IBM Security

Cost of a Data Breach Report 2021

IBM

Executive summary

Key findings

How we calculate cost

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Executive summary

Now in its 17th year, the Cost of a Data Breach Report has become one of the leading benchmark reports in the cybersecurity industry. This report offers IT, risk management and security leaders a lens into dozens of factors that can increase or help mitigate the rising cost of data breaches.

With research conducted independently by the Ponemon Institute, this report – sponsored, analyzed, and published by IBM Security – studied 537 real breaches across 17 countries and regions and 17 different industries.

In the course of nearly 3,500 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 include:

1. Initial attack vectors that were primarily responsible for causing the breaches
2. The length of time it took the organizations to detect and contain their breaches
3. The effects of incident response and security artificial intelligence (AI) and automation on the average total cost

Executive summary

Key findings

How we calculate cost

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Each year, we aim to renew the report to offer analysis that builds upon past years' research while breaking new ground to keep up with changing technology and events to form a more relevant picture of the risks and strategies for securing data and responding to a breach. The 2021 edition of this report has new analysis related to the advancement of the zero trust approach, risks that continue to make cloud security essential, and the acceleration of remote working as a result of the pandemic.

The report is divided into six major sections, including:

- This executive summary with key findings and comments about how data breach costs were calculated
- A deep dive into the report's complete findings, with dozens of charts
- An exploration of a methodology for risk quantification
- Security recommendations that can help organizations mitigate the financial impacts of a breach
- Notes on the geographic, industry and company size characteristics of the organizations studied
- And a more detailed explanation of the study's methodology and limitations

IBM Security and the Ponemon Institute are pleased to present the results of the 2021 Cost of a Data Breach Report.

Years in this report refer to the year the report was published, not necessarily the year the breach occurred. Breaches in the 2021 report took place between May 2020 and March 2021.

Executive summary

Key findings

How we calculate cost

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Key findings

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

10%

Increase in average total cost of a breach, 2020-2021

The average total cost of a data breach increased by nearly 10% year over year, the largest single year cost increase in the last seven years.

Data breach costs rose from $3.86 million to $4.24 million, the highest average total cost in the history of this report. Costs were significantly lower for some of organizations with a more mature security posture, and higher for organizations that lagged in areas such as security AI and automation, zero trust and cloud security.

Note: Cost amounts in this report are measured in U.S. dollars.

$1.07m

Cost difference where remote work was a factor in causing the breach

Remote working and digital transformation due to the COVID-19 pandemic increased the average total cost of a data breach.

The average cost was $1.07 million higher in breaches where remote work was a factor in causing the breach, compared to those where remote work was not a factor. The percentage of companies where remote work was a factor in the breach was 17.5%. Additionally, organizations that had more than 50% of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50% or less working remotely. IT changes such as cloud migration and remote work increased costs, yet organizations that did not implement any digital transformation changes as a result of COVID-19 experienced $750,000 higher costs compared to the global average, a difference of 16.6%.

11

Consecutive years healthcare had the highest industry cost of a breach

Healthcare organizations experienced the highest average cost of a data breach, for the eleventh year in a row.

Healthcare data breach costs increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase. Costs varied widely across industries, and year over year. Costs in the energy sector decreased from $6.39 million in 2020 to an average $4.65 million in 2021. Costs surged in the public sector, which saw a 78.7% increase in average total cost from $1.08 million to $1.93 million.

Executive summary

Key findings

How we calculate cost

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

38%

Lost business share of total breach costs

Lost business represented the largest share of breach costs, at an average total cost of $1.59M.

Lost business represented 38% of the overall average and increased slightly from $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.

$180

Per record cost of personally identifiable information

Customer personally identifiable information (PII) was the most common type of record lost, included in 44% of breaches.

Customer PII was also the costliest record type, at $180 per lost or stolen record. The overall average cost per record in the 2021 study was $161, an increase from $146 per lost or stolen record in the 2020 report year.

20%

Share of breaches initially caused by compromised credentials

Compromised credentials was the most common initial attack vector, responsible for 20% of breaches.

Business email compromise (BEC) was responsible for only 4% of breaches, but had the highest average total cost of the 10 initial attack vectors in the study, at $5.01 million. The second costliest was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million).

Executive summary

Key findings

How we calculate cost

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

287

Average number of days to identify and contain a data breach

The longer it took to identify and contain, the more costly the breach.

Data breaches that took longer than 200 days to identify and contain cost on average $4.87 million, compared to $3.61 million for breaches that took less than 200 days. Overall, it took an average of 287 days to identify and contain a data breach, seven days longer than in the previous report. To put this in perspective, if a breach occurring on January 1 took 287 days to identify and contain, the breach wouldn't be contained until October 14th. The average time to identify and contain varied widely depending on the type of data breach, attack vector, factors such as the use of security AI and automation, and cloud modernization stage.

100x

Cost multiplier of > 50 million records vs. average breach

Average cost of a mega breach was $401 million for breaches between 50 million and 65 million records, an increase from $392 million in 2020.

In a small sample of mega breaches of 1 million to 65 million records, breaches were many times more expensive than the average cost of smaller breaches. Breaches of 50 million to 65 million records were nearly 100x more expensive than breaches of 1,000-100,000 records.

$1.76m

Cost difference in breaches where mature zero trust was deployed vs. no zero trust

A zero trust approach helped reduce the average cost of a data breach.

The average cost of a breach was $5.04 million for those without zero trust deployed. Yet in the mature stage of zero trust deployment, the average cost of a breach was $3.28 million, $1.76 million less than organizations without zero trust, representing a 2.3% difference.

Executive summary

Key findings

How we calculate cost

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

80%

Cost difference where security AI and automation was fully deployed vs. not deployed

Security AI and automation had the biggest positive cost impact.

Organizations with fully deployed security AI and automation experienced breach costs of $2.90 million, compared to $6.71 million at organizations without security AI and automation. The difference of $3.81 million, or nearly 80%, represents the largest gap in the study when comparing breaches with vs. without a particular cost factor. The share of organizations with fully or partially deployed security AI and automation was 65% in 2021 vs. 59% in 2020, a 6 percentage point increase and continuing an upward trend. Security AI/automation was associated with a faster time to identify and contain the breach.

$3.61m

Average cost of a breach in hybrid cloud environments

Hybrid cloud had the lowest average total cost of a data breach, compared to public, private and on premise cloud models.

Data breaches in hybrid cloud environments cost an average of $3.61 million, $1.19 million less than public cloud breaches, or a difference of 28.3%. While companies that were in the midst of a large cloud migration experienced higher breach costs, those that were further along in their cloud modernization maturity were able to identify and contain breaches 77 days faster than those in the early stages of modernization.

$2.30m

Cost difference for breaches with high vs. low level of compliance failures

System complexity and compliance failures were top factors amplifying data breach costs.

Organizations with a high level of system complexity had an average cost of a breach $2.15 million higher than those who had low levels of complexity. The presence of a high level of compliance failures was associated with breach costs that were $2.30 million higher than breach costs at organizations without this factor present.

Executive summary

Key findings

How we calculate cost

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

$4.62m

Average total cost of a ransomware breach

Ransomware and destructive attacks were costlier than other types of breaches.

Ransomware attacks cost an average of $4.62 million, more expensive than the average data breach ($4.24 million). These costs included escalation, notification, lost business and response costs, but did not include the cost of the ransom. Malicious attacks that destroyed data in destructive wiper-style attacks cost an average of $4.69 million. The percentage of companies where ransomware was a factor in the breach was 7.8%.

Executive summary

Key findings

How we calculate cost

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

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 2021 study ranged in size between 2,000 and 101,000 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 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

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

Notification

Activities that enable the company to notify datasubjects, 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

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

Post breach 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 fine

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

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. Initial attack vectors
3. Lifecycle of a breach
4. Regulatory compliance failures
5. Impact of zero trust
6. Security AI and automation
7. Cloud breaches and migration
8. COVID-19 and remote work
9. Cost of a mega breach

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Global findings and highlights

The Cost of a Data Breach Report is a global report, combining results from 537 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 finding

$4.24m

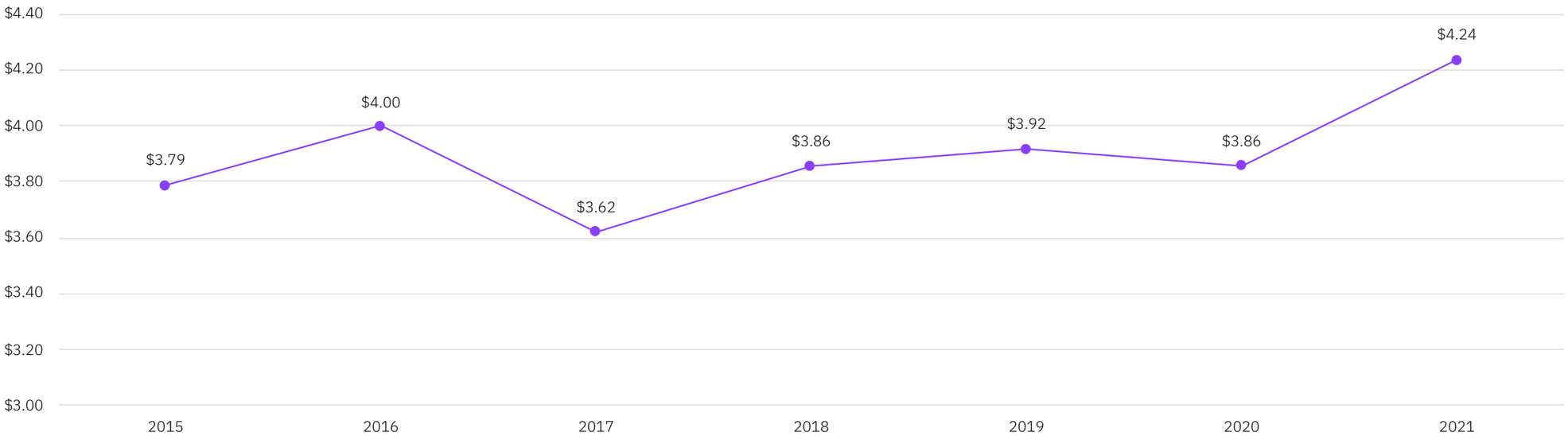
Global average total cost of a data breach

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 1

Average total cost of a data breach

Measured in US$ millions



The average total cost of a data breach increased by the largest margin in seven years.

Data breach costs increased significantly year-over year from the 2020 report to the 2021 report, increasing from $3.86 million in 2020 to $4.24 million in 2021.

The increase of $0.38 million ($380,000) represents a 9.8% increase. This compares to a decrease of 1.5% from the 2019 to 2020 report year. The cost of a data breach has increase by 11.9% since 2015.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

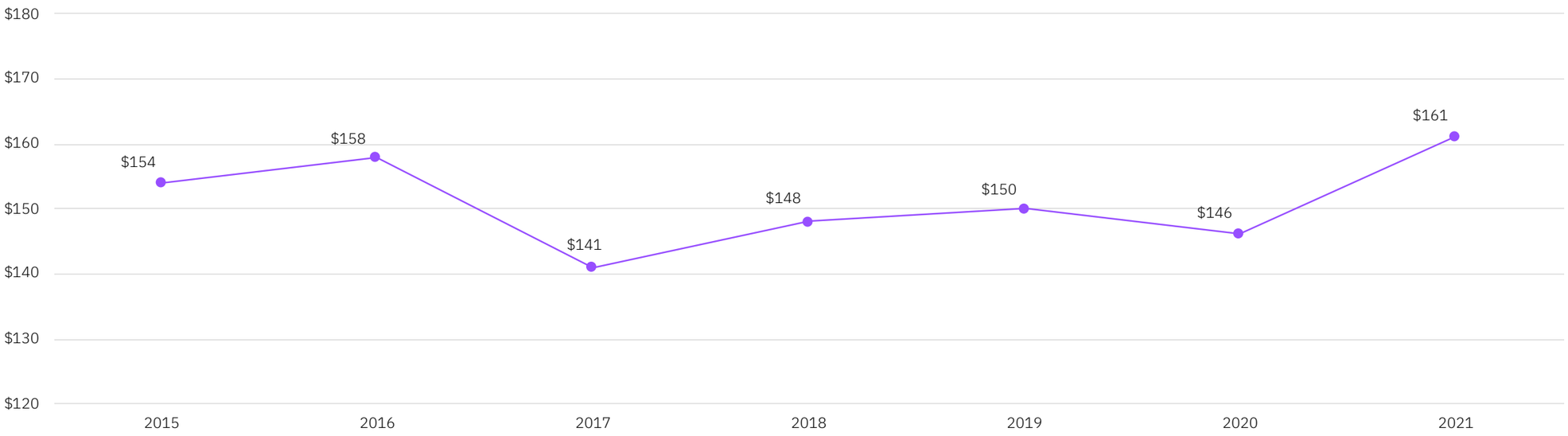
About IBM Security and the Ponemon Institute

Take the next steps

Figure 2

Average per record cost of a data breach

Measured in US$



The average per record (per capita) cost of a data breach increased 10.3% from 2020 to 2021.

In 2021 the per record cost of a breach was $161, compared to an average cost of $146 in 2020. This represents an increase of 14.2% since the 2017 report, when the average per record cost was $141.

*It is not consistent with this research to use the per record cost to calculate the cost of single or multiple breaches above 100,000 records. For more information, see the research methodology section.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 3

Average total cost of a data breach by country or region

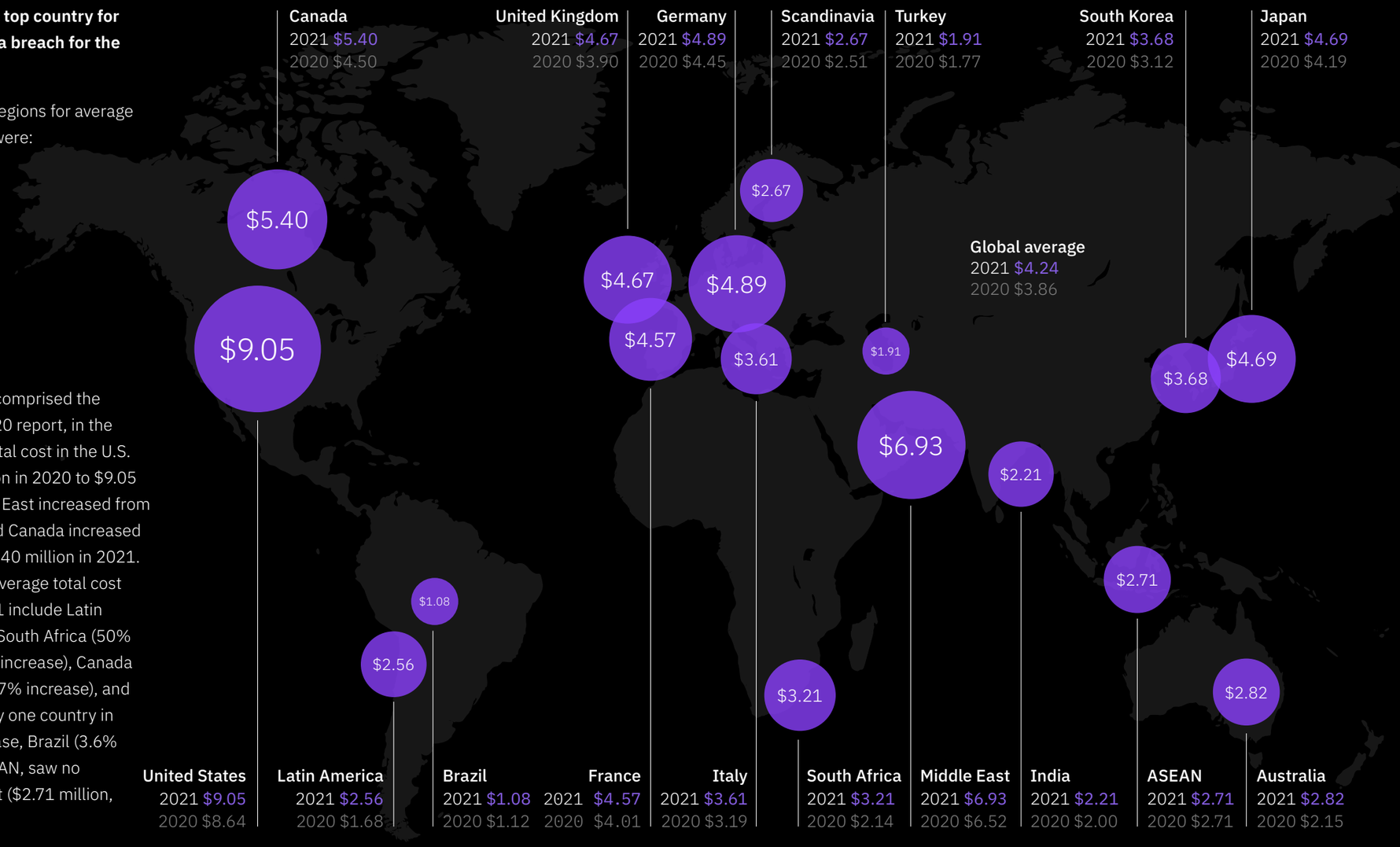
Measured in US$ millions

The United States was the top country for average total cost of a data breach for the eleventh year in a row.

