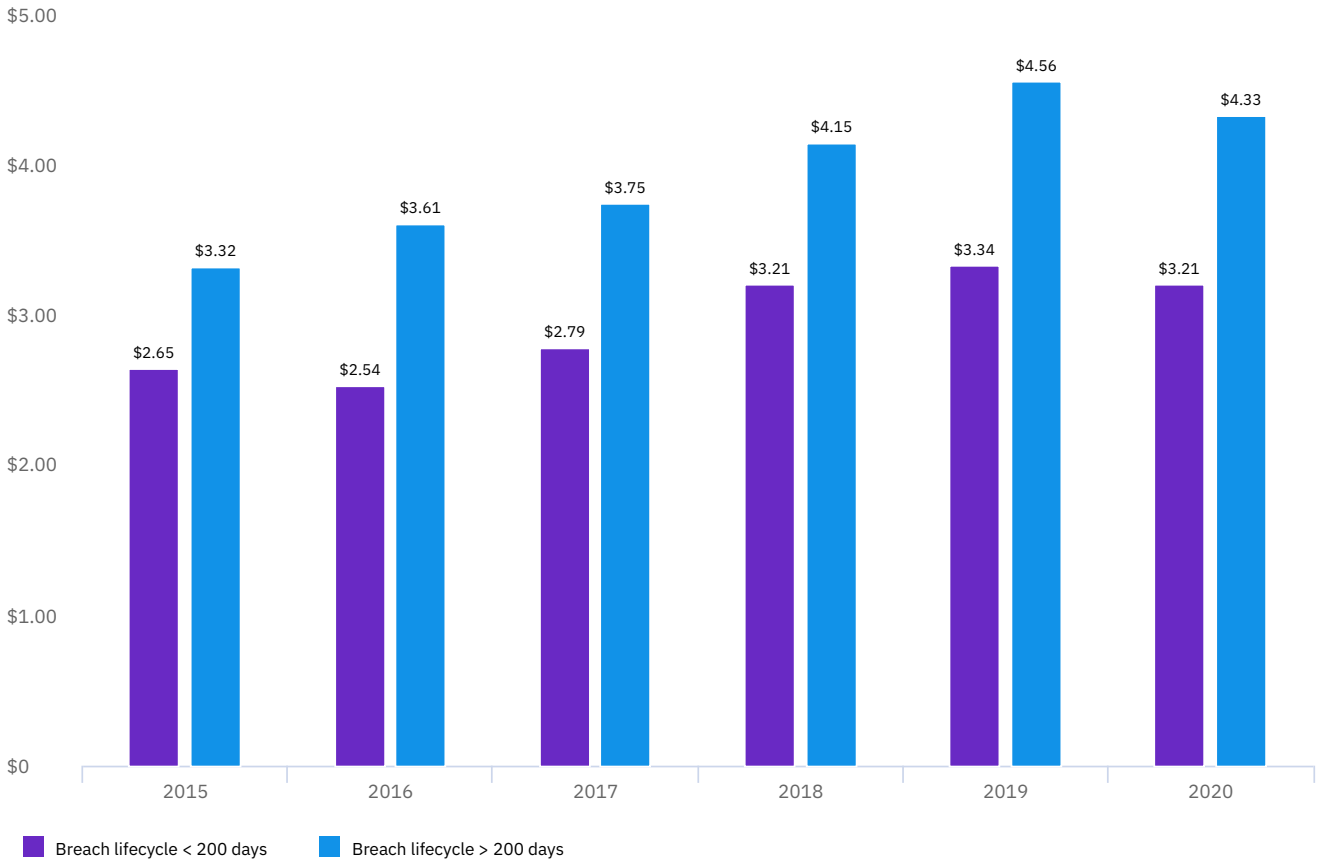

### Security automation reduced the time needed to identify and contain a data breach.

For the first time, this study examined the impact of automation on the data breach lifecycle. **Figure 38** shows that when automation was fully deployed, the time to identify averaged 175 days and the time to contain averaged 59 days. Without automation, the time significantly increased to an average of 228 days to identify a breach and 80 days to contain, for a total of 308 days.

**Figure 39**

## Average total cost of a data breach based on average data breach lifecycle

Measured in US$ millions




### Data breach lifecycle influenced the average cost of a breach.

Over the past six years, the research has been consistent in showing that breaches with a lifecycle (time to identify plus time to contain a breach) of more than 200 days had a much higher cost than breaches with a lifecycle of less than 200 days. As shown in **figure 39**, breaches in the 2020 study with a lifecycle longer than 200 days cost an average of $1.12 million more than breaches with a lifecycle of less than 200 days ($4.33 million for 200-plus days versus $3.21 million for less than 200 days).

# Longtail costs of a data breach

The cost consequences of a data breach can continue for years following the event. In last year's study, we first examined how organizations might be impacted by data breach costs over a span of two or more years. The analysis showed that costs were greatest in the first year after a breach, but tended to pick up again after two years.

We then looked at the difference in these "longtail costs" in breaches at organizations in highly regulated industries versus those in industries with less stringent data protection regulations. We defined highly regulated industries to include energy, health, consumer, financial, technology, pharma, communication, public sector and education. Organizations in retail, industrial, entertainment, media, research services, and hospitality were considered to be in a low regulatory environment. In the analysis of industries in the high versus low regulation categories, we concluded that regulatory and legal costs may have contributed to higher costs in the years following a breach.

In the 2020 study, we examined a sample of 101 companies that captured two or more years of data breach costs.

## Key findings

61%

Average share of data breach costs incurred in the first year

44%

Average share of data breach costs incurred in the first year in highly regulated industries