The top five countries and regions for average total cost of a data breach were:

1. U.S.
2. Middle East
3. Canada
4. Germany
5. Japan

These same five countries comprised the top five countries in the 2020 report, in the same order. The average total cost in the U.S. increased from $8.64 million in 2020 to $9.05 million in 2021. The Middle East increased from $6.52 million to $6.93M and Canada increased from $4.50M in 2020 to $5.40 million in 2021. Countries with the largest average total cost increase from 2020 to 2021 include Latin America (52.4% increase), South Africa (50% increase), Australia (30.2% increase), Canada (20% increase), the UK (19.7% increase), and France (14% increase). Only one country in the study saw a cost decrease, Brazil (3.6% decrease). One region, ASEAN, saw no change in average total cost ($2.71 million, no change in 2021).



Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

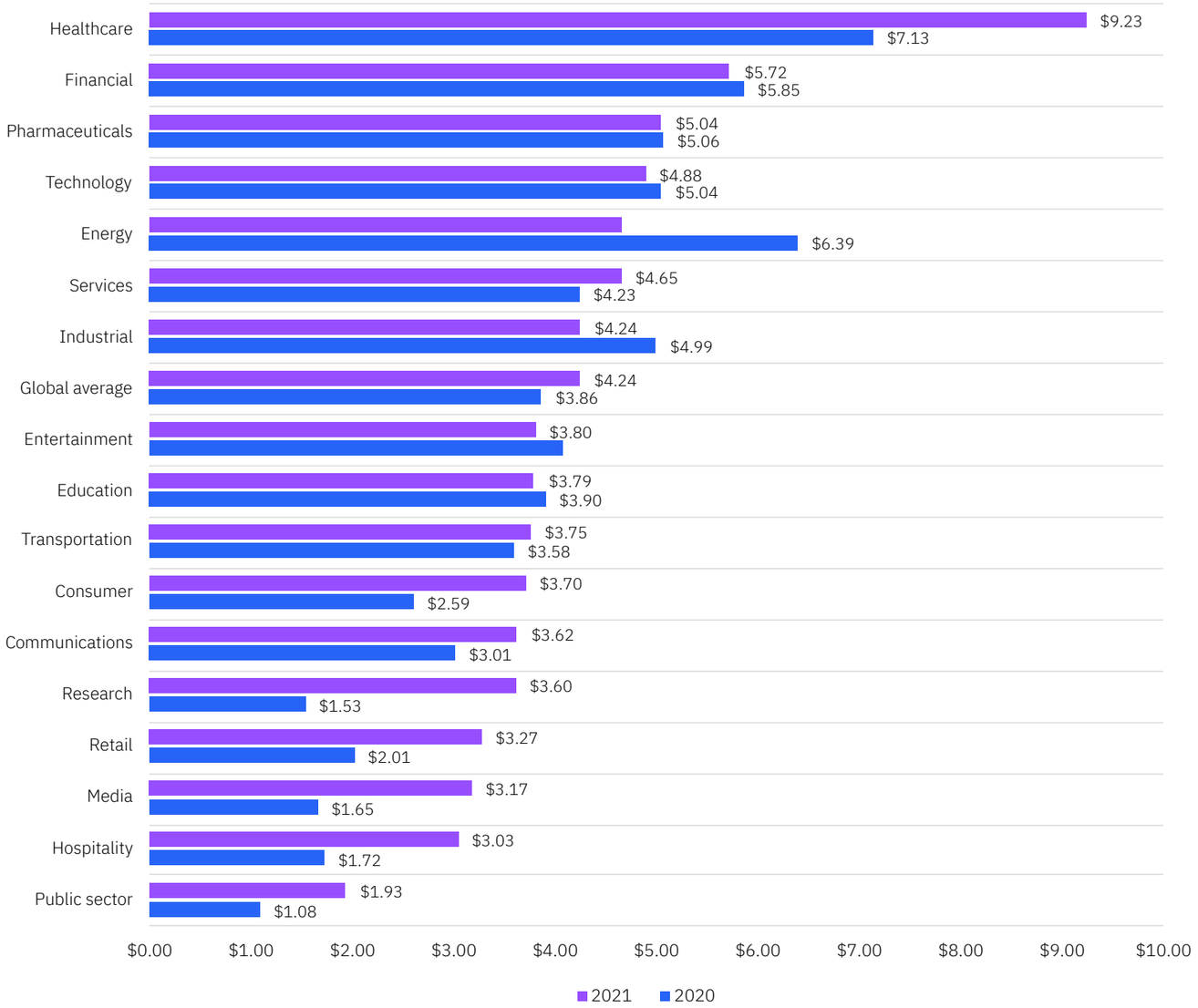
About IBM Security and the Ponemon Institute

Take the next steps

Figure 4

Average total cost of a data breach by industry

Measured in US$ millions



Healthcare was the top industry in average total cost for the eleventh year in a row.

The top five industries for average total cost were:

1. Healthcare
2. Financial
3. Pharmaceuticals
4. Technology
5. Energy

The average total cost for healthcare increased from $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase. Energy dropped from the second most costly industry to fifth place, decreasing in cost from $6.39 million in 2020 to $4.65 million in 2021 (27.2% decrease).

Other industries that saw large cost increases included services (7.8% increase), communications (20.3% increase), consumer (42.9% increase), retail (62.7% increase), media (92.1% increase), hospitality (76.2% increase), and public sector (78.7% increase).

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

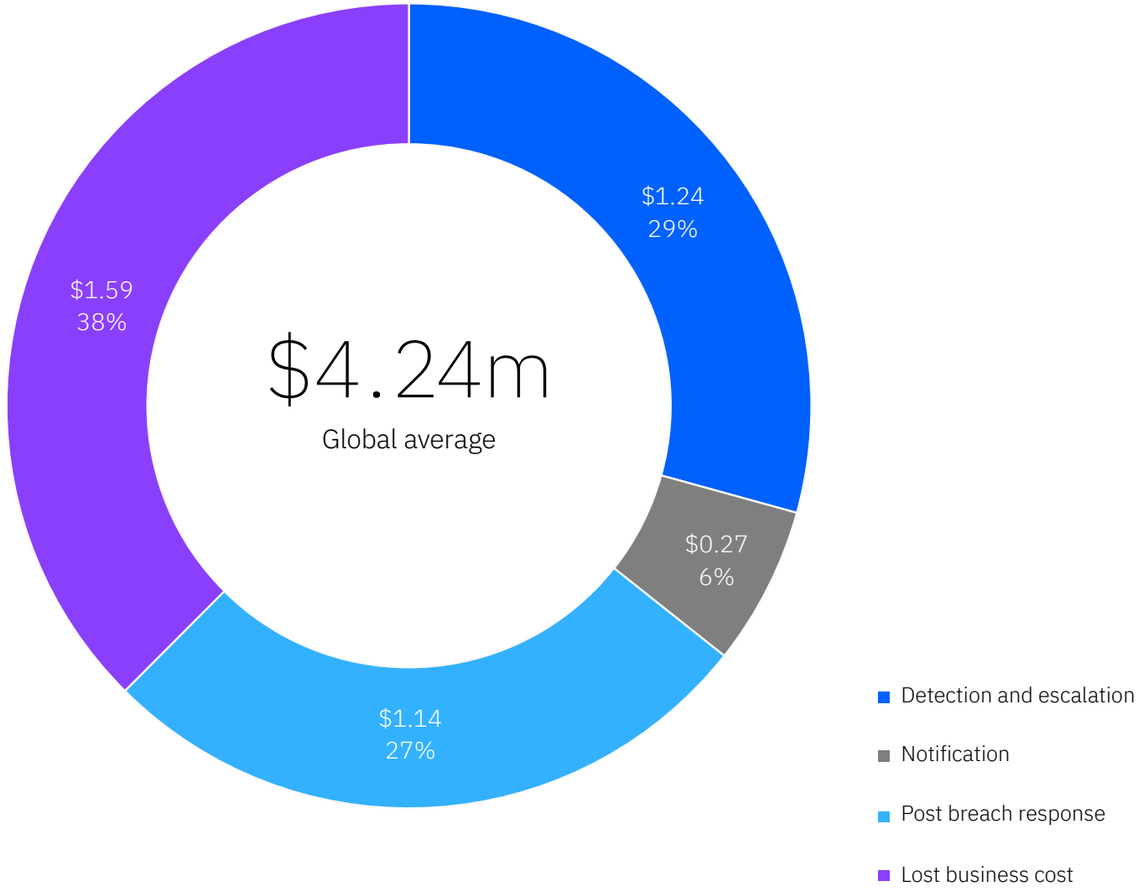
About IBM Security and the Ponemon Institute

Take the next steps

Figure 5

Average total cost of a data breach divided into four categories

Measured in US$ millions



Lost business continued to represent the largest share of data breach costs for the seventh year in a row.

Of the four cost categories, at an average total cost of $1.59 million, lost business accounted for 38% of the average total cost of a data breach. Lost business costs include: business disruption and revenue losses from system downtime, cost of lost customers and acquiring new customers, reputation losses and diminished goodwill.

The second most costly was detection and escalation costs, which had an average total cost of $1.24 million, or 29% of the total cost. The other cost categories are notification and post data breach response.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

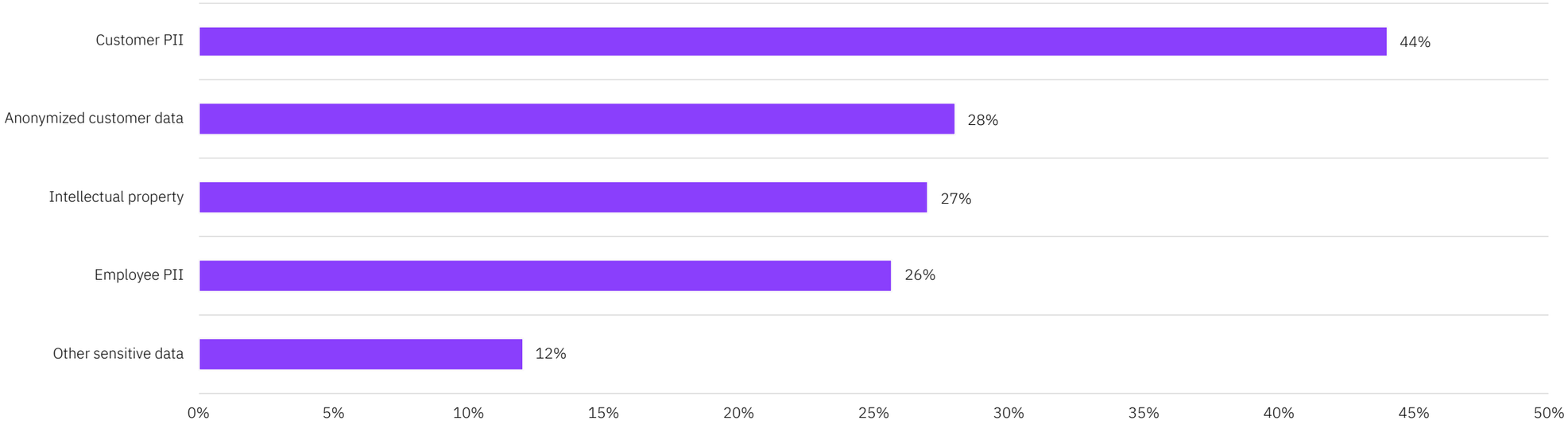
About IBM Security and the Ponemon Institute

Take the next steps

Figure 6

Types of records compromised

Percentage of breaches involving data in each category



Customer personally identifiable information (PII) was the most common type of record lost or stolen.

Customer PII was included in 44% of all breaches in the study. Anonymized customer data (i.e., data that is modified to remove PII) was compromised in 28% of the breaches studied, the second most common type of record compromised in breaches.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

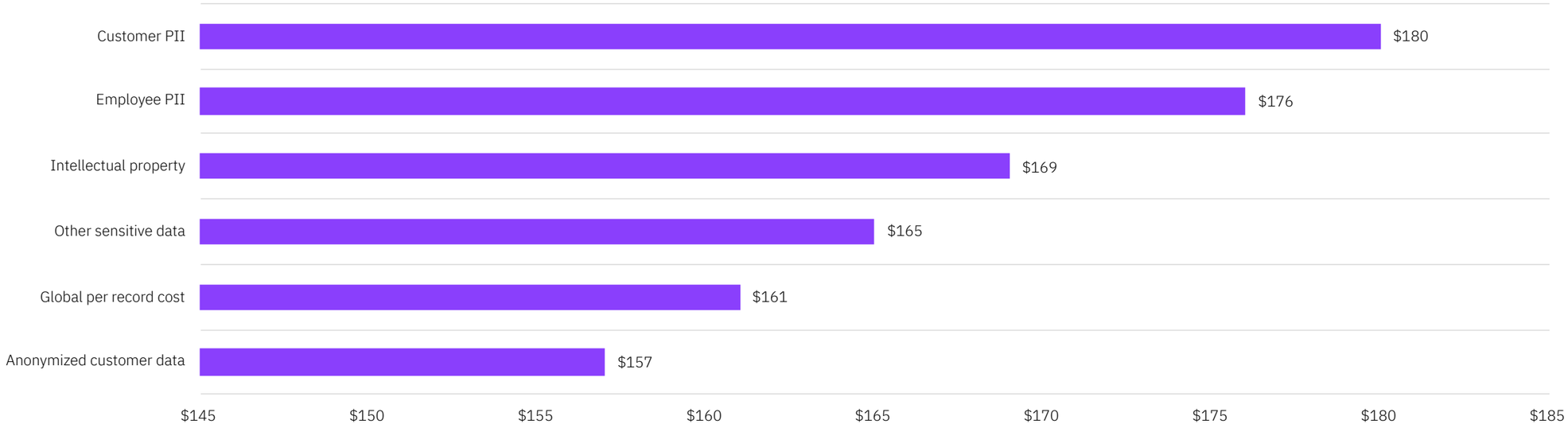
About IBM Security and the Ponemon Institute

Take the next steps

Figure 7

Average cost per record by type of data compromised

Measured in US$



Customer PII was the costliest type of record lost or stolen in breaches.

Customer PII cost an average of $180 per lost or stolen record in 2021. In 2020, customer PII cost $150 per lost or stolen record, representing an increase of 20%.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Initial attack vectors

This section looks at the prevalence and cost of initial attack vectors of data breaches. The breaches in the study are divided into 10 initial attack vectors, ranging from accidental data loss and cloud misconfiguration to phishing, insider threats, and lost or stolen (i.e., compromised) credentials.

Key finding

$5.01m

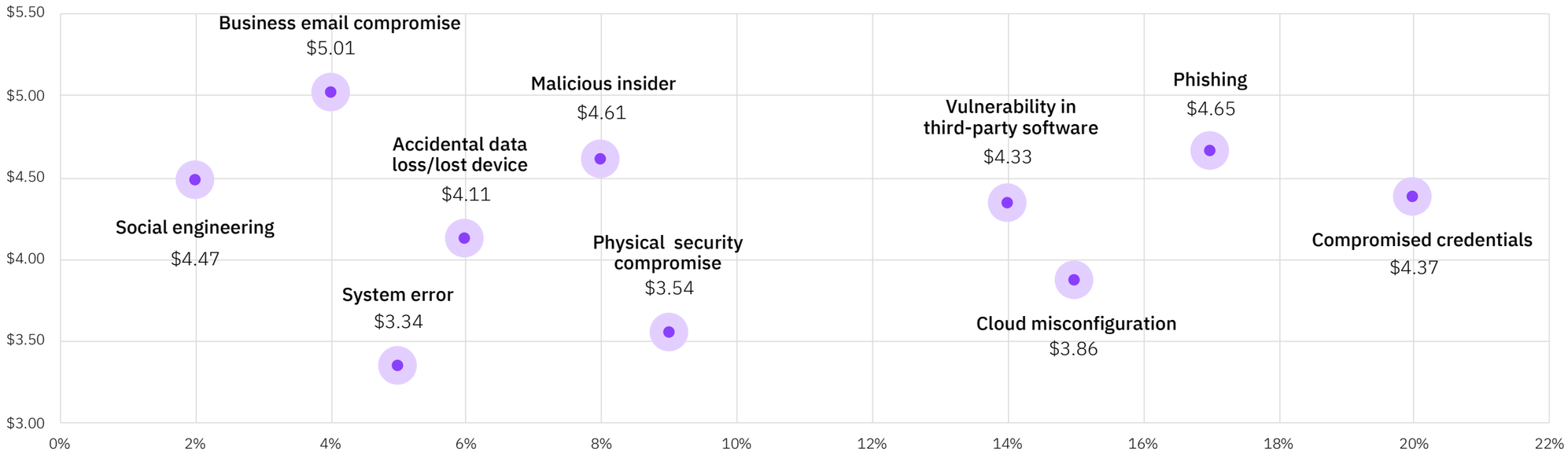
Average total cost of a breach caused by business email compromise

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 8

Average total cost and frequency of data breaches by initial attack vector

Measured in US$ millions



The most common initial attack vector in 2021 was compromised credentials, responsible for 20% of breaches.