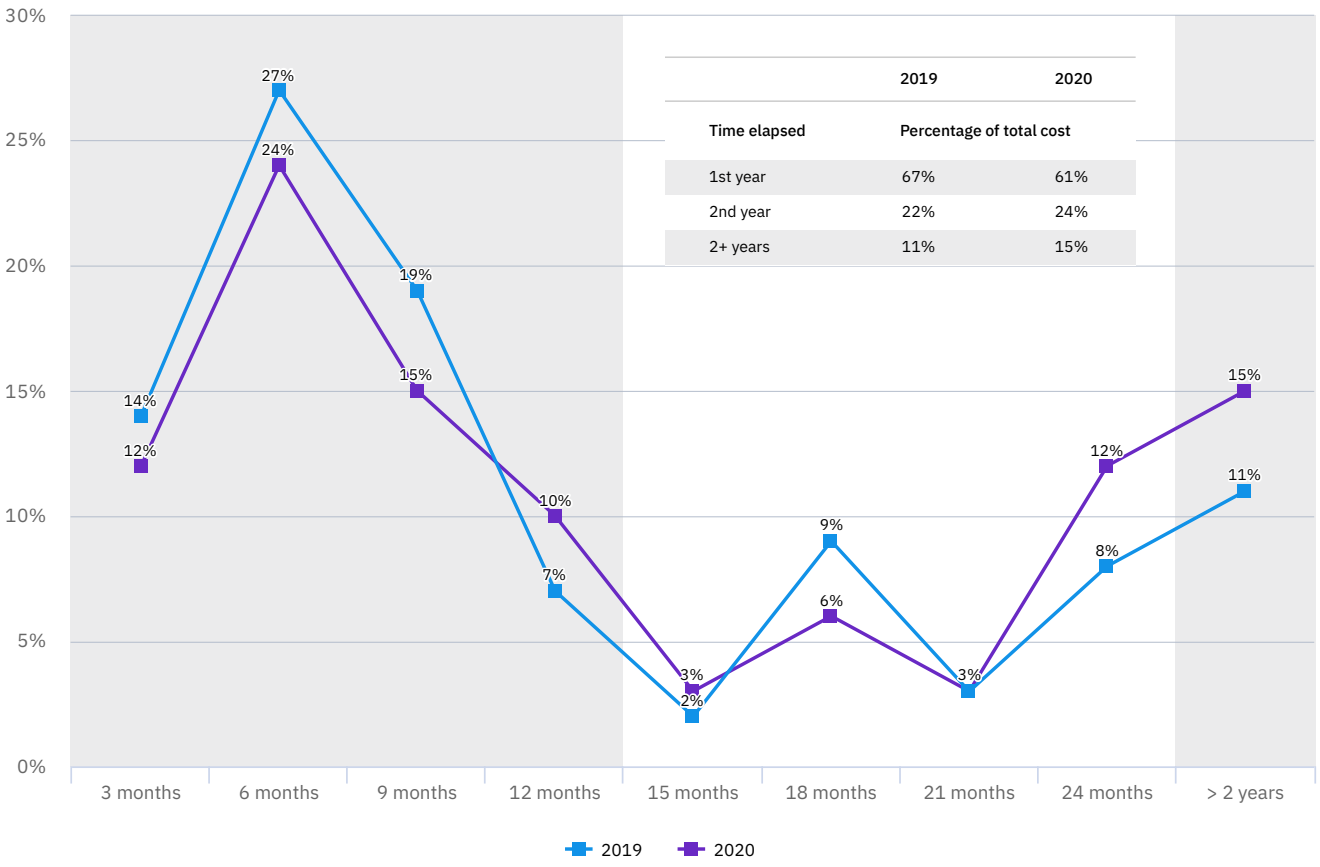
92%

Average share of data breach costs incurred in the first two years in less regulated industries

**Figure 40**

# Average distribution of data breach costs over two-plus years

Percentage of costs accrued at three-month intervals




| | 2019 | 2020 |
|---|---|---|
| Time elapsed | Percentage of total cost | |
| 1st year | 67% | 61% |
| 2nd year | 22% | 24% |
| 2+ years | 11% | 15% |

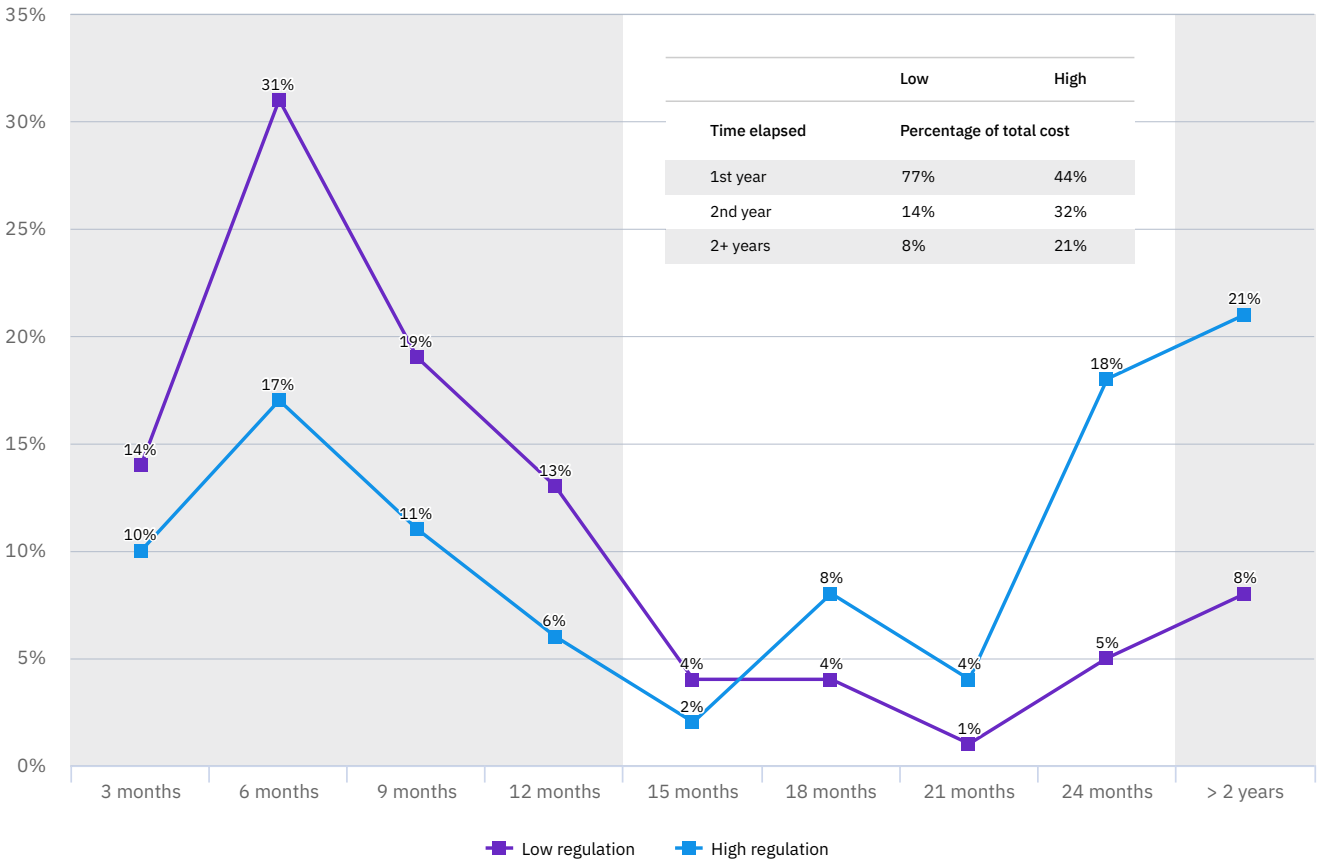
## The share of breach costs incurred after two years increased in the 2020 study.

According to **figure 40**, the longtail cost analysis found an average of 61% of the cost of the data breach was incurred during the first year, 24% during the second year and 15% after two years. That was a slight increase in costs more than two years after the breach, compared to 11% in the 2019 analysis.

**Figure 41**

# Average distribution of data breach costs over time in low vs. high regulatory environments

Percentage of total costs accrued at three month intervals




| | Low | High |
|---|---|---|
| Time elapsed | Percentage of total cost | |
| 1st year | 77% | 44% |
| 2nd year | 14% | 32% |
| 2+ years | 8% | 21% |

## Breaches in highly regulated industries experienced a majority of the costs after the first year.

According to **figure 41**, organizations in low regulatory environments were far more likely to realize the full cost of the data breach during the first year. In less regulated industries, an average of 77% of costs were incurred during the first year, compared to an average of 44% of costs during the first year for breaches in highly regulated organizations.

**Figure 42**

# Average distribution of data breach costs over time in low vs. high regulatory environments in the 2019 report year

Percentage of total costs accrued at three month intervals


| Time elapsed | Low | High |
|---|---|---|
| | Percentage of total cost | |
| 1st year | 81% | 53% |
| 2nd year | 14% | 31% |
| 2+ years | 5% | 16% |

## The 2019 analysis of high and low regulatory environments showed a lower proportion of costs occurred more than two years after a breach.

**Figure 42** shows the longtail breach costs of low versus high data protection regulatory environments from the 2019 study. In the 2019 study, an average of 16% of costs in highly regulated industries were incurred after two years. That compares to 21% of costs incurred after two years in highly regulated industries in the 2020 study (see figure 41).

# Potential impacts of COVID-19

The COVID-19 pandemic has had a tremendous impact on the way many organizations do business, with large numbers of people working from home and increased demand for video conferencing, cloud applications and network resources. To understand this new reality, we added several questions to the research to gather the opinions of study participants on potential impacts of COVID-19 on the cost of a data breach.

## Key findings

**54%**

Share of organizations that required remote work in response to COVID-19

**76%**

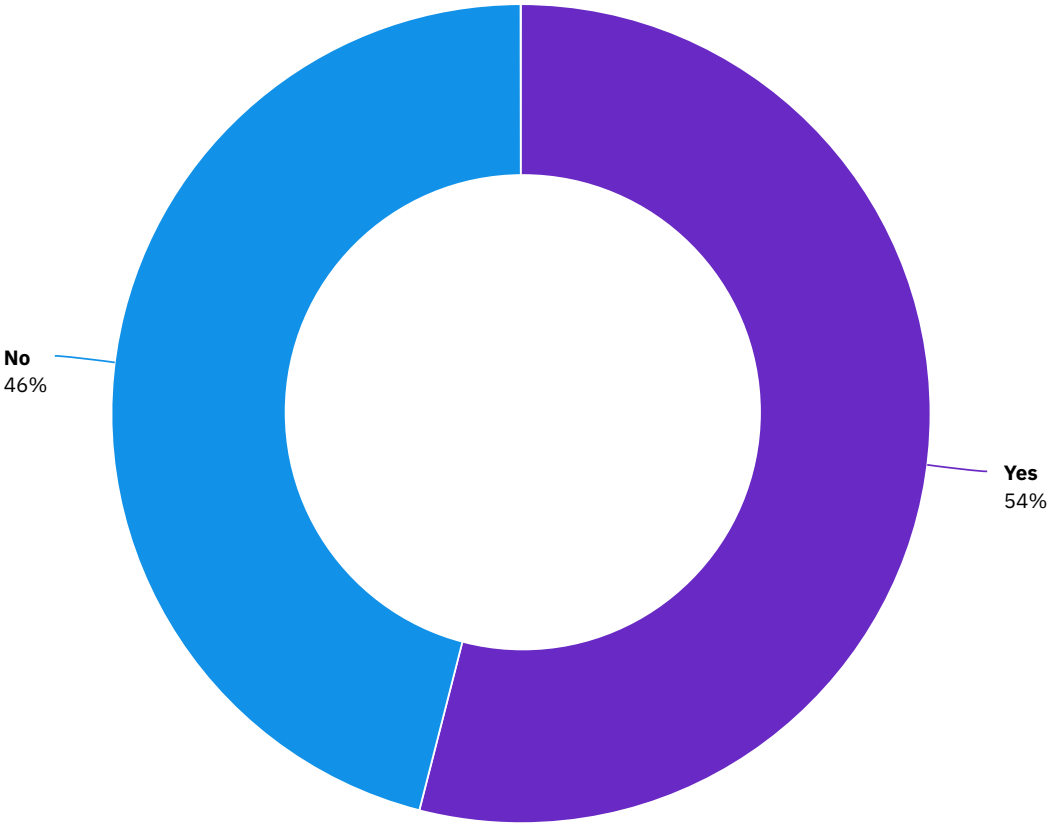
Share of participants who said remote work would increase the time to identify and contain a data breach

**70%**

Share of participants who said remote work would increase the cost of a data breach

**Figure 43**

## Did your organization require employees to work remotely in response to COVID-19?

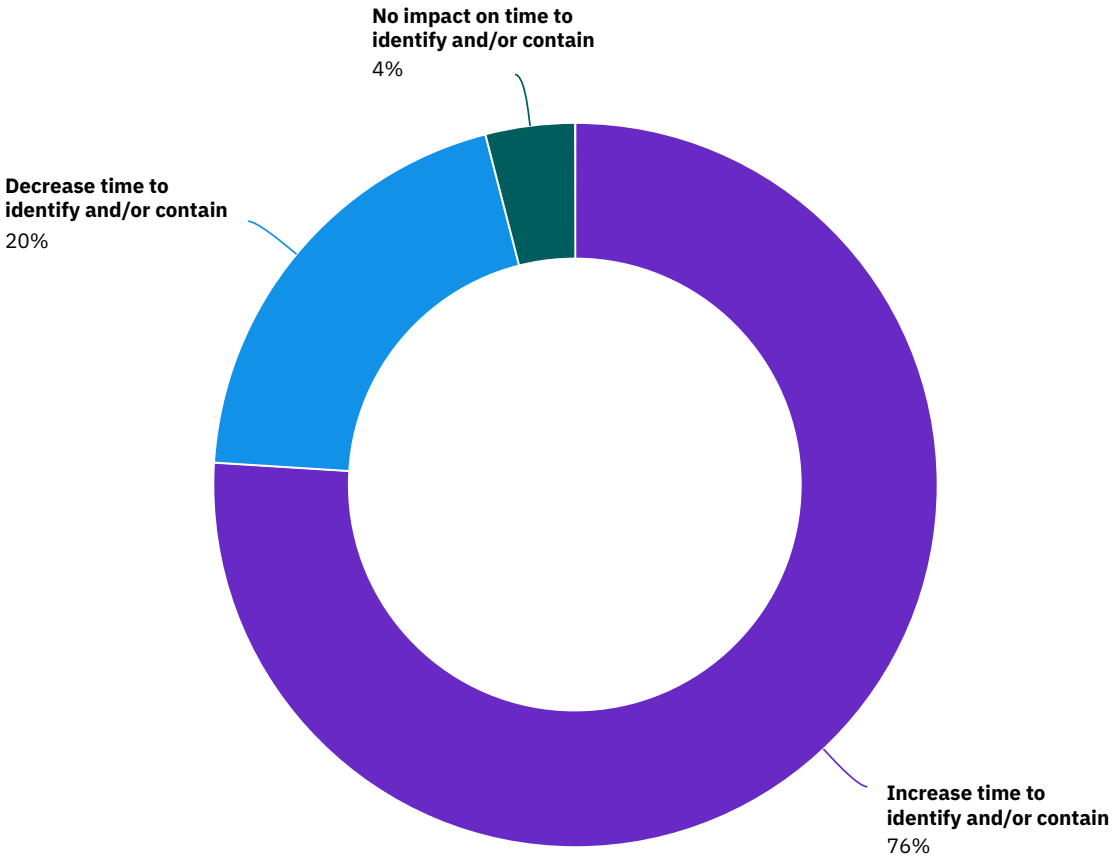



### A majority of organizations required remote work in response to COVID-19.

As shown in **figure 43**, a majority of organizations in the study (54%) required remote work in response to the COVID-19 pandemic.