In 2021, the most frequent initial attack vectors were (1) compromised credentials, 20% of breaches (2) phishing, 17% (3) cloud misconfiguration, 15%. Business email compromise was responsible for only 4% of breaches but had the highest average total cost at $5.01 million. The second costliest initial attack vector was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million). The top four initial attack vectors were the same in 2021 as compared to the 2020 study, but slightly re-ordered. Phishing moved up from fourth to second most common, and cloud misconfiguration fell from second to third-most common. Vulnerabilities in third-party software (average cost of $4.33 million) fell from third to fourth in frequency, a category that was the initial attack vector in 14% of breaches in 2021, compared to about 16% of breaches in 2020.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Lifecycle of a breach

The time elapsed between the first detection of the breach and its containment is referred to as the data breach lifecycle. 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. These metrics can be used to determine the effectiveness of an organization's incident response and containment processes.

Key finding

$4.87m

Average cost of a breach with a lifecycle over 200 days

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

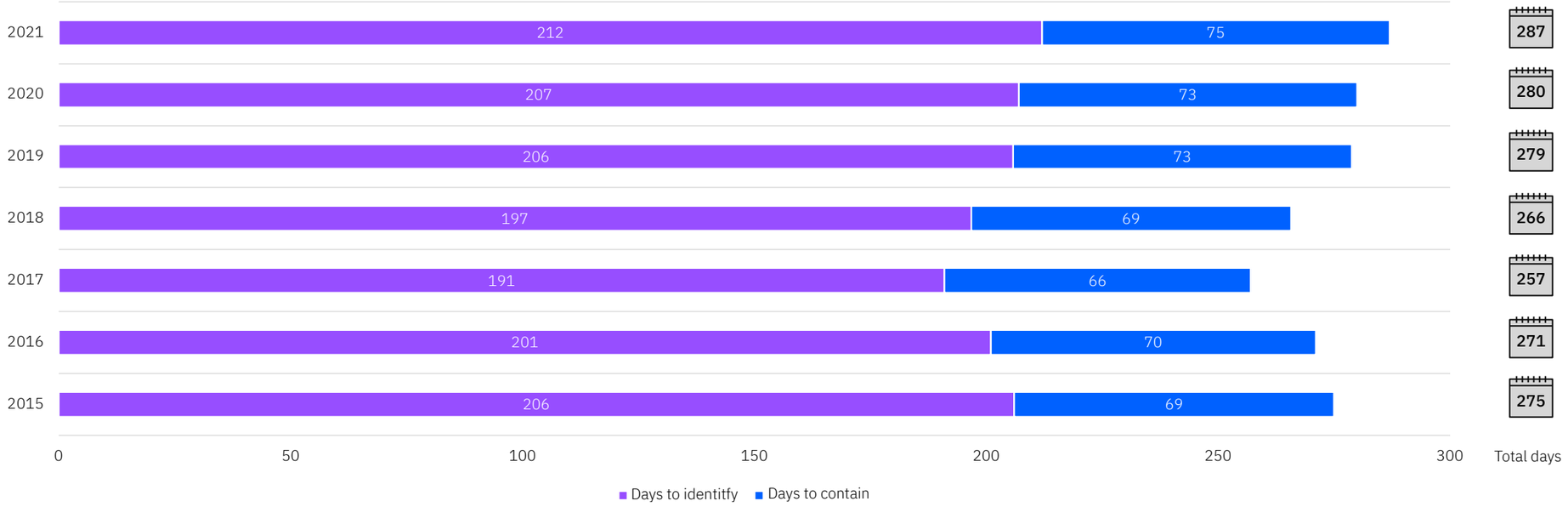
About IBM Security and the Ponemon Institute

Take the next steps

Figure 9

Average time to identify and contain a data breach

Measured in days



The data breach lifecycle took a week longer in 2021 than in 2020.

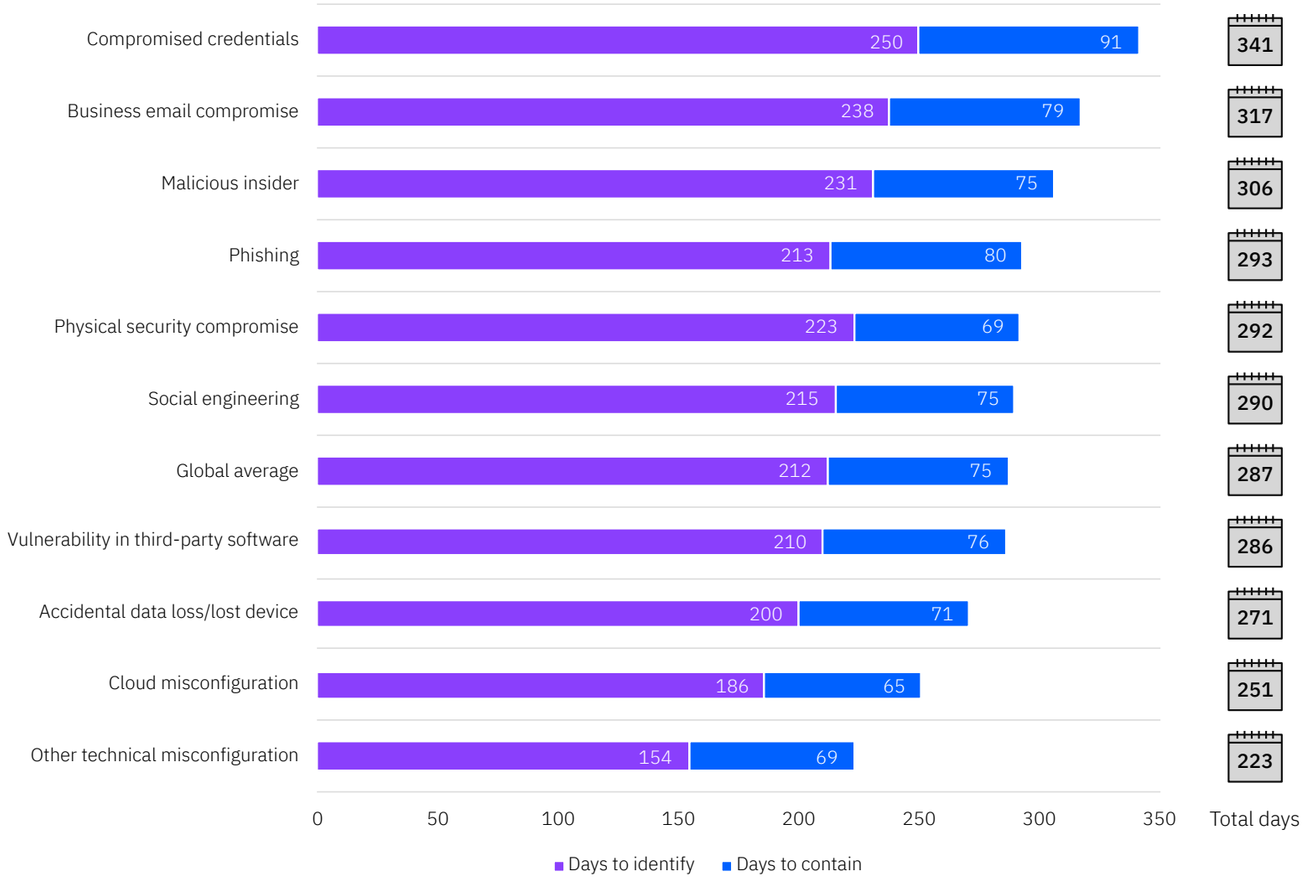
In 2021 it took an average of 212 days to identify a breach and an average 75 days to contain a breach, for a total lifecycle of 287 days. If a breach occurred on January 1st and it took 287 days to identify and contain, the breach would not be contained until October 14th.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 10

Average time to identify and contain a breach by initial attack vector

Measured in days



On average, a breach caused by stolen credentials that occurred on January 1st would take until December 7 to be contained.

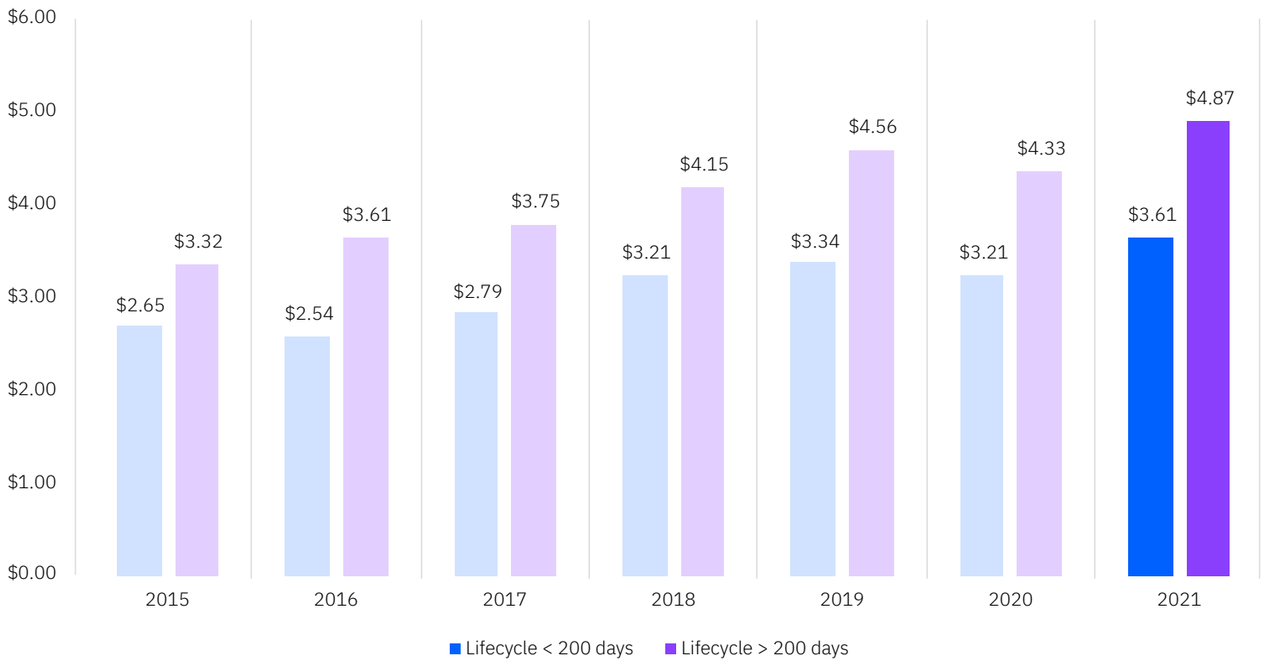
Breaches caused by stolen/compromised credentials took the longest number of days to identify (250) and contain (91) on average, for an average total of 341 days. Business email compromise had the second longest breach lifecycle at 317 days and malicious insider breaches took the third longest number of days to identify and contain at 306 days.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 11

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

Measured in US$ millions



A data breach lifecycle of less than 200 days produced a cost savings of nearly a third over a breach lifecycle longer than 200 days.

A breach with a lifecycle over 200 days cost an average of $4.87 million in 2021, vs. $3.61 million for a breach with a lifecycle of less than 200 days. The gap of $1.26 million represents a difference of 29.7%. This gap between breaches with a lifecycle shorter/longer than 200 days was $1.12 million in 2020. That means the beneficial cost impact of containment in less than 200 days grew from 2020 to 2021.

Tweet →

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 12

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

Measured in US$ millions

Incident response teams and incident response plan testing continued to mitigate costs in 2021.

The gap in average total cost between breaches at organizations with both IR teams and IR plan testing (IR capabilities), and organization with no IR team and no IR plan testing continued to grow. Breaches at organizations with IR capabilities cost an average of $3.25 million in 2021, compared to $3.32 million in 2020. The average total cost of a breach at organizations with no IR capabilities was $5.71 million in 2021, an increase from $5.09 million in 2020. The average total cost gap between IR capabilities vs. no IR capabilities was $2.46 million in 2021, representing a 54.9% difference.

The average cost difference between breaches at organizations with IR capabilities and organizations without IR capabilities was 42.1% in 2020. This indicates a growing cost difference effectiveness of IR capabilities from 2020 to 2021 (difference of $2.46 million in 2021 vs. $1.77 million in 2020). The average total cost of a breach at organizations with IR capabilities had a difference of 26.4% compared to the overall average total cost of $4.24 million in 2021.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Regulatory compliance failures

This year's research study looked closely at the impacts of regulatory compliance failures. In this section, we first looked at the impact of compliance failures on the average total cost of a data breach. Out of a selection of 25 cost factors that either amplify or mitigate data breach costs, compliance failures was the top cost amplifying factor.

We then looked at the difference in "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, healthcare, consumer goods, financial, technology, pharmaceuticals, 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.

Key finding

$5.65m

Average cost of a breach at organizations with high level compliance failures

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

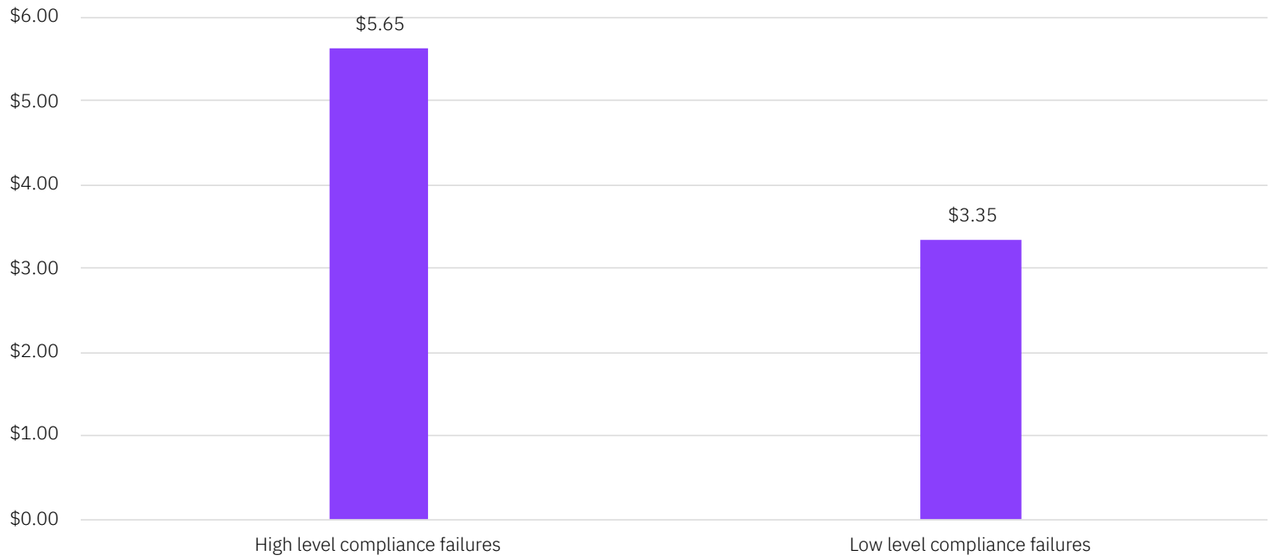
About IBM Security and the Ponemon Institute

Take the next steps

Figure 13

Impact of compliance failures on the average cost of a data breach

Measured in US$ millions



Compliance failures was the top factor found to amplify data breach costs.