**Figure 44**

## How would remote work impact your ability to respond to a data breach?

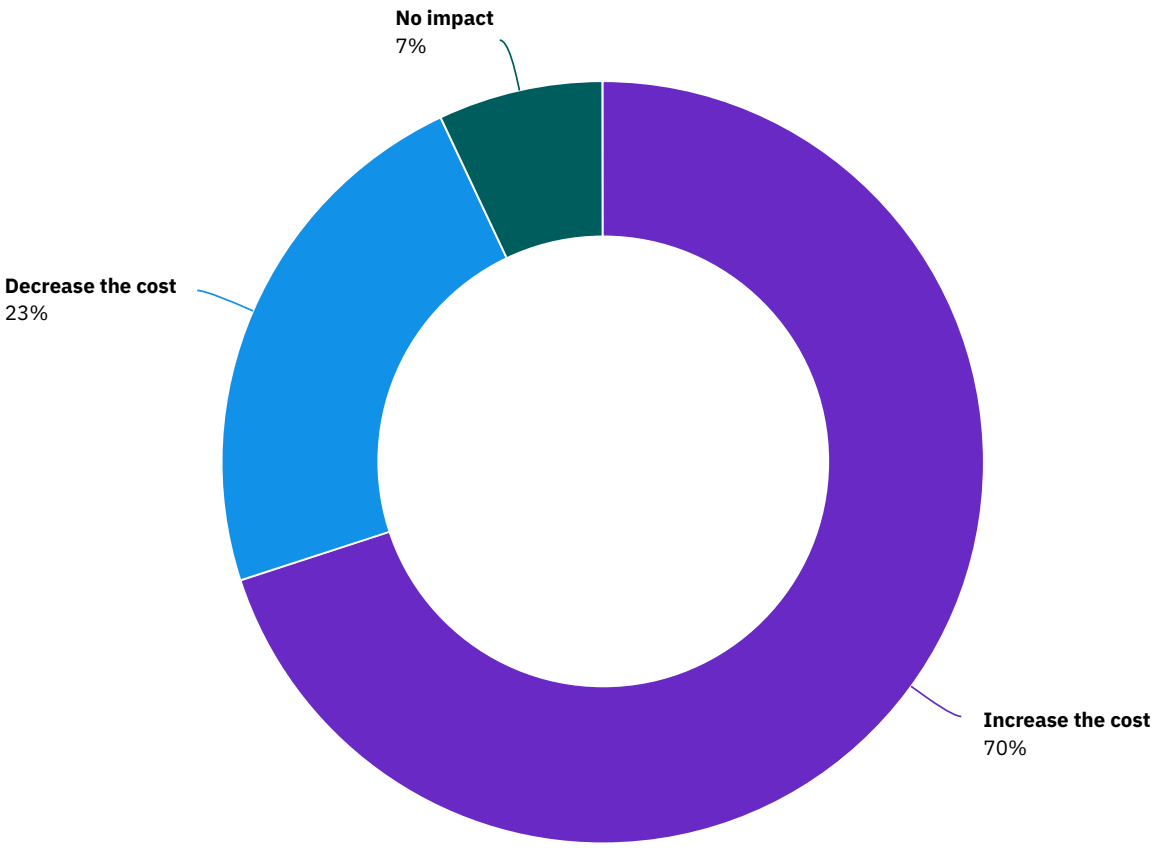



### Three-quarters of participants expected a data breach would take longer to identify and contain.

Of participants who said their organizations required remote work in response to COVID-19, more than three-quarters (76%) said it would increase the time to identify and contain a data breach, 20% said it would decrease the time to identify and contain a breach, and 4% said there would be no impact, according to **figure 44**.

**Figure 45**

## How would remote work impact the cost of a data breach?




### Remote work was expected to increase the cost of a potential data breach.

Of participants who said their organizations required remote work in response to COVID-19, 70% said it would increase the cost of a potential data breach, according to **figure 45**. Another 23% said remote work would decrease the cost of a data breach, and 7% said there would be no impact.

# Cost of a mega breach

This is the third year we have examined the cost of mega breaches, those with more than 1 million compromised records. They are not the normal experience for most businesses, but mega breaches have an outsized impact on consumers and industries. The average cost of a mega breach has continued to grow since we introduced this analysis in the 2018 study.

This year's investigation is based on the analysis of 17 companies that experienced a data breach involving the loss or theft of 1 million or more records. For a full explanation of our methodology, see the cost of a data breach FAQ at the end of this report.

## Key findings

**$392 million**

Average cost of a breach of more than 50 million records

**100x**

Difference between average costs of a breach over 50 million records and an average data breach

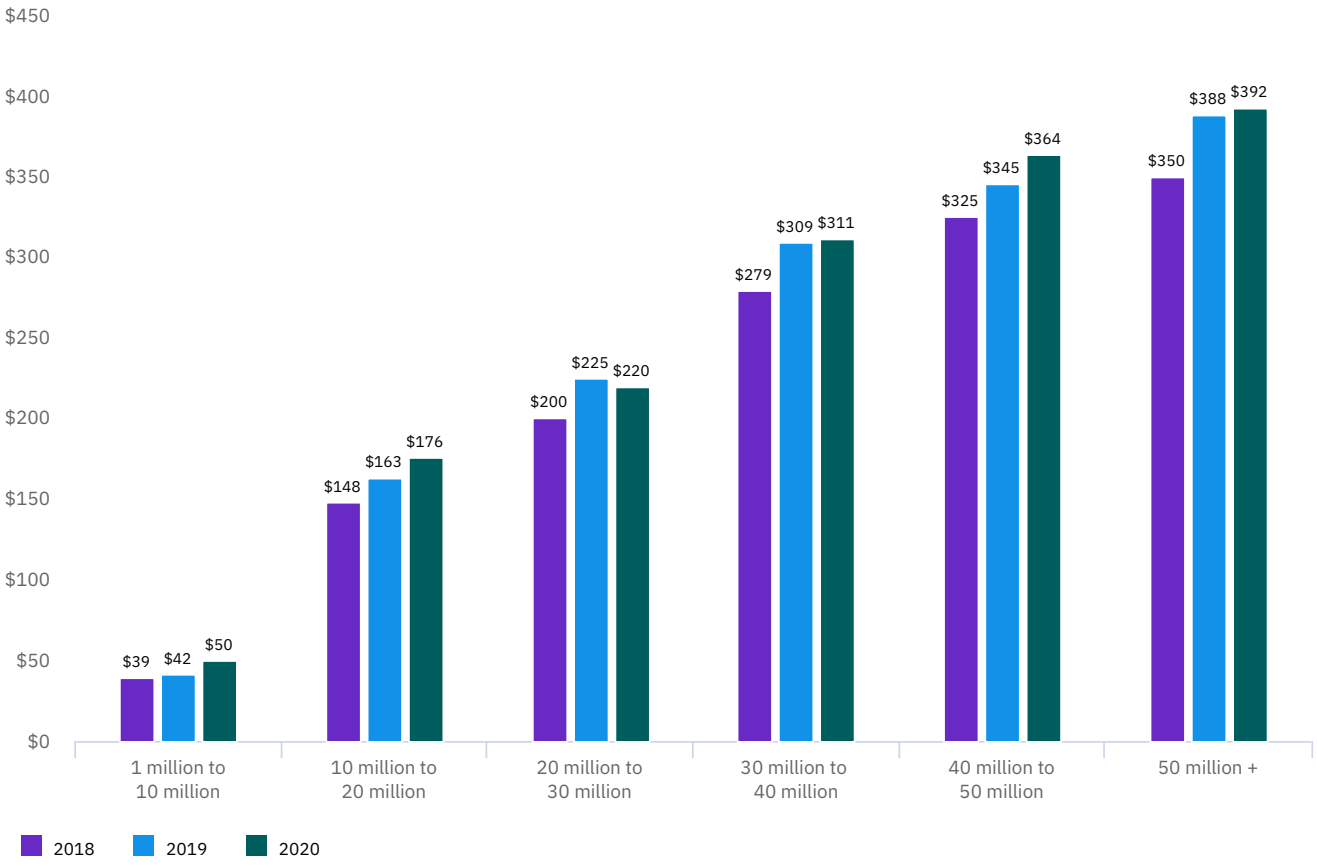
**$19 million**

Increase in average cost of a breach of 40 to 50 million records between 2019 and 2020 study

**Figure 46**

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

Measured in US$ millions




### The cost of a mega breach soared to new heights.

As shown in **figure 46**, breaches of 1 million to 10 million records cost an average of $50 million, more than 25 times the average cost of $3.86 million, for breaches of less than 100,000 records. The 1 million to 10 million records size of breach experienced the greatest growth rate, increasing by 22% from an average $39 million in 2018 to $50 million in 2020.