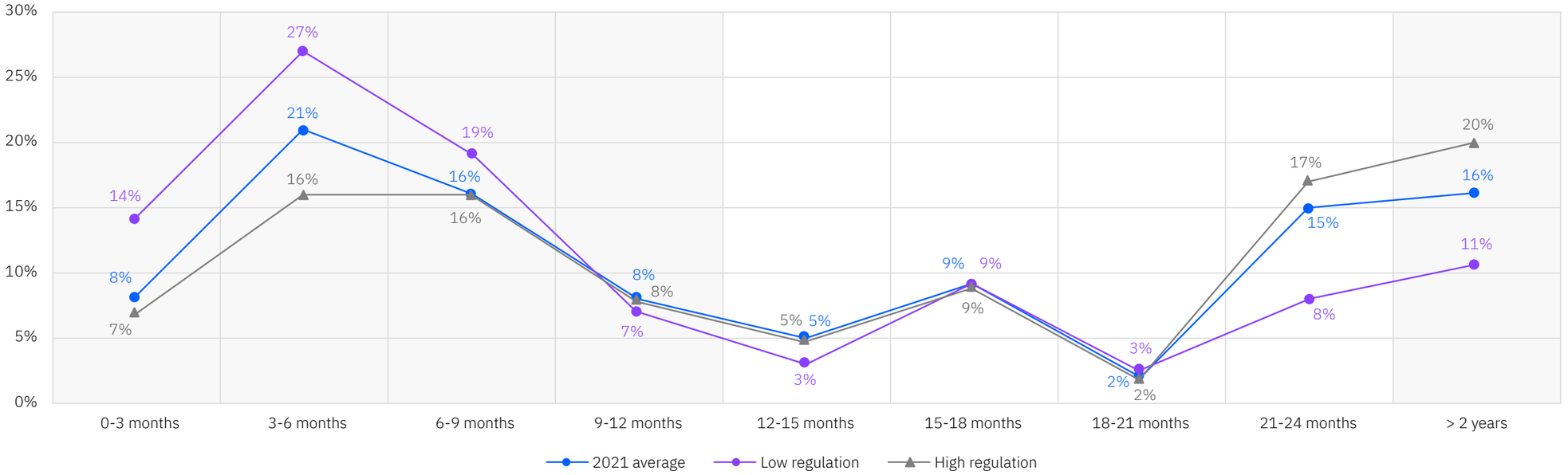
Organizations with a high level of compliance failures (resulting in fines, penalties and lawsuits) experienced an average cost of a data breach of $5.65 million, compared to $3.35 million at organizations with low levels of compliance failures, a difference of $2.3 million or 51.1%.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 14

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

Percentage of total costs accrued in three month intervals



Breaches in stricter regulatory environments tended to see more costs accrue in later years following the breach.

The difference between high regulatory environments and low regulatory environments was most pronounced in breach costs incurred more than two years after the breach. In highly regulated industries, 20% of costs were incurred after two years, vs. 11% of costs in less regulated industries. Overall averages found that 16% of breach costs were incurred after two years. In less regulated industries, 68% of costs were incurred in the first 12 months, vs. 46% of costs in highly regulated industries. Note: This research examined a sample of breaches over two-plus years – 83 breaches in a high regulatory environment and 101 in a low regulatory environment.

	2021 avg.	Low	High
Time elapsed	**Percentage of total cost**		
1st year	53%	67%	47%
2nd year	31%	22%	33%
2+ years	16%	11%	20%

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Impact of zero trust

For the first year, this study examined the prevalence and impact of a zero trust security architecture. This approach operates on the assumption that user identities or the network itself may already be compromised, and instead relies on AI and analytics to continuously validate connections between users, data and resources.

Key finding

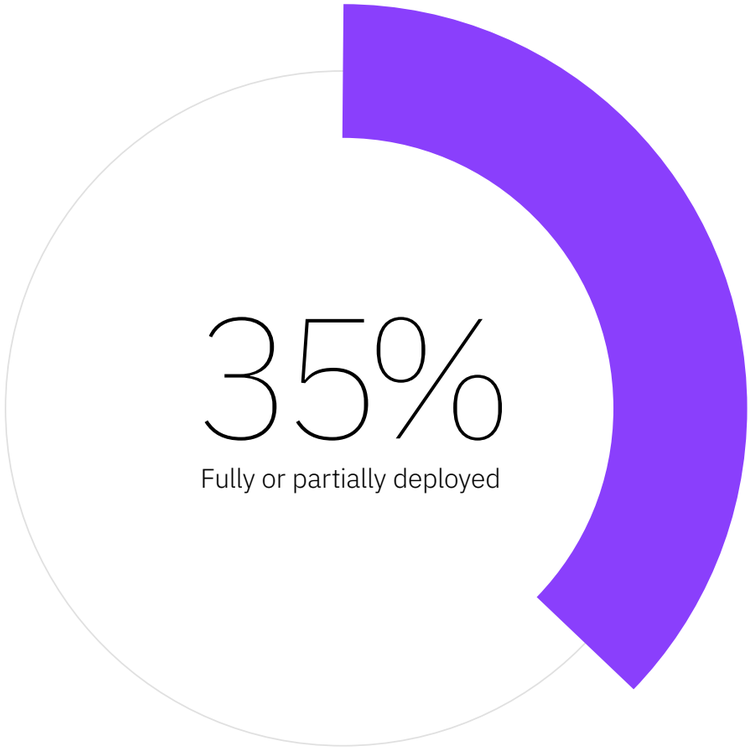
$5.04m

Average cost of a breach at organizations without zero trust deployed

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 15

Has your organization deployed zero trust?



Only about a third of organizations have a zero trust approach.

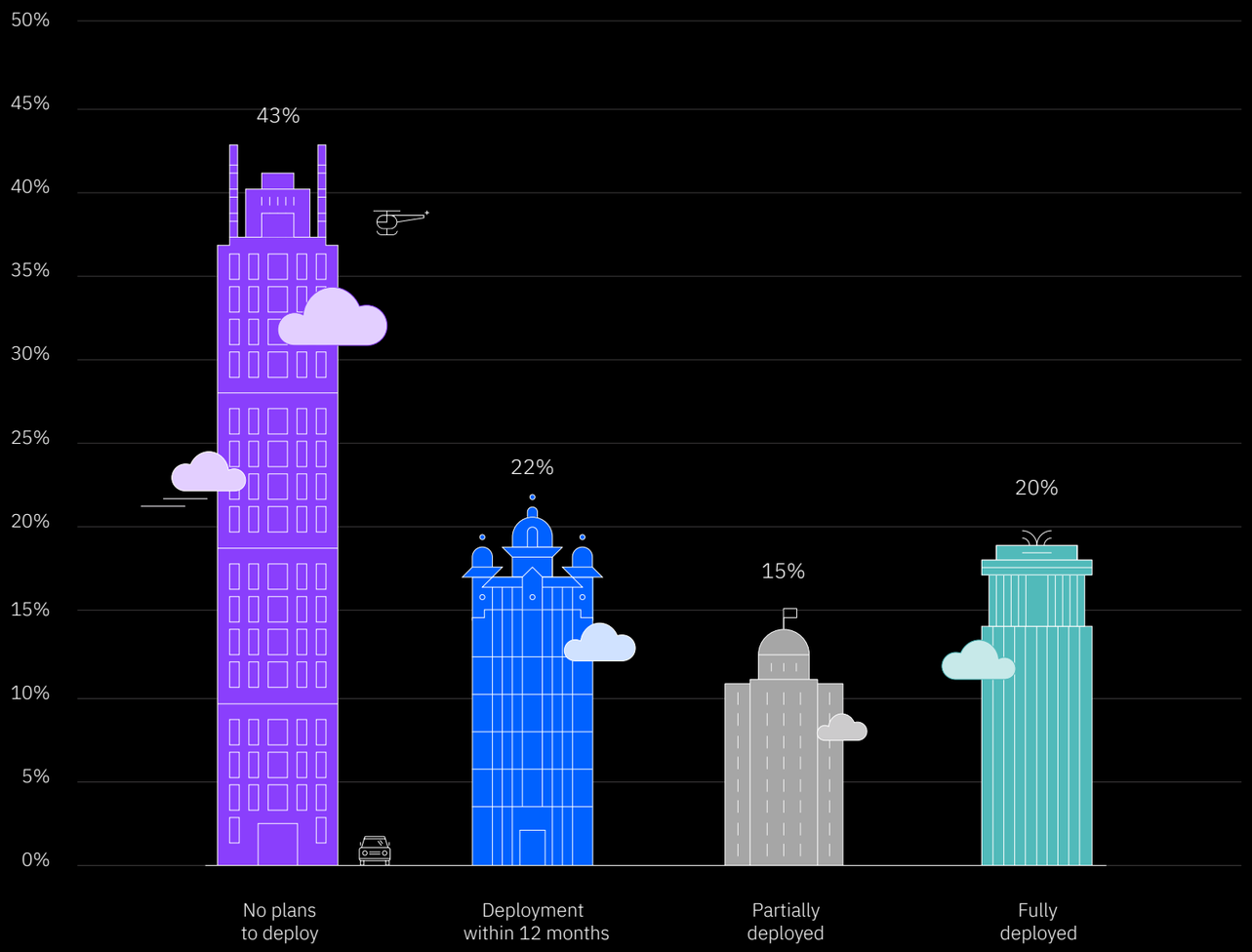
While 65% of respondents do not have zero trust deployed, 35% have a partially or fully deployed zero trust approach.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 16

State of zero trust deployment

Percentage of organizations per deployment category



Close to half of organizations have no plans in place to deploy zero trust.

Just 20% are fully deployed and 15% are partially deployed. While 22% say they plan to deploy zero trust in the next 12 months, 43% say they have no current plans to deploy zero trust.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

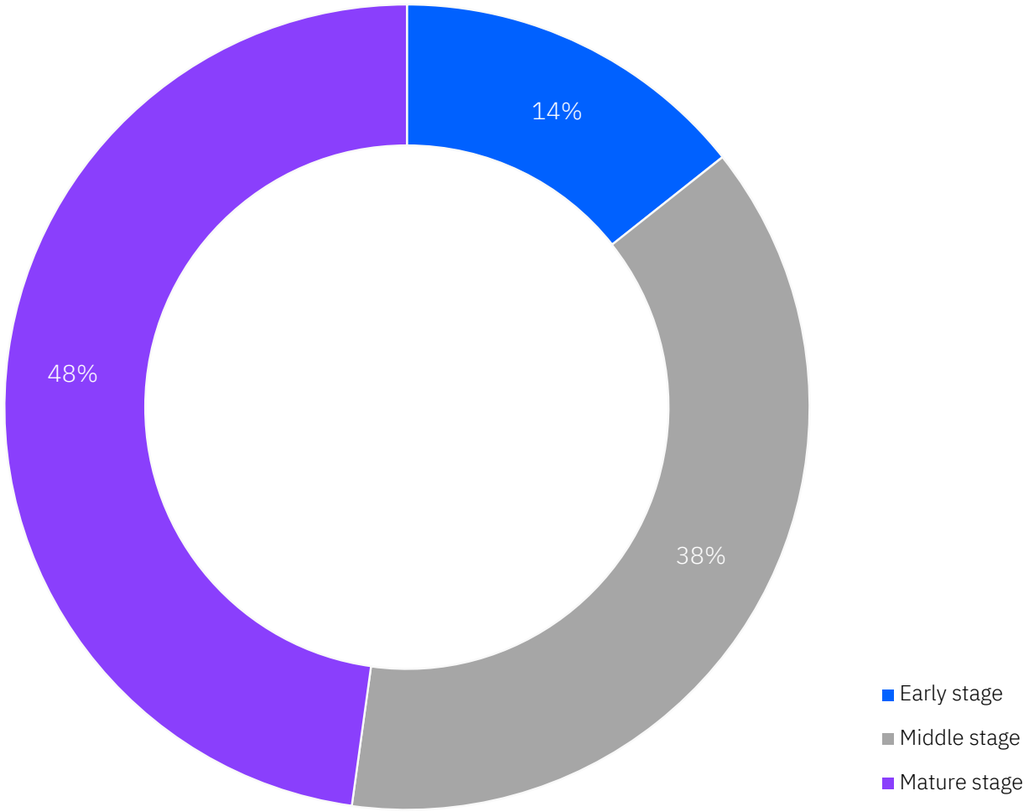
About IBM Security and the Ponemon Institute

Take the next steps

Figure 17

Zero trust maturity level

Percentage of organizations per maturity stage



Those who have deployed zero trust tend to be in the middle or mature stages of deployment.

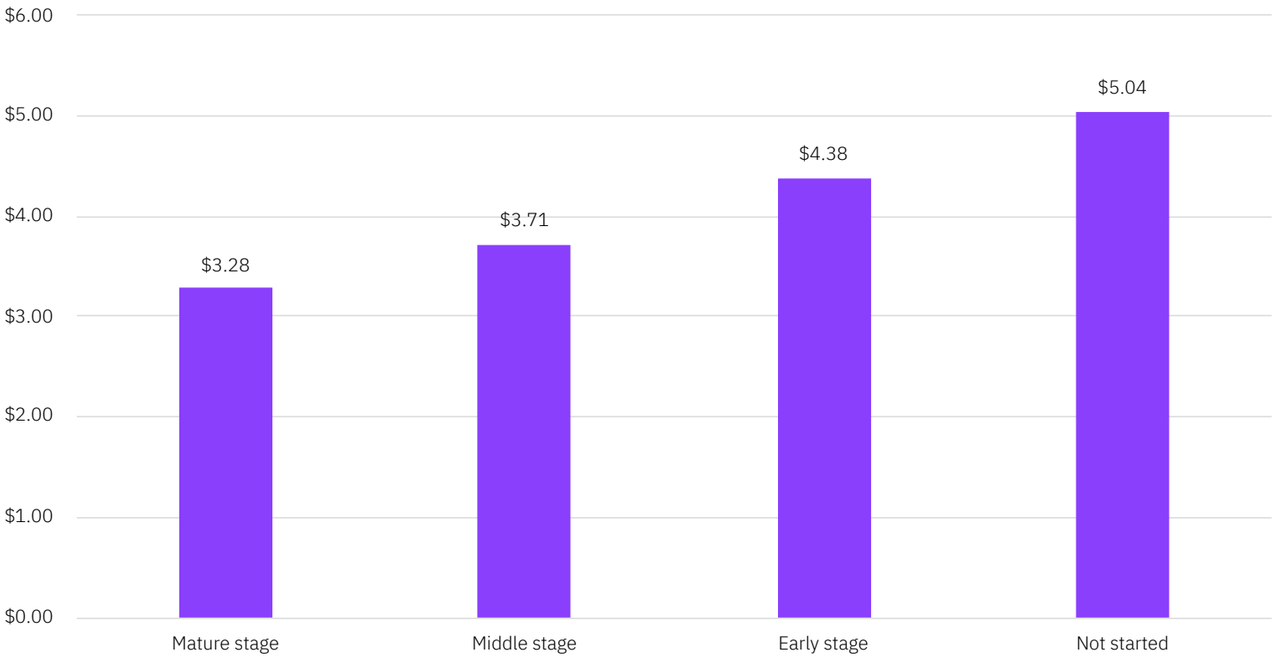
Of respondents that have fully or partially or fully deployed zero trust, 14% are in early stage deployment, 38% middle stage and 48% mature stage. This means just 16.8% of organizations in the study have a mature stage zero trust approach (i.e., 48% of the 35% of respondents that have deployed zero trust).

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 18

Average total cost of a breach by the state of zero trust deployment

Measured in US$ millions



Costs stayed lower for organizations in the mature stage of zero trust.

The average cost of a data breach was higher for organizations that had not deployed/not started to deploy zero trust. Costs for those that had zero trust depend on level of maturity. The average cost of a breach was $5.04 million in 2021 for those with no zero trust approach.

In mature stage of deployment, the average cost of a breach was $3.28 million. This difference of $1.76 million between mature zero trust organizations and organizations without zero trust is a cost difference of 42.3%.
The difference between early stage zero trust (average cost of a breach $4.38 million) and mature stage ($3.28 million) was $1.10 million, for a cost difference of 28.7%.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

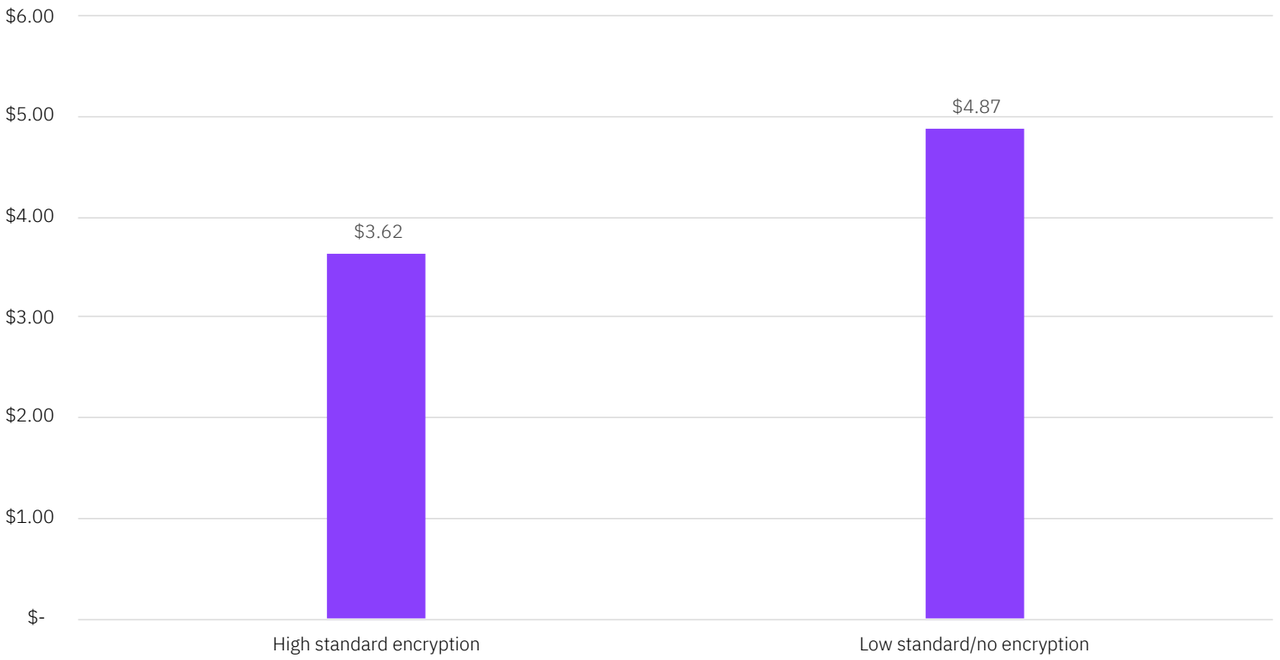
About IBM Security and the Ponemon Institute

Take the next steps

Figure 19

Impact of encryption on average cost of a data breach

Measured in US$ millions



Use of strong encryption, a key component of zero trust, was a top mitigating cost factor.

In an analysis of 25 cost factors that either amplified or mitigated the average total cost of a data breach, use of high standard encryption was third among cost mitigating factors, after mature use of AI platforms and mature use of analytics.

Organizations using high standard encryption (using at least 256 AES encryption, at rest and in motion), had an average total cost of a breach of $3.62 million, compared to $4.87 million at organizations using low standard or no encryption, a difference of $1.25M or 29.4%.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Security AI and automation

This was the fourth 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 incidents and intrusion attempts. Such technologies depend upon artificial intelligence, machine learning, analytics and automated security orchestration.

On the opposite end of the spectrum are processes driven by manual inputs, often across dozens of tools and complex, non-integrated systems, without data shared between them. On average, organizations in the study had 34 security tools.

Key finding

$2.90m

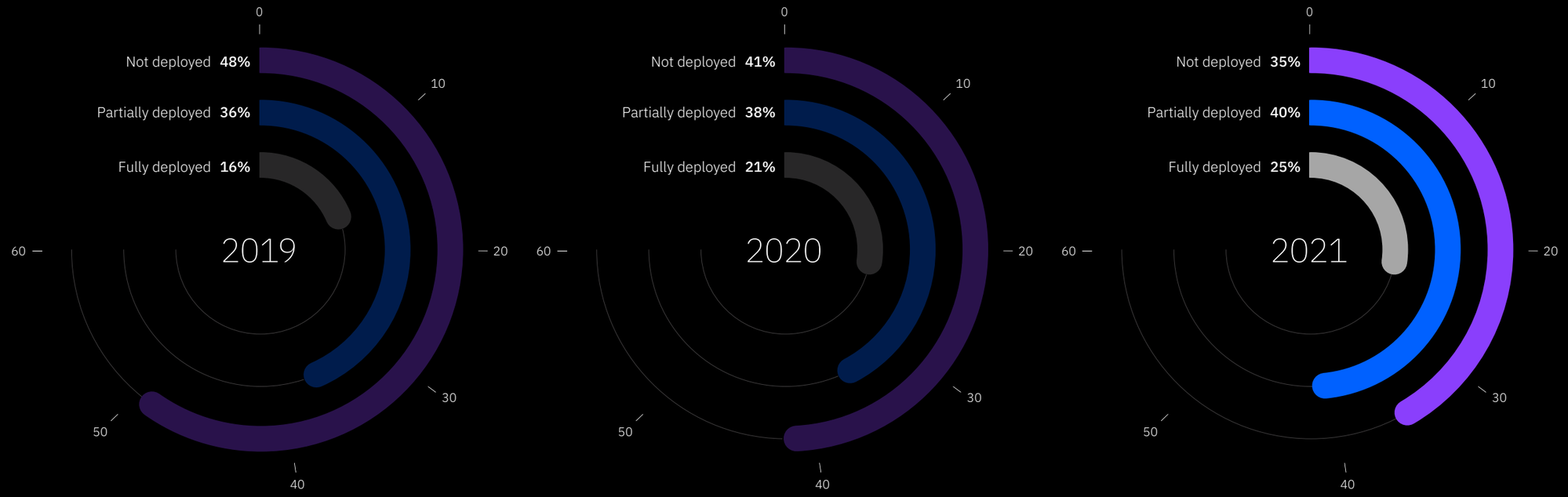
Average cost of a data breach at organizations with security AI and automation fully deployed

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 20

State of security AI and automation comparing three levels of deployment

Percentage of organizations per deployment level



The share of organizations with fully or partially deployed security automation increased by six percentage points.

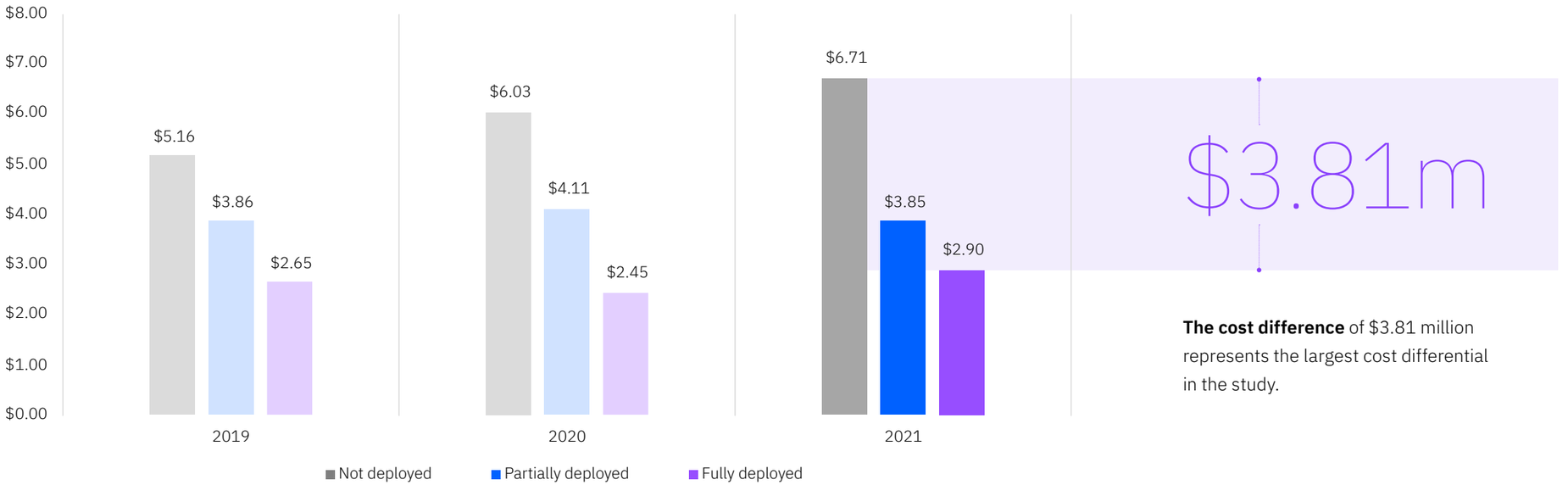
In 2021, 25% of respondents had fully deployed security automation, vs. 40% partially deployed and 35% not deployed. In 2020, 21% of respondents had fully deployed security automation, vs. 38% partially deployed and 41% not deployed. The share of organizations with fully or partially deployed security automation was 65% in 2021 vs. 59% in 2020. This represents a six percentage point increase in organizations with either fully or partially deployed automation from 2020 to 2021, and a decrease of 6 percentage points in the share of organizations with no security automation deployed.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 21

Average cost of a data breach by security automation deployment level

Measured in US$ millions



The cost difference of $3.81 million represents the largest cost differential in the study.

The biggest cost savings in the study was to organizations with high levels of security AI and automation.

Organizations with no security automation experienced breach costs of $6.71 million on average in 2021, vs. $2.90 million on average at organizations with fully deployed security automation.

In 2020, organizations without security AI/automation saw breach costs of $6.03M, vs. $2.45M with fully deployed security automation, a difference of $3.58 million, or 84.4%. Between 2019 and 2021, the cost of a breach at organizations with fully deployed security automation increased.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

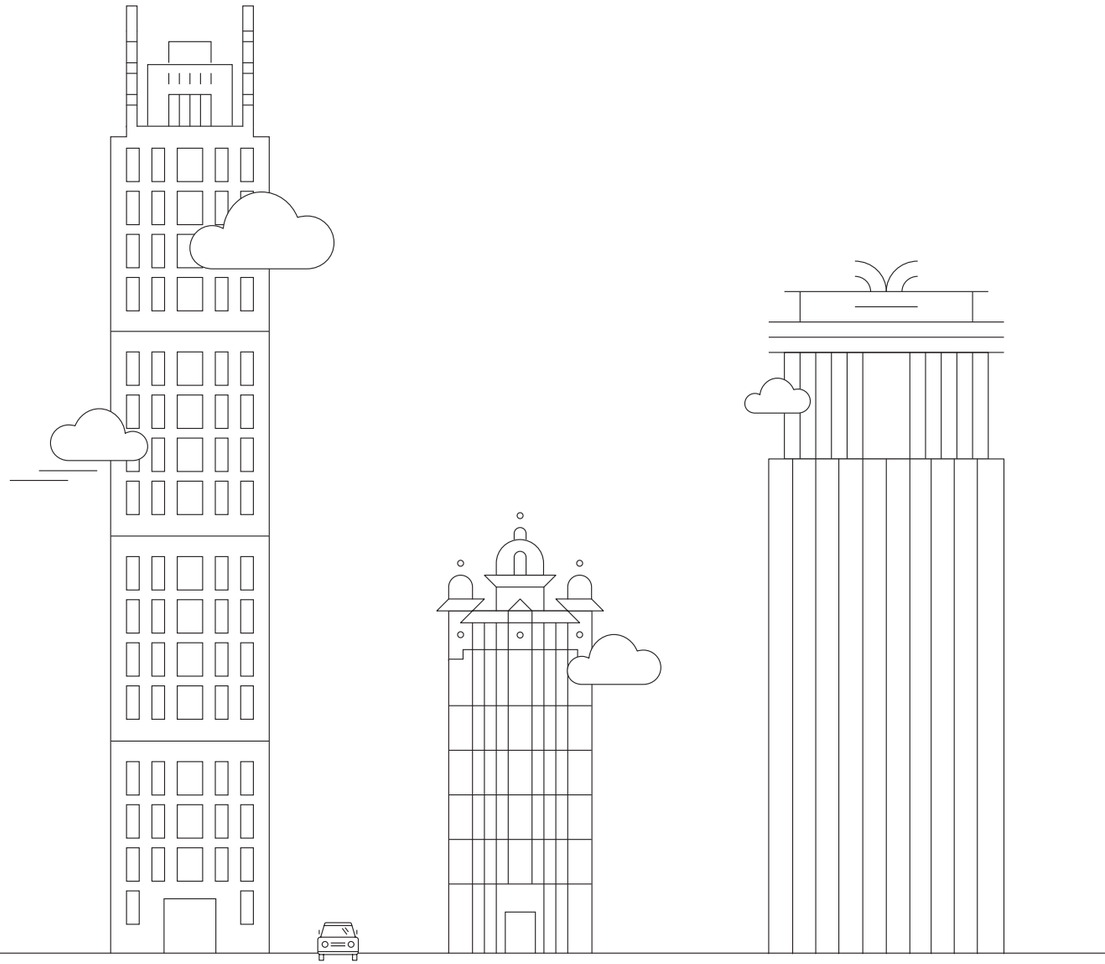
Organizations with fully deployed security AI and automation were able to detect and contain a breach must more quickly than organizations with no security AI/automation deployed.

For organizations with fully deployed security AI/automation, it took an average of 184 days to identify the breach and 63 days to contain the breach, for a total lifecycle of 247 days.

For organizations with no security AI/automation deployed, it took an average of 239 days to identify the breach and 85 days to contain, for a total lifecycle of 324 days. The difference in breach lifecycle of 77 days represents a difference of 27%. For fully deployed organizations, a breach occurring on January 1 would on average take until September 4 to identify and contain.

For organizations with no automation deployed, a breach on January 1 would take on average until November 20 to identify and contain.