In breaches of more than 50 million records, the average cost was $392 million, more than 100 times the average cost of a data breach. The largest absolute cost increase was in breaches of greater than 50 million records, which increased from an average of $350 million in 2018 to $392 million in 2020.

# Steps to help minimize financial and brand impacts of a data breach

*In this section, IBM Security outlines steps organizations in the study have taken to help reduce the financial cost and reputational consequences of a data breach.**

## Invest in security orchestration, automation and response (SOAR) to help improve detection and response times.

In the cost of a data breach study, security automation was found to significantly reduce the average time to identify and respond to a breach as well as the average cost. SOAR software and services can help your organization accelerate incident response with automation, process standardization and integration with your existing security tools. Automation technologies including artificial intelligence, analytics and automated orchestration were all associated with lower than average data breach costs.

## Adopt a zero trust security model to help prevent unauthorized access to sensitive data.

Results from the study showed that lost and stolen credentials, along with cloud misconfigurations were the most common root causes of a data breach. As organizations have shifted to incorporate remote work and more disconnected, hybrid multicloud environments, a zero trust strategy can help protect data and resources by making them accessible only on a limited basis and in the right context.

## Stress test your incident response plan to increase cyber resilience.

Organizations in the study who have formed incident response (IR) teams and tested their incident response plans reduced the average total cost of a data breach by $2 million, compared to organizations without IR teams that had not tested any IR plans. The mantra “train like you fight and fight like you train” means developing and testing incident response playbooks to help optimize your business’ ability to respond quickly and effectively to attacks.

*Recommendations for security practices are for educational purposes and do not guarantee results.

## Use tools that help protect and monitor endpoints and remote employees.

In the study, 70% of organizations that required remote work in response to the COVID-19 pandemic believed it would increase the cost of a data breach. Unified endpoint management (UEM) and identity and access management (IAM) products and services can help provide security teams with deeper visibility into suspicious activity on company and bring your own (BYO) laptops, desktops, tablets, mobile devices and IoT, including endpoints the organization doesn't have physical access to, speeding investigation and response time to isolate and contain the damage.

## Invest in governance, risk management and compliance programs.

Behind only the cost of lost business, detection and escalation costs were the second-largest category of breach costs in the study. An internal framework for audits, evaluating risk across the enterprise and tracking compliance with governance requirements can help improve an organization's ability to detect a data breach and escalate containment efforts.

## Minimize the complexity of IT and security environments.

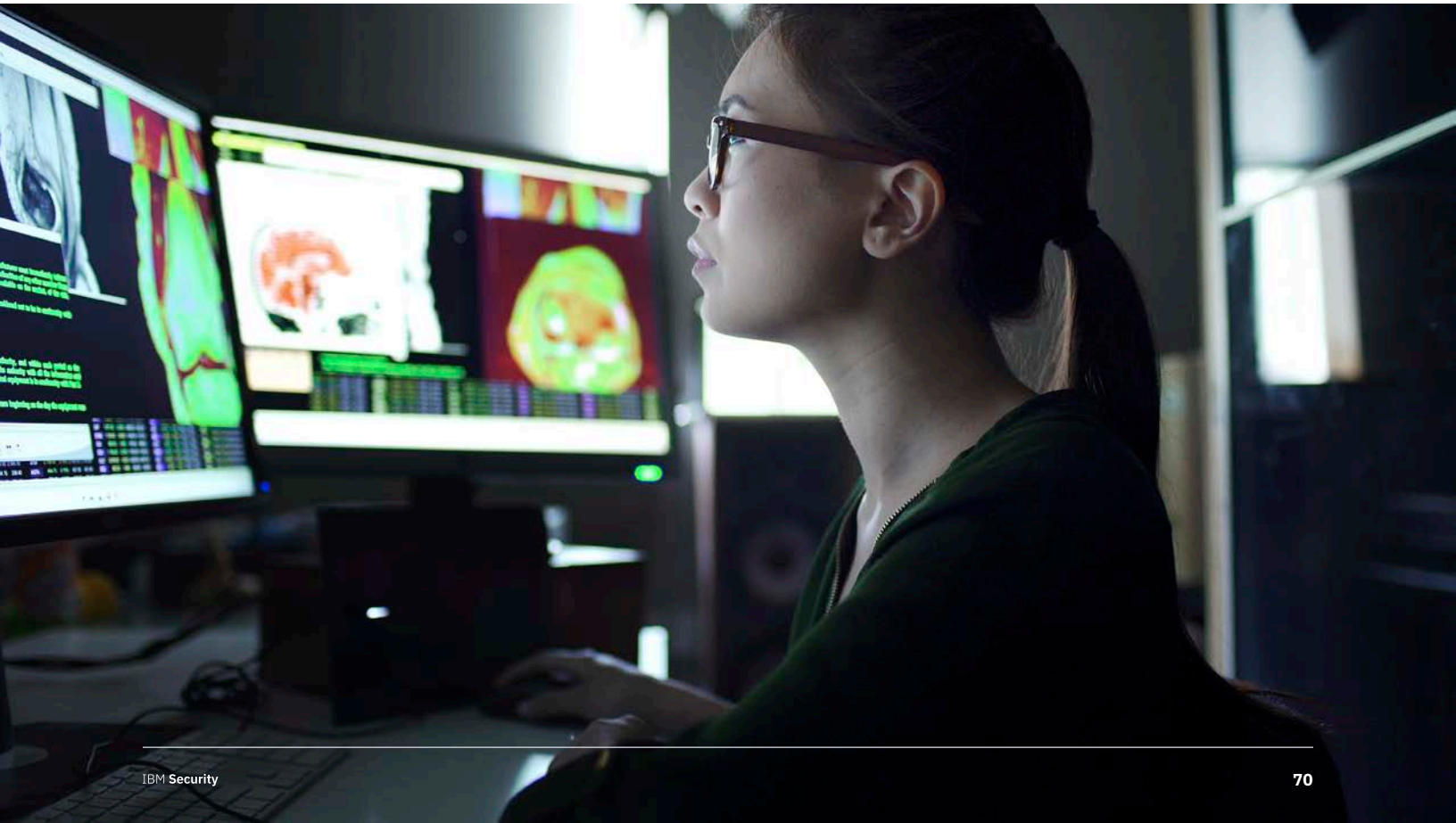
In this year's study, the complexity of security systems was the number one factor contributing to higher average data breach costs, from a list of 25 cost factors. Data breaches caused by a third party, extensive cloud migration and IoT/OT environments were also associated with higher data breach costs. Security tools with the ability to share data between disparate systems can help security teams detect incidents across complex hybrid multicloud environments.

## Protect sensitive data in cloud environments using policy and technology.

With the increasing amount and value of data being hosted in cloud environments, organizations should take steps to protect cloud-hosted databases. Use data classification schema and retention programs to help bring visibility into and reduce the volume of the sensitive information that is vulnerable to a breach, and protect it using encryption. Use vulnerability scanning, penetration testing and red teaming to help identify cloud-hosted database vulnerability exposures and misconfigurations. All of these solutions were associated in the study with lower average data breach costs.

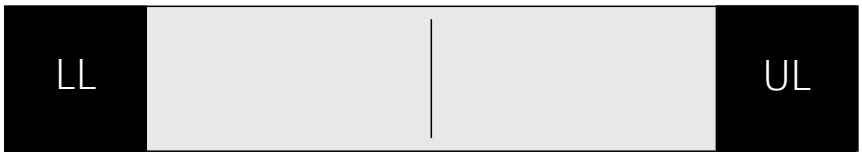
## Use managed security services to help close the security skills gap.

Organizations in the study identified security skills shortages as one of the leading factors contributing to increased data breach costs, while managed security services were associated with lower average data breach costs. A managed security services provider can help simplify security and risk with continuous monitoring and integrated solutions and services.