See figure 22 on page 39 →

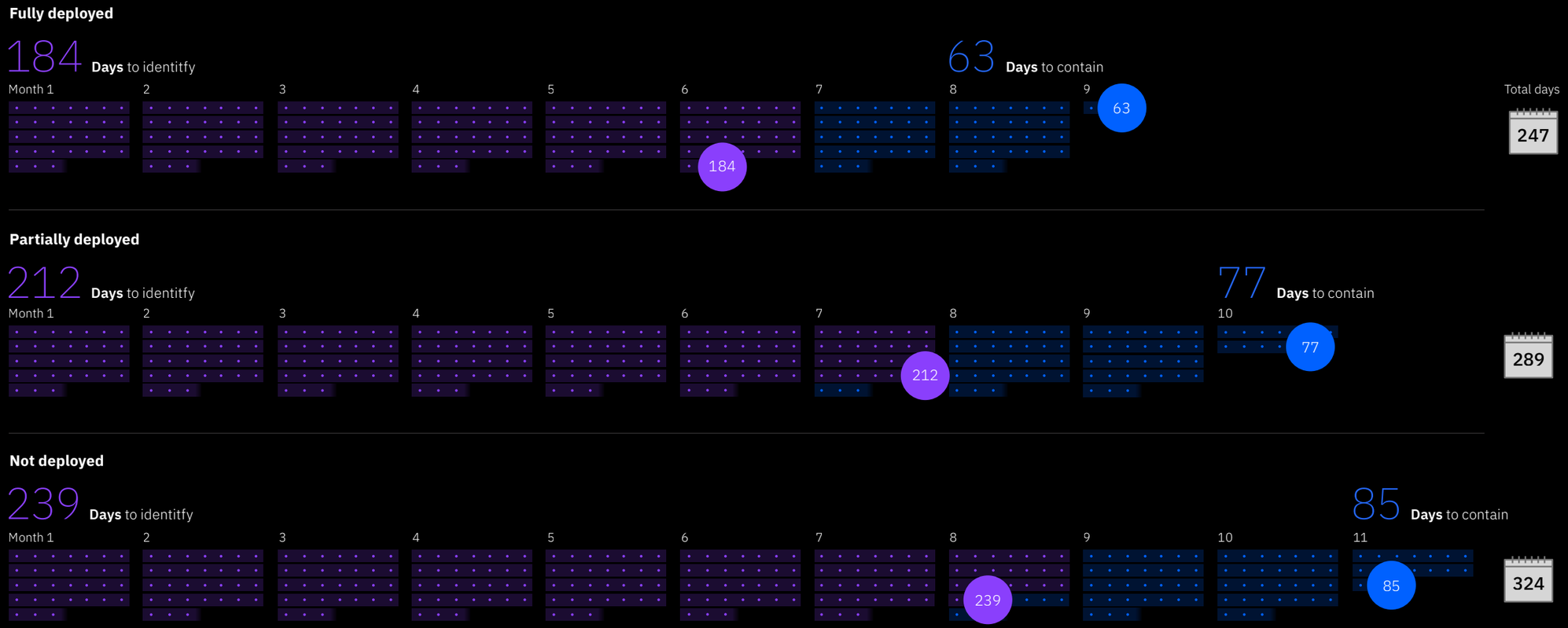


Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 22

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

Measured in days



Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

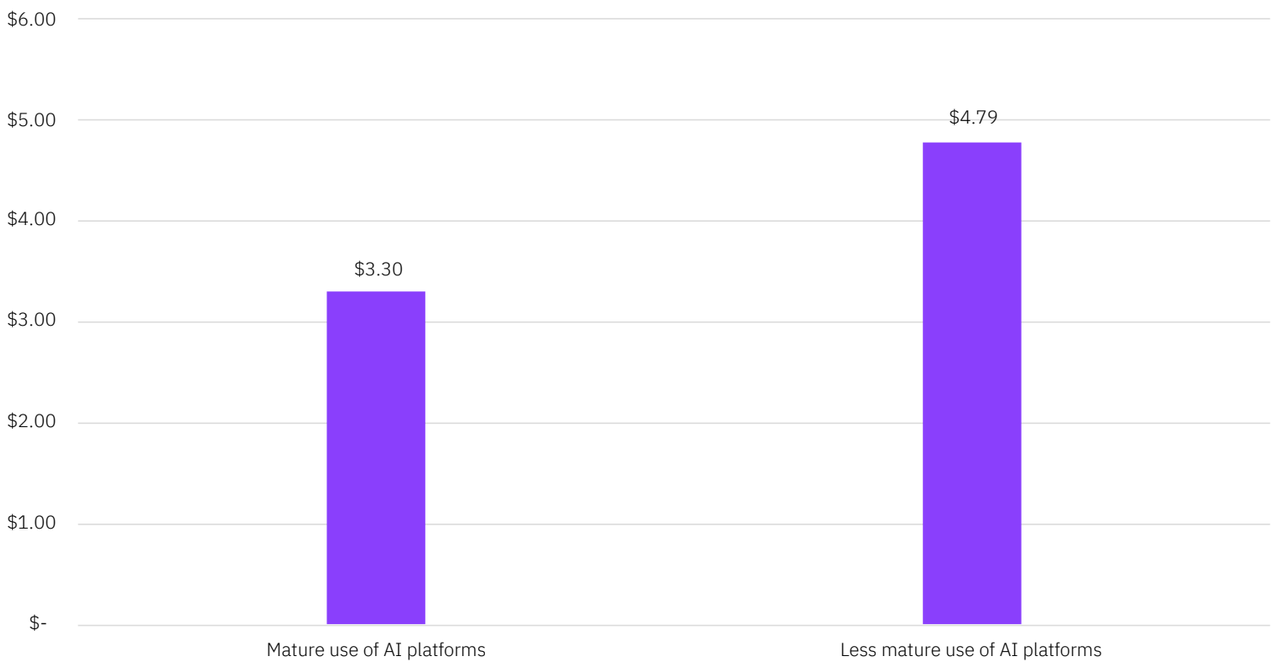
About IBM Security and the Ponemon Institute

Take the next steps

Figure 23

Impact of AI platforms on average cost of a data breach

Measured in US$ millions



Organizations with a mature use of AI platforms had a significantly lower average cost.

The average total cost of a data breach was $3.30 million at organizations with a more mature use of AI platforms (e.g., machine learning projects that cut across multiple tools).

At organizations with less mature use of AI platforms (e.g., just one application using machine learning), he average total cost was $1.49 million higher, a cost difference of 36.8%.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

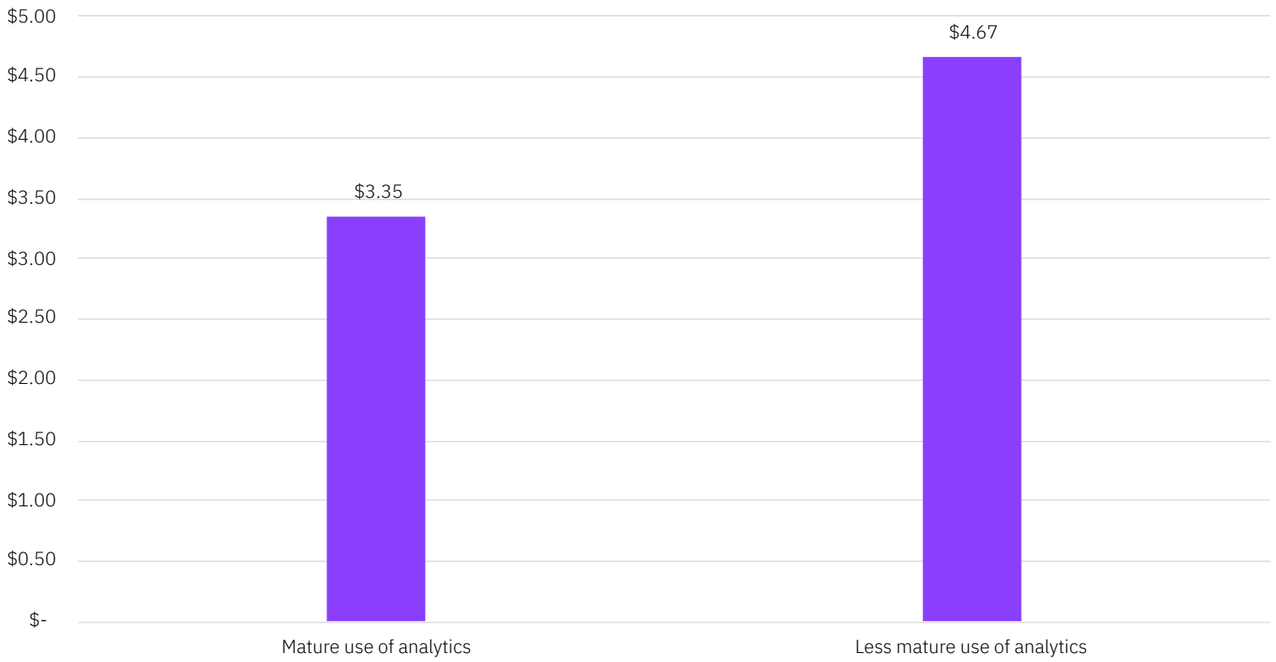
About IBM Security and the Ponemon Institute

Take the next steps

Figure 24

Impact of security analytics on average cost of a data breach

Measured in US$ millions



Mature use of analytics was associated with lower breach costs.

Organizations with a mature use of analytics had an average total cost of a breach of $3.35 million, compared to $4.67 million at organizations with a less mature use of analytics, a difference of $1.32 million or 32.9%.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

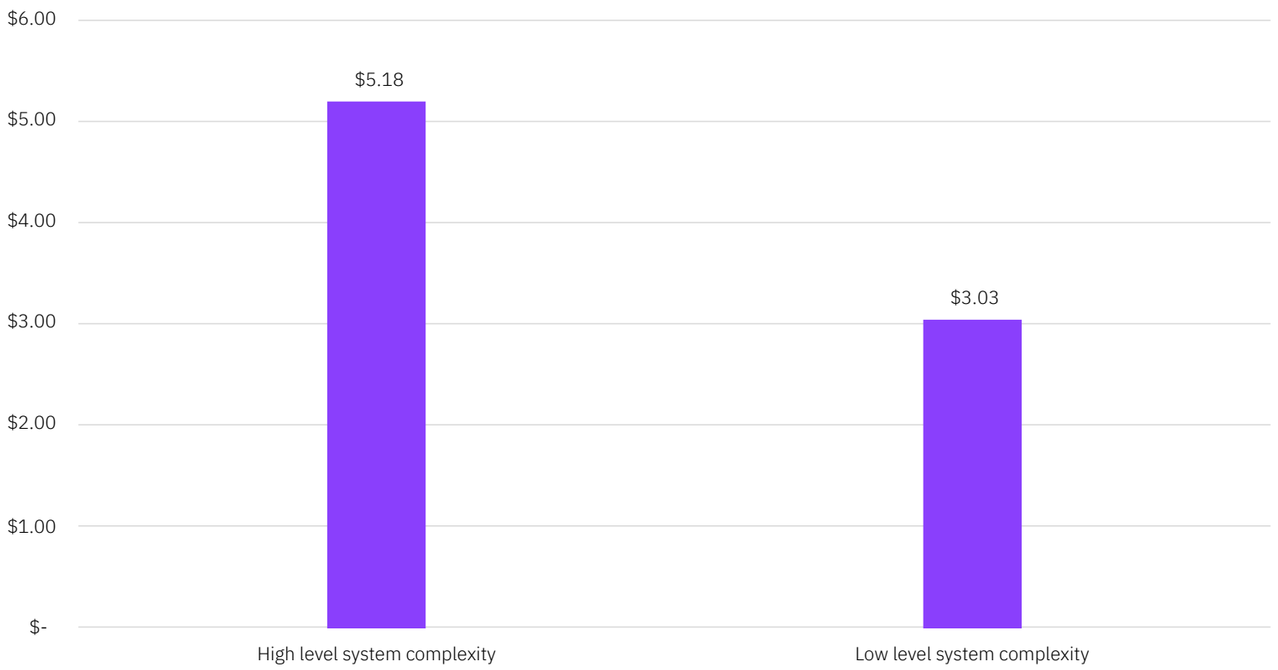
About IBM Security and the Ponemon Institute

Take the next steps

Figure 25

Impact of system complexity on average cost of a data breach

Measured in US$ millions



System complexity was associated with higher breach costs.

Organizations with a high level of system complexity (e.g., a higher number of tools, systems, devices, data and users) had an average cost of a breach of $5.18 million, compared to $3.03 million at organizations with low levels of system complexity, for a difference of $2.15 million or 52.4%.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Cloud breaches and migration

This was the first year we took an extensive look at the effects of breaches in the cloud and the cost impact of cloud migration.

Key finding

252 days

Average time to identify and contain a breach at organizations in mature stage of cloud modernization

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

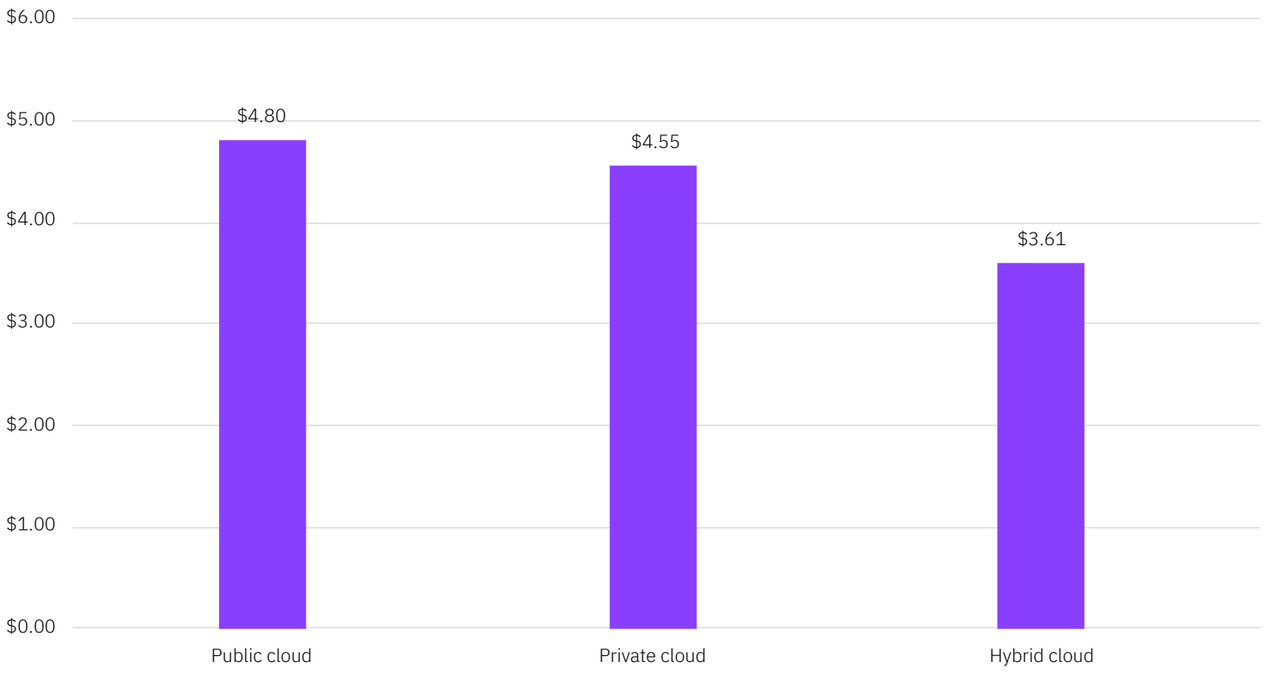
About IBM Security and the Ponemon Institute

Take the next steps

Figure 26

Average total cost of a cloud-based breach by cloud model

Measured in US$ millions



The hybrid cloud model had the lowest average total cost of a data breach.

Public cloud breaches cost an average of $4.80 million compared to $4.55 million for breaches in private clouds, and $3.61 million for hybrid cloud breaches. Hybrid cloud breaches cost an average of $1.19 million less than public cloud breaches, or a difference in cost of 28.3%.

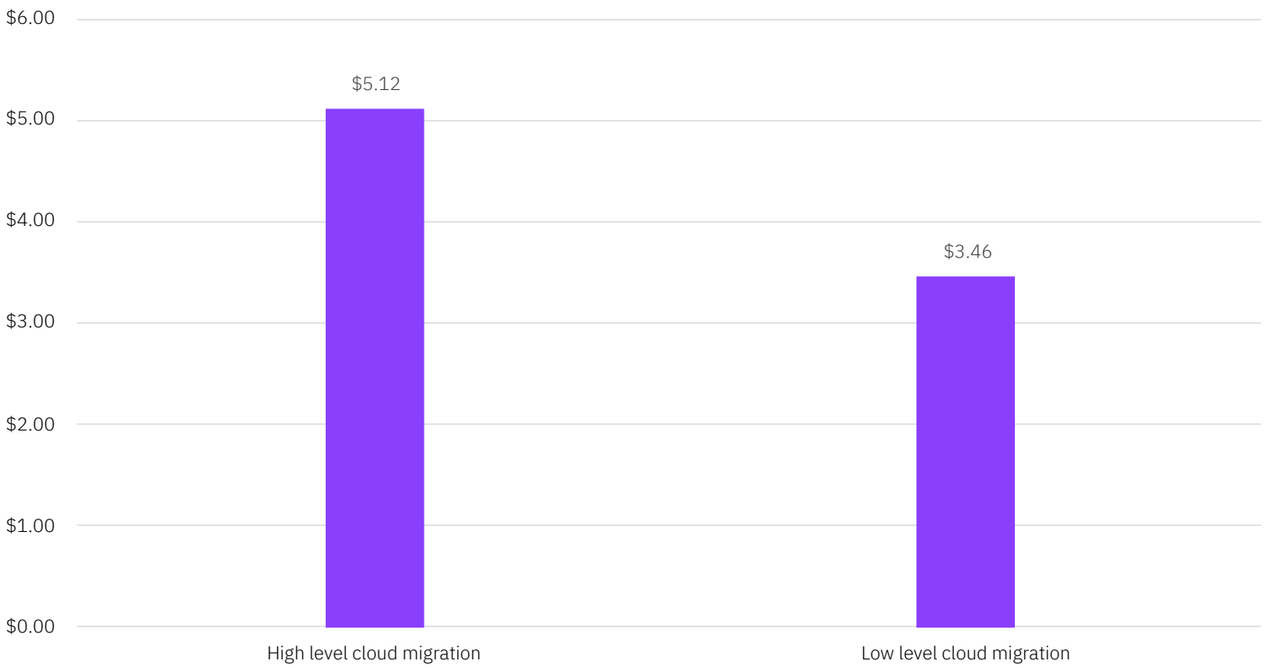
Public cloud = at least 80% conforming to the public cloud environment and no more than 20% conforming to hybrid cloud. Private cloud = at least 80% conforming to the private cloud environment and no more than 20% conforming to hybrid cloud.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 27

Impact of cloud migration on average cost of a data breach

Measured in US$ millions



Extensive cloud migration was the third highest cost amplifying factor in a study of 25 cost factors.