# Research methodology

To preserve confidentiality, the benchmark instrument did not capture any company-specific information. Data collection methods did not include actual accounting information but instead relied upon participants estimating direct costs by marking a range variable on a number line. Participants were instructed to mark the number line in one spot between the lower and upper limits of a range for each 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 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.

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.

# Cost of a data breach FAQ

**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. Breaches included in the study ranged from 3,400 to 99,730 compromised records.

**What is a compromised record?**
A record is information that identifies the natural person (individual) whose information has been lost or stolen in a data breach. Examples include a database with an individual's name, credit card information and other personally identifiable information (PII) or a health record with the policyholder's name and payment information.

**How do you collect the data?**
Our researchers collected in-depth qualitative data through more than 3,200 separate interviews with individuals at 524 organizations that suffered a data breach between August 2019 and April 2020. Recruiting organizations began in October 2019, and interviews were completed April 21, 2020. Interviewees included IT, compliance and information security practitioners who are knowledgeable about their organization's data breach and the costs associated with resolving the breach. For privacy purposes, we did not collect organization-specific information.

**How do you calculate the cost?**
To calculate the average cost of 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.

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) and the California Consumer Privacy Act (CCPA) 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.

For consistency with prior years, we use the same currency translation method rather than adjusting accounting costs.

**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 524 organizations to participate in this study.

**Can the average per record cost be used to calculate the cost of breaches involving millions of lost or stolen records?**
The average cost of data breaches in our research does not apply to catastrophic or mega data breaches, such as Equifax, Capital One 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. It is not consistent with this research to use the per record cost to calculate the cost of single or multiple breaches totaling millions of records. However, the study uses a simulation framework for measuring the cost impact of a "mega breach" involving 1 million or more records, based on a sample of 17 very large breaches of this size.

**Why are you using simulation methods to estimate the cost of a mega data breach?**
The sample size of 17 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 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. To be consistent with previous reports, we recruit and match companies each year 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 3,940 organizations.

# Organization characteristics

This year's study included 524 organizations of various sizes, sampled across a wide range of geographies and industries. The 2020 study was conducted in 17 countries or regional samples and 17 industries.

For the first time, the study examined a cluster of organizations in Latin America, which is inclusive of Mexico, Argentina, Chile and Colombia.

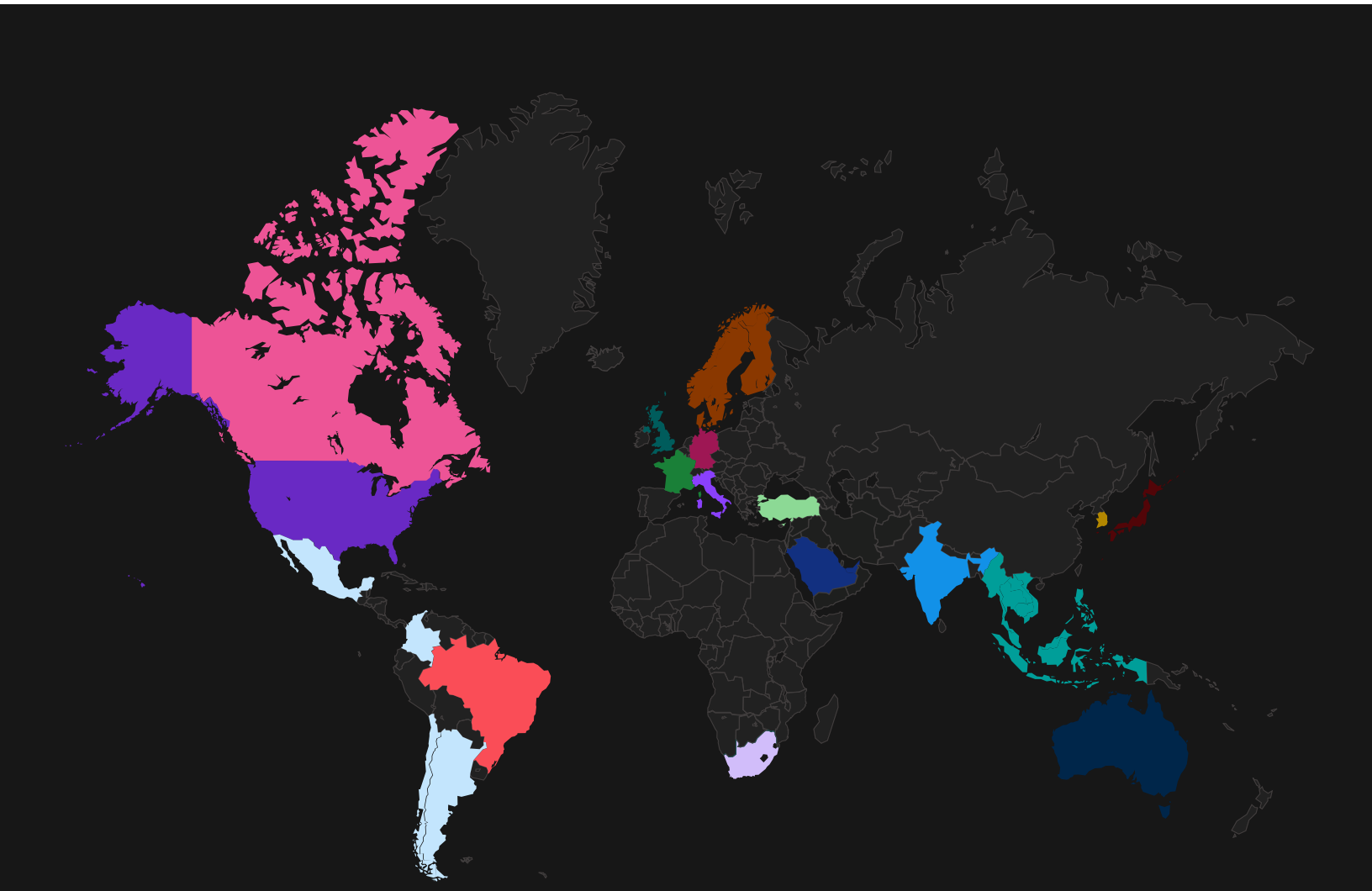
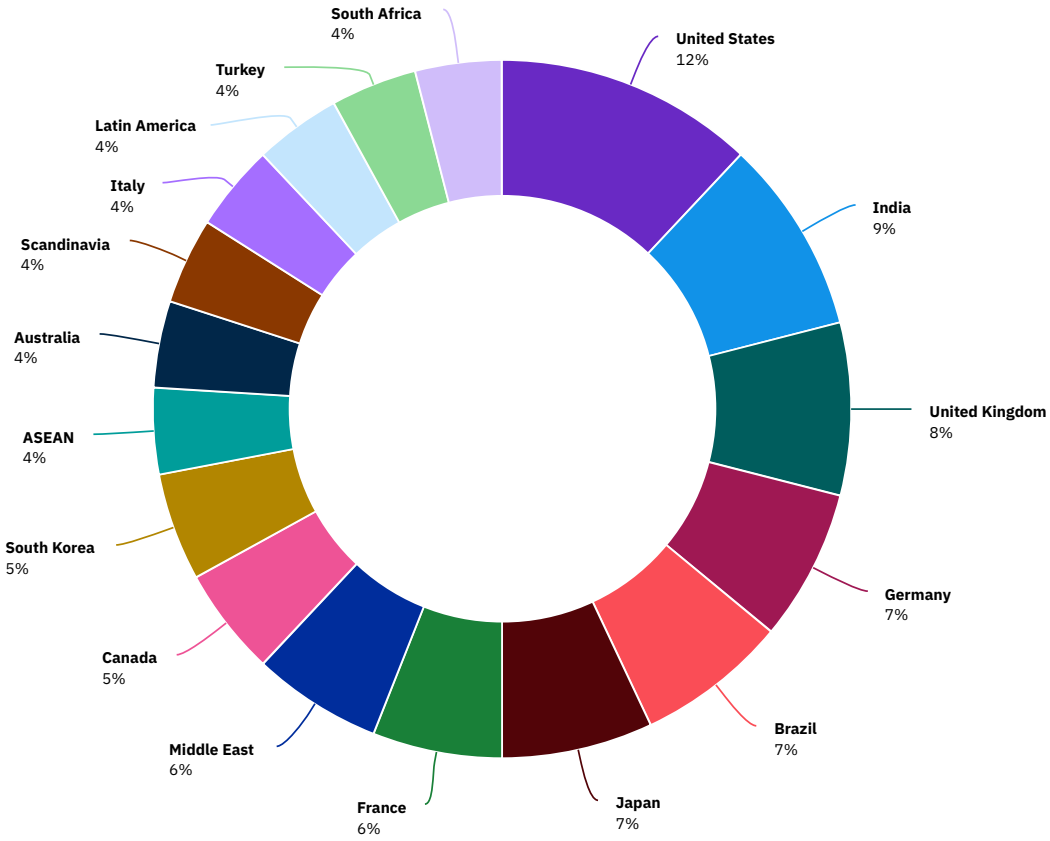