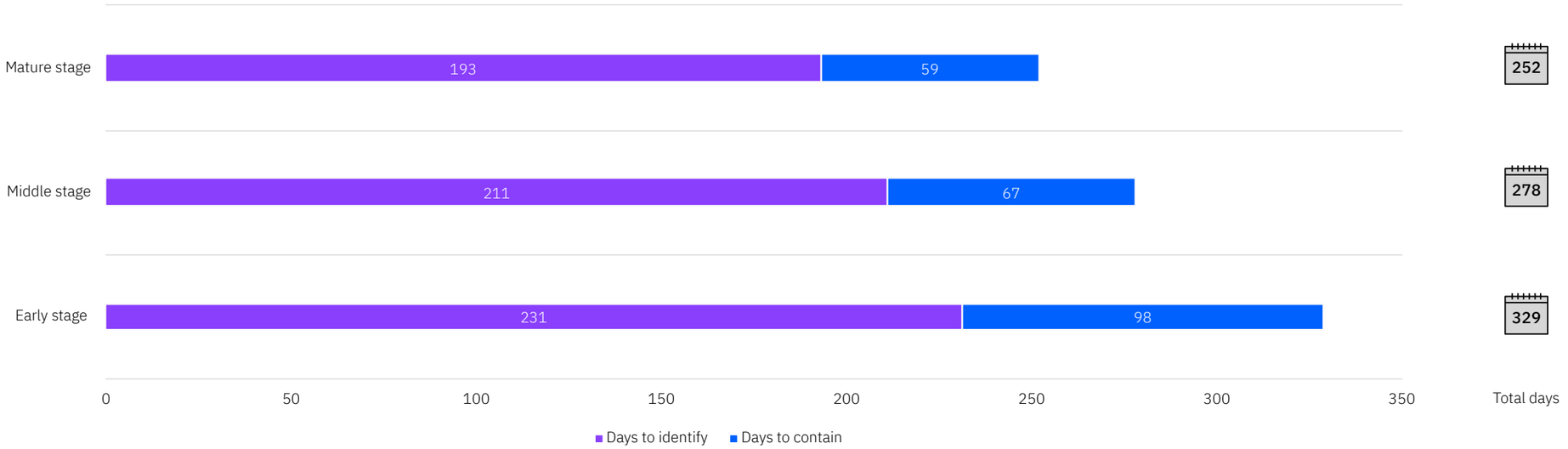
Organizations with a high level of cloud migration had an average cost of a breach of $5.12 million, compared to $3.46 million for organizations with low levels of cloud migration, for a difference of $1.66 million or 38.7%.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 28

Days to identify and contain a cloud-based data breach by cloud modernization stage

Measured in days



Cloud-based data breaches took longer on average to identify and contain among organizations in early stages of their overall cloud modernization journey, compared to those in middle and mature stages.

It took organizations an average of 231 days to identify and 98 days to contain a cloud-based breach in the early stage of cloud modernization (329 days total), compared to 193 days to identify and 59 days to contain a cloud breach in the mature stage of cloud modernization (252 days total). In the early stage of cloud modernization, it took an average of 42 days longer to identify and contain a breach than the global average time to identify and contain a breach (329 days vs. 287 days).

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

COVID-19 and remote work

This is the second year of this report that has been published during the pandemic. Last year, the pandemic began after most of the breaches in the study had already happened, so we re-surveyed organizations to get their predictions about how remote working due to COVID-19 would impact breach costs and the breach lifecycle. For this year's report we were able to assess the impacts of remote working on breaches that all occurred during the pandemic.

Key finding

$5.54m

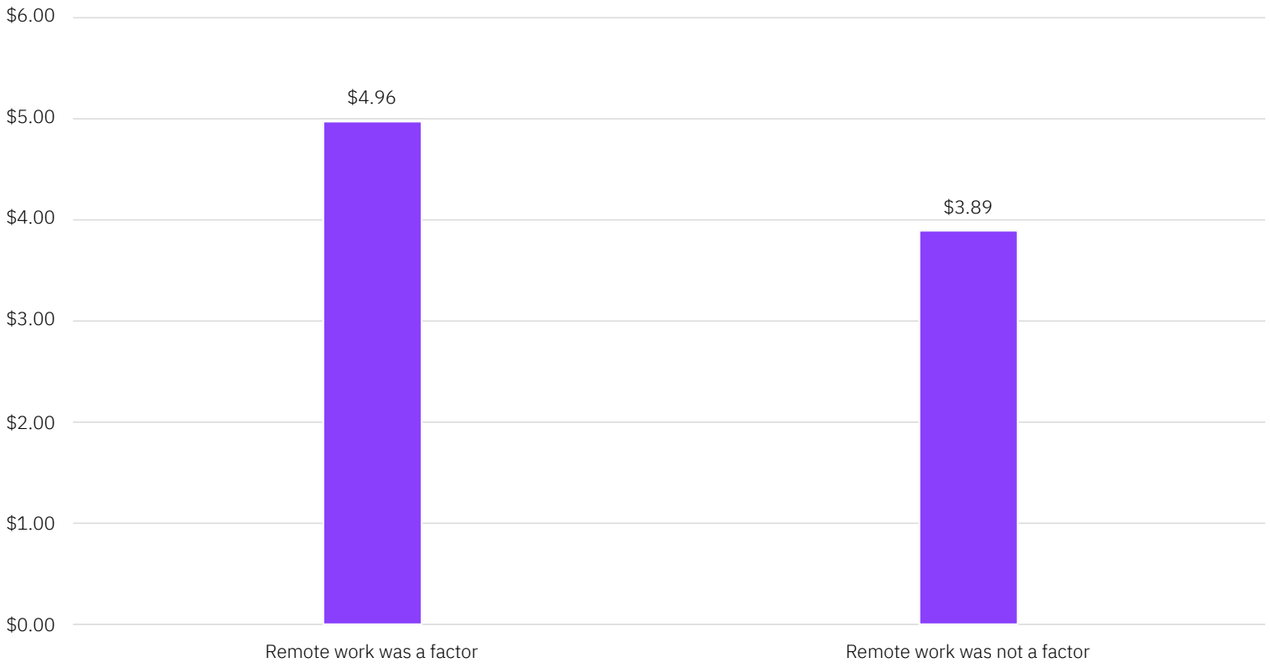
Average cost of a breach at organizations with 81-100% of employees working remotely

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 29

Average cost of a data breach where remote work was a factor

Measured in US$ millions



The average total cost of a data breach was more than $1 million higher where remote working was a factor in causing the breach compared to breaches where remote working was not a factor.

At organizations where remote work was a factor in the breach, the average total cost of a data breach was $4.96 million. When remote work was not a factor in causing the breach, the average total cost was $3.89 million. The difference in cost between breaches where remote work was a factor and where remote work was not a factor in the breach was $1.07 million, or 24.2%.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 30

Average cost of a breach based on share of employees working remotely

Measured in US$ millions

Organizations where more than 60% of employees were working remotely, had an average cost of a data breach that was higher than the overall average cost of a breach.

For organizations with 61-80% of employees working remotely, the average cost was $4.39 million, or $0.15 million more than the overall average of $4.24 million. At organizations with 81-100% of employees working remotely, the average cost of a data breach was $5.54 million, or $1.30 million more than the overall average of $4.24 million, a cost difference of 26.6%.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 31

Average cost of a data breach based on level of digital transformation due to COVID-19

Measured in US$ millions

The cost of a breach was higher than average at organizations that had not undergone a digital transformation due to COVID-19.

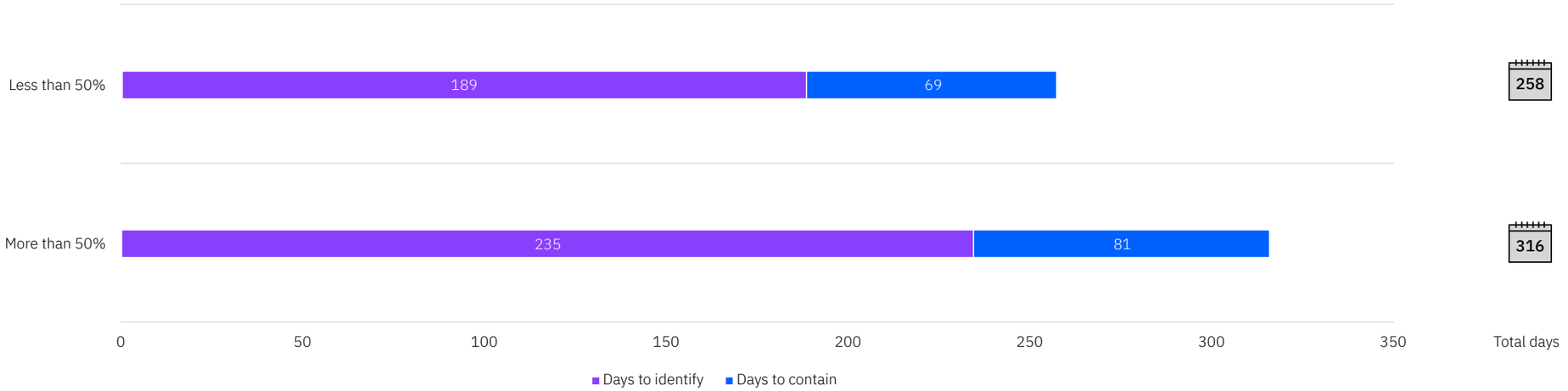
When organizations made no effort at digital transformation (i.e., adapted their IT to cope with the pandemic) the average cost of a breach was $5.01 million, or $0.77 million more than the global overall average of $4.24 million.

Executive summary
Complete findings
Global findings and highlights
Initial attack vectors
Lifecycle of a breach
Regulatory compliance failures
Impact of zero trust
Security AI and automation
Cloud breaches and migration
COVID-19 and remote work
Cost of a mega breach
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 32

Average time to identify and contain a breach based on level of remote work adoption

Measured in days



Organizations that had implemented remote work at greater than a 50% level experienced a longer than average time to identify and contain a data breach.

At organizations where remote work was at greater than 50% adoption, it took an average of 235 days to identify and 81 days to contain a breach (316 days total), compared to the overall average of 212 days to identify and 75 days to contain (287 days total), for a difference of 9.6%. With less than 50% remote work adoption, a data breach took an average of 189 days to identify and 69 days to contain (258 days total), a difference of 10.6%.

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Cost of a mega breach

Mega breaches, those with more than 1 million compromised records, 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 14 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 finding

$401m

Average total cost for breaches of 50 million to 65 million records

Executive summary

Complete findings

Global findings and highlights

Initial attack vectors

Lifecycle of a breach

Regulatory compliance failures

Impact of zero trust

Security AI and automation

Cloud breaches and migration

COVID-19 and remote work

Cost of a mega breach

Risk quantification

Security recommendations

Organization characteristics

Research methodology

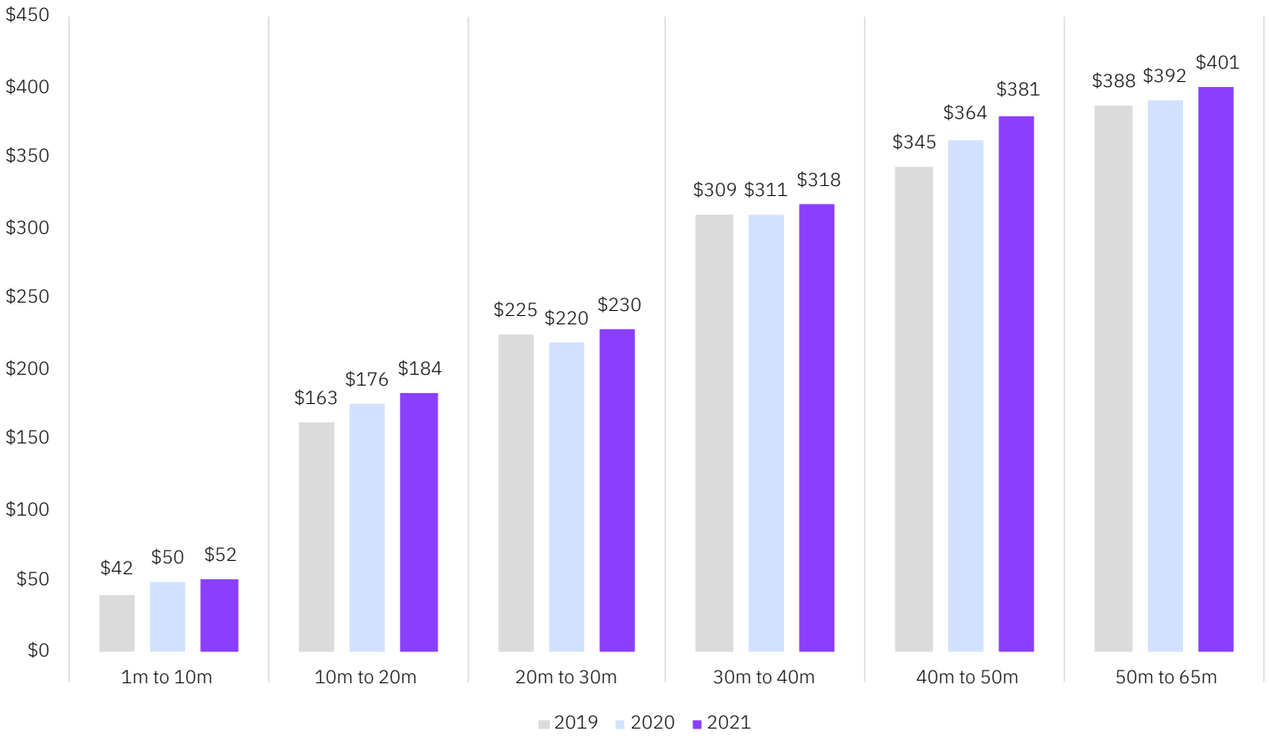
About IBM Security and the Ponemon Institute

Take the next steps

Figure 33

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

Measured in US$ millions



The average cost of a mega breach was $401 million for the largest breaches (50 million to 65 million records), an increase from $392 million in 2020.

This represents an increase of 2.3%. The cost increased across all subsets of the mega breaches (1 million up to 65 million records). The largest cost increase was in the 40 million to 50 million records range, from $364 million in 2020 to $381 million in 2021, an increase of 4.7%. In the range of 1 million to 10 million records, costs increased 4% year over year and have increase by 23.8% since the 2019 report.

Executive summary
Complete findings
Risk quantification
Financial services scenario
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Quantifying security risk

Security is a business problem. Board executives and business leaders want to know the likelihood of a cyber incident occurring and the impact to the company's ability to produce and sell its products or services as well as the potential impact to the brand.

Risk quantification can help organizations identify and prioritize security risk to inform decisions such as deploying new technologies, making investments in their business, and changing processes. CISOs, risk managers and security teams can use benchmark research like the Cost of a Data Breach Report to infer general trends and cost averages in their industry or geography.

However, using data specific to the organization, rather than industry averages, organizations can get clarity and understanding on potential security gaps and how to reduce overall risk by quantifying security risk into financial terms.

Below we explain how the Factor Analysis of Information Risk (FAIR), an open international standard for cyber risk modeling, combined with threat intelligence, can help organizations assess the potential impacts of cyber risks through financial projections and probabilities.

Executive summary
Complete findings
Risk quantification
Financial services scenario
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Case study

How IBM Security uses FAIR in risk modeling

To quantify risk specific to your organization, IBM Security uses the FAIR model to estimate the probability of a data breach and size of the breach in financial terms. We look at variables such as frequency of breach events, vulnerabilities and strength of security.

We then use threat intelligence from IBM Security X-Force to assess the capability of the threat actor and their probability to attack.

We take these variables through statistical analysis using Monte Carlo Simulations to estimate the range of financial loss. Understanding these key variables allows an organization to identify gaps in current controls or processes that put them at risk for larger financial loss.

We can define the material impact of security gaps into components of primary and secondary loss; with primary loss being the loss associated with managing and responding to the event and secondary loss being the loss associated with outside parties such as regulatory bodies, customers and the stock market.

Once we understand the potential financial loss an organization faces, we can look at cost-benefit and ROI analysis into possible investments around mitigating controls or processes. For example, improvements around security awareness training can help to reduce threat event frequency, or changes to the identity and access management program can help minimize the size of a breach.

Data from the IBM X-Force Threat Intelligence Index shows us that the banking and financial services industry is a highly targeted sector of business year after year. In this example, we look at a hypothetical loss event in financial services.

Executive summary
Complete findings
Risk quantification
Financial services scenario
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Scenario

Financial services sensitive data breach

This hypothetical scenario analyzes the risk associated with a malicious external actor gaining access to a sensitive database and using ransomware to halt operations and extort the organization by threatening to expose stolen data publicly.

In a real-world client engagement, our assumptions, which serve as data inputs for our analysis, are gathered via consultative workshops. In this scenario, we use financial industry averages and learnings from previous client engagements as inputs to run the statistical analysis.