**Figure 47**

## Distribution of the sample by country or region



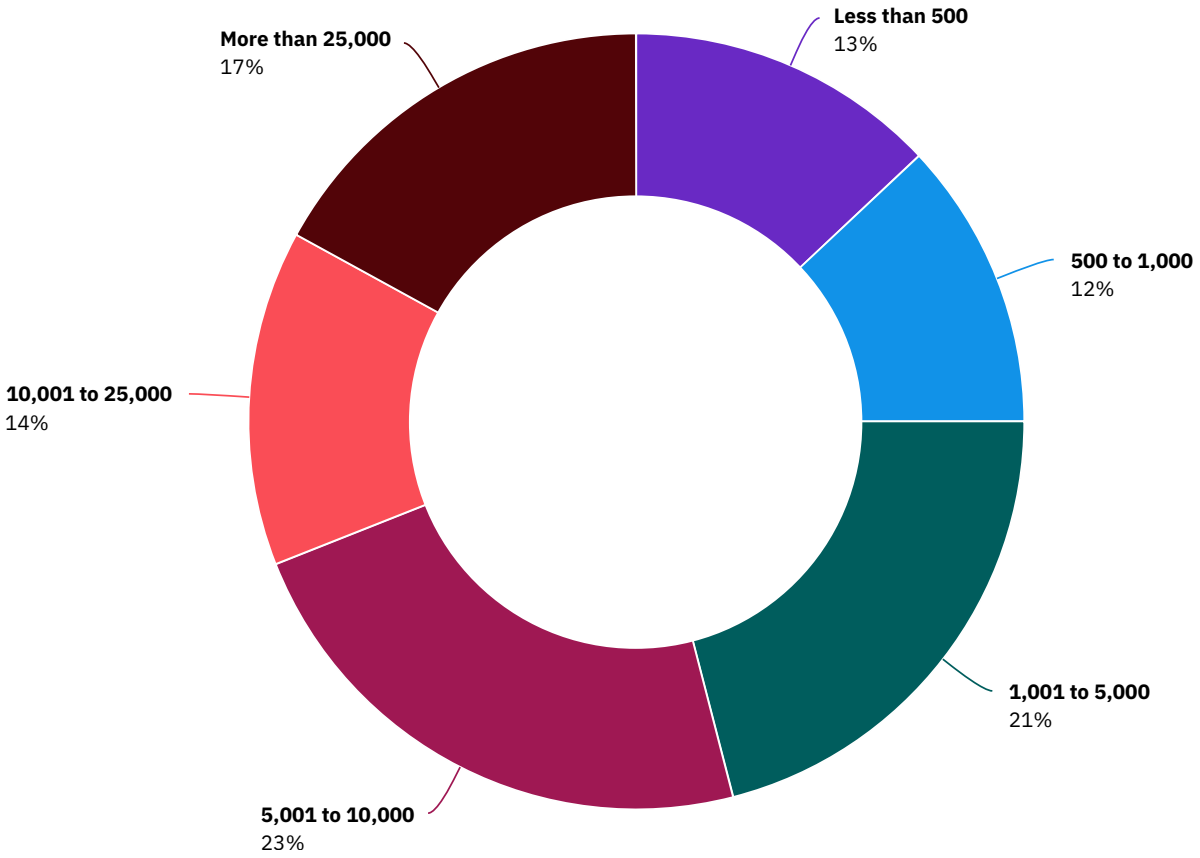

## Countries/regions from six continents were represented in the study.

**Figure 47** shows the distribution of benchmark organizations by their country or region. The United States had the highest representation at 12%, followed by India at 9% and the United Kingdom at 8%. Countries/regions with the smallest representation were ASEAN, Australia, Scandinavia, Italy, Latin America, Turkey and South Africa.

**Figure 48**

## Distribution of the sample by company size

Measured by employee headcount

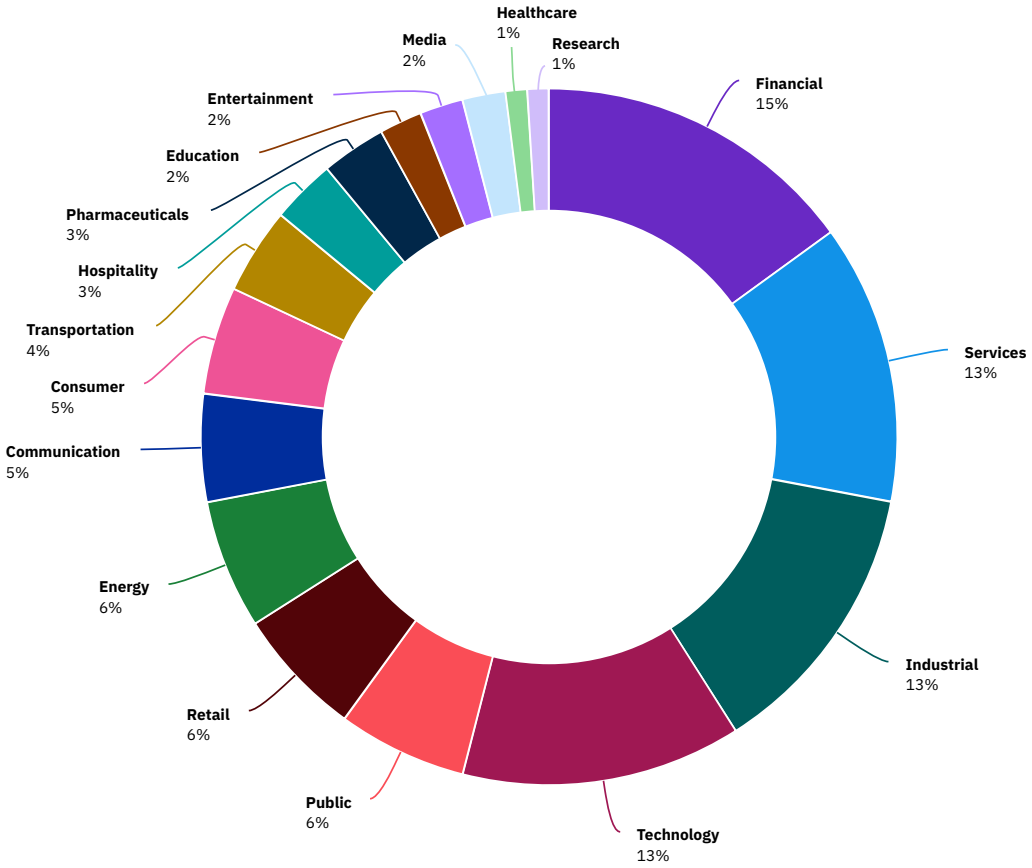



### Small, medium and large organizations were represented.

**Figure 48** shows distribution of the 524 organizations in the sample by headcount, which is a proxy for company size. The sample was weighted slightly more towards mid-sized organizations, with 58% of organizations between 1,001 and 25,000 employees, while 25% had less than 1,000 employees and 17% had more than 25,000 employees.

**Figure 49**

## Distribution of the sample by industry




## Industry representation leaned towards a few large sectors.

**Figure 49** shows the distribution of benchmark organizations by industry. Seventeen industries were represented in this year's study. The largest sectors were financial, services, industrial and technology. The explanation of industry definitions is provided separately.

# Definitions of industries

**Healthcare**
Hospitals, clinics

**Financial**
Banking, insurance, investment companies

**Energy**
Oil and gas companies, utilities, alternative energy producers and suppliers

**Pharmaceuticals**
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

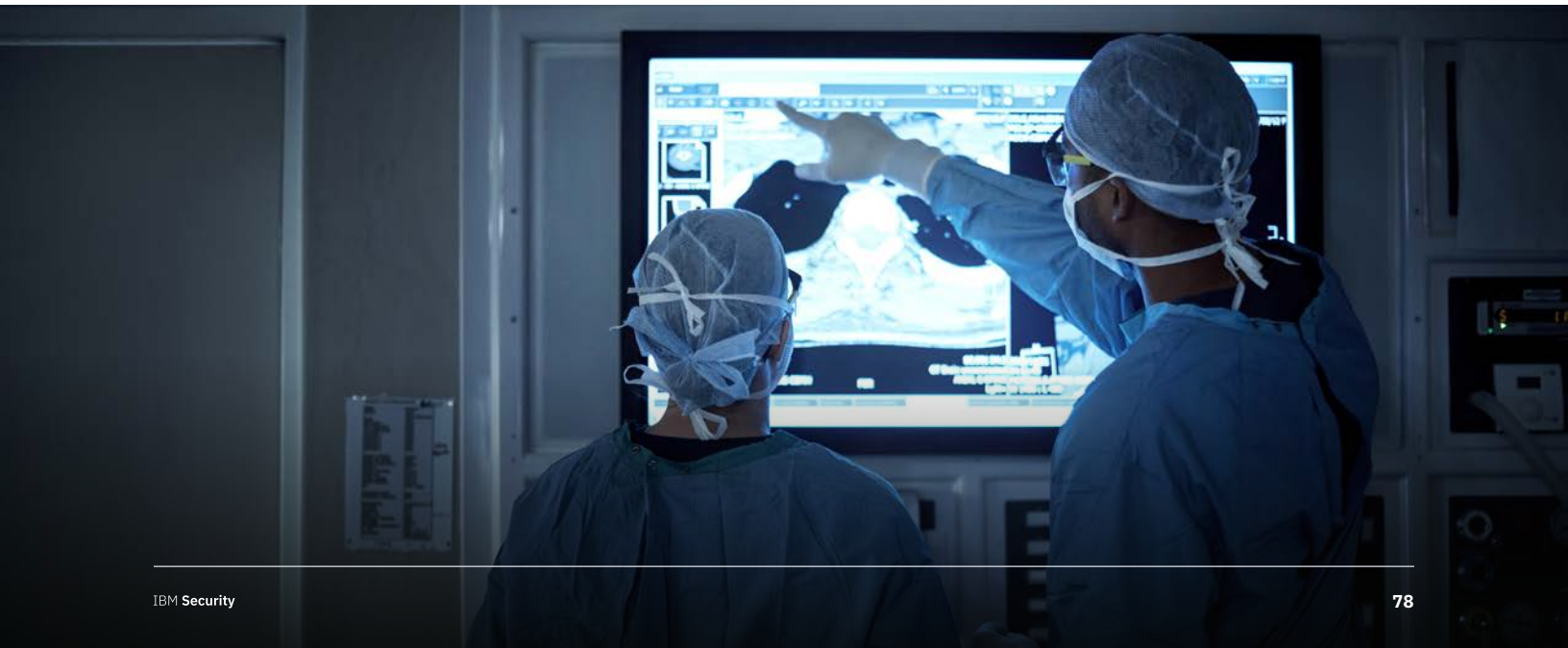
**Media**
Television, satellite, social media, Internet

**Hospitality**
Hotels, restaurant chains, cruise lines

**Retail**
Brick and mortar and e-commerce

**Research**
Market research, think tanks, R&D

**Public**
Federal, state and local government agencies and NGOs



# 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. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.

**Non-response**
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 does not capture company-identifying information. It allows individuals to use categorical response variables to disclose demographic information about the company and industry category.

**Unmeasured factors**
We omitted 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**
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.

**Extrapolated cost results**
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.

# About Ponemon Institute and IBM Security

The *Cost of a Data Breach Report* is produced jointly between Ponemon Institute and IBM Security. The research is conducted independently by Ponemon Institute, and the results are sponsored, analyzed, reported and published by IBM Security.


*If you have questions or comments about this research report, including for permission to cite or reproduce the 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


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.

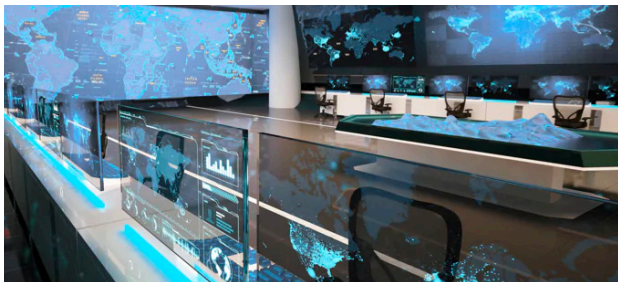
Ponemon Institute upholds strict data confidentiality, privacy and ethical research standards, and does not collect any personally identifiable information from individuals (or company identifiable information in business research). Furthermore, strict quality standards ensure that subjects are not asked extraneous, irrelevant or improper questions.

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 drive security into the fabric of their business so they can thrive in the face of uncertainty.

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

# Take the next steps



**Cybersecurity services**

Reduce risk with consulting, cloud and managed security services

Learn more →

**Identity and access management**

Connect every user, API and device to every app securely

Learn more →

**Data security**

Discover, classify and protect sensitive enterprise data

Learn more →

**Security information and event management**

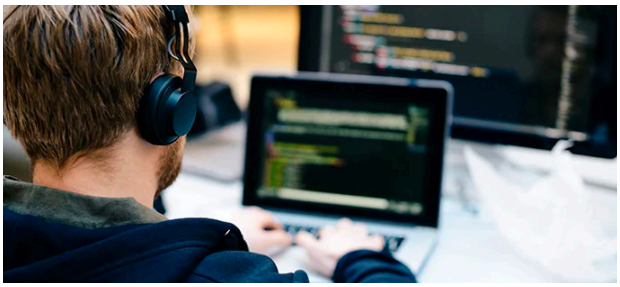
Gain visibility to detect, investigate and respond to threats

Learn more →

**Security orchestration, automation and response**

Accelerate incident response with orchestration and automation

Learn more →



**Cloud security**

Integrate security into your journey to hybrid multicloud

Learn more →

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2020



IBM **Security**