Scope

Threat	Threat type	Method category	Asset	Loss effect
External actor(s)	Malicious	Ransomware	Database containing PII and PCI data	Loss of confidentiality

Assumptions

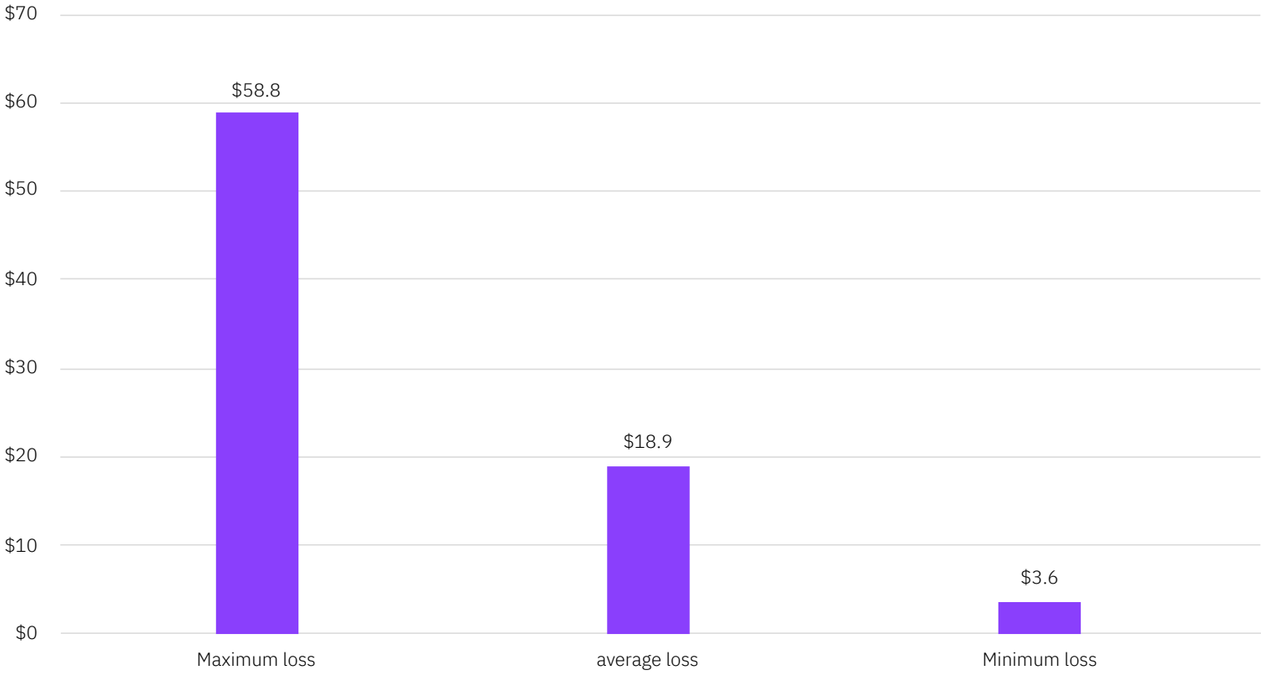
Threat event frequency	
2-4 times per year	Based on the current contact frequency, phishing and spam attempts and controls in place.
Vulnerability	
5% - 15%	Based on the strength of security controls and threat actor capability. The assumption is the controls are strong against this specific type of threat.
Direct loss	
Response time to manage the event - Person hours	
50 - 150 hours	Based on the size of the loss
Employee wages based on skill level needed to repair and restore	
$75 - $150 per hour	Based on skill level required for specific response
Secondary loss to customers	
Sensitive Records	
500,000 to 1M	Estimated database of sensitive records
75 - 100% PII/PCI	Estimated percentage that contain PCI or PII
10 - 25% IP	Estimated percentage that contain IP

Executive summary
Complete findings
Risk quantification
Financial services scenario
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 34

Range of financial loss

Measured in US$ millions



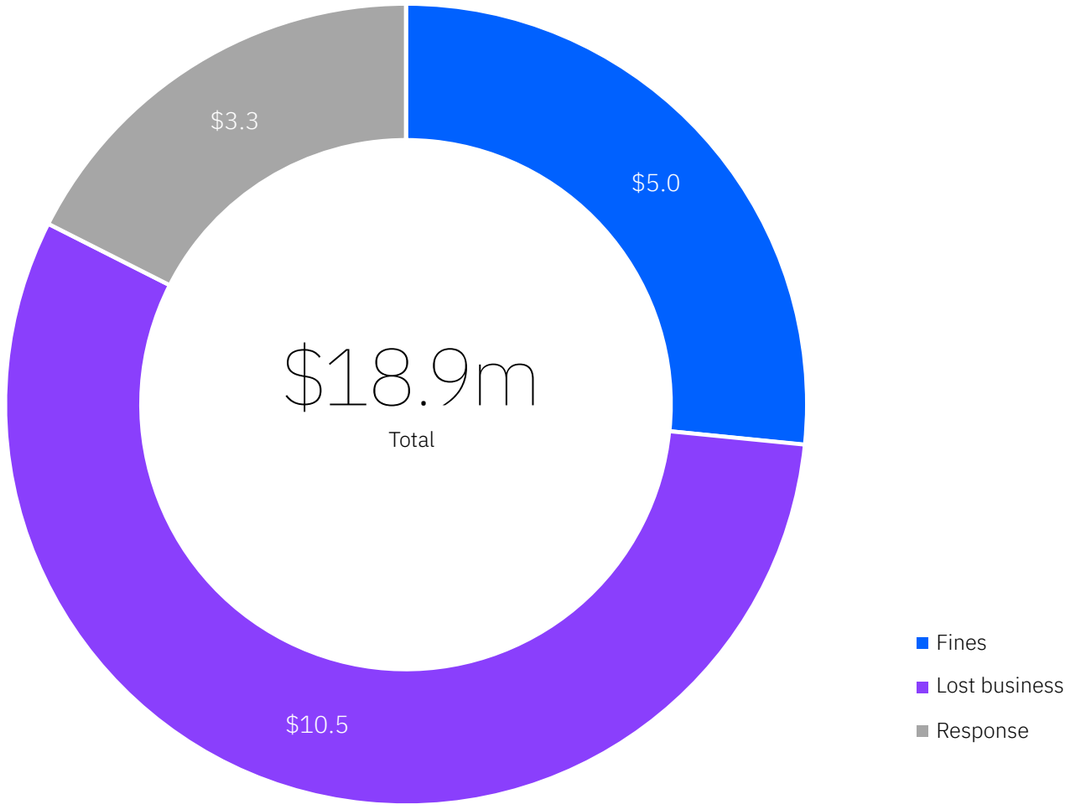
Quantifying the security risk of a specific bank being hit by ransomware, shows a 30% probability of the event occurring given that bank's strong security controls and an $18.9 million average financial loss that is composed of response costs, lost business and regulatory fines.

Executive summary
Complete findings
Risk quantification
Financial services scenario
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 35

Components of financial loss

Measured in US$ millions



Largest primary form of loss

Response costs

Largest secondary form of loss

Lost business

Most severe event

$18.9 million

Probability of loss exceeding $1 million

30%

Top annualized risk

$5.7 million

Executive summary

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Recommendations to help minimize financial impacts 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 AI and automation significantly reduced the average time to identify and respond to a data breach had a lower average cost. SOAR and SIEM software, and managed detection and response 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 just 35% of organizations had implemented a zero trust security approach. However, those in the mature stage of their zero trust deployment had an average breach cost that was $1.76 million less than organizations without zero trust. 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 saw an average total cost of a data breach that was $2.46 million less than organizations that experienced a breach without an IR team or a tested IR plan. The mantra “train like you fight and fight like you train” means developing and testing incident response playbooks to help optimize your ability to respond quickly and effectively to attacks.

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

In the study, organizations that had more than 60% of their employees working remotely in response to the COVID-19 pandemic had a higher than average 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.

Executive summary

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Invest in governance, risk management and compliance programs.

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. The FAIR risk quantification methodology can help ascertain the probability of security incidents and calculate the associated costs in business value. Quantifying the cost of a potential breach can help in the decision-making process for allocating resources.

Embrace an open security architecture and minimize the complexity of IT and security environments.

In this year's study, complexity of IT and security systems and extensive cloud migration were among the top factors contributing to higher average 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. A managed security services provider can also help simplify security and risk with continuous monitoring and integrated solutions and services.

Protect sensitive data in cloud environments using policy and encryption.

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 data encryption and fully homomorphic encryption. Use vulnerability scanning, penetration testing and red teaming to help identify cloud-hosted database vulnerability exposures and misconfigurations.

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

Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Geographic and industry samples
Industry definitions
Impact of organization size
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Organization characteristics

This section shows the breakdown of organizations in the study by geography and industry. It includes definitions used for classifying the organizations by industry, and data on the average cost of a data breach by organization size.

Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Geographic and industry samples
Industry definitions
Impact of organization size
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 36

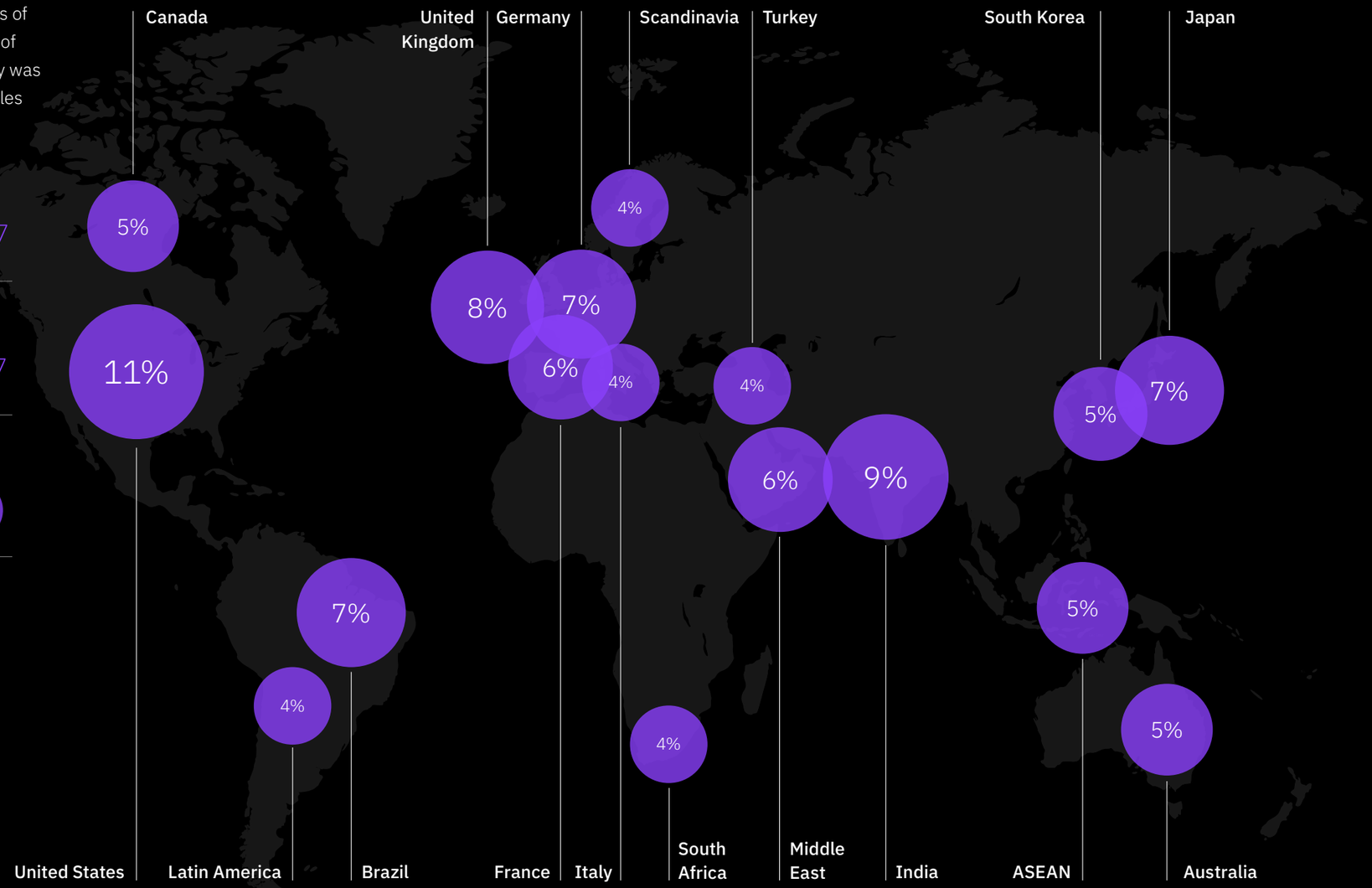
Distribution of the sample by geography

This year's study included 537 organizations of various sizes, sampled across a wide range of geographies and industries. The 2021 study was conducted in 17 countries or regional samples and 17 industries.

Countries 17

Organizations 537

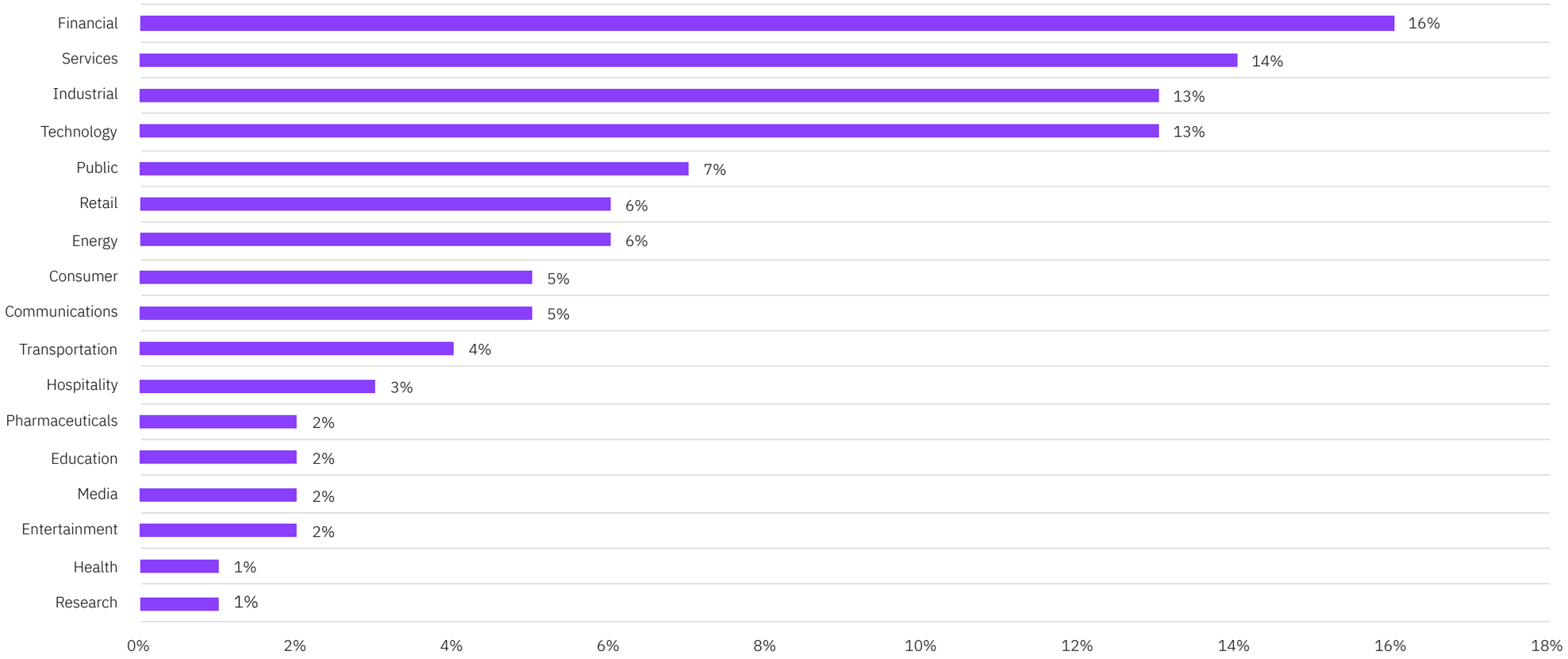
Contribution to study %



Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Geographic and industry samples
Industry definitions
Impact of organization size
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 37

Distribution of the sample by industry



Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Geographic and industry samples
Industry definitions
Impact of organization size
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Industry definitions

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

Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Geographic and industry samples
Industry definitions
Impact of organization size
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Impact of organization size

The Cost of a Data Breach report drew on 537 organizations across small, medium and large-sized organizations. In this analysis of the impact of organization size, we examined the cost by employee headcount, which is a proxy for size.

Key finding

$5.33m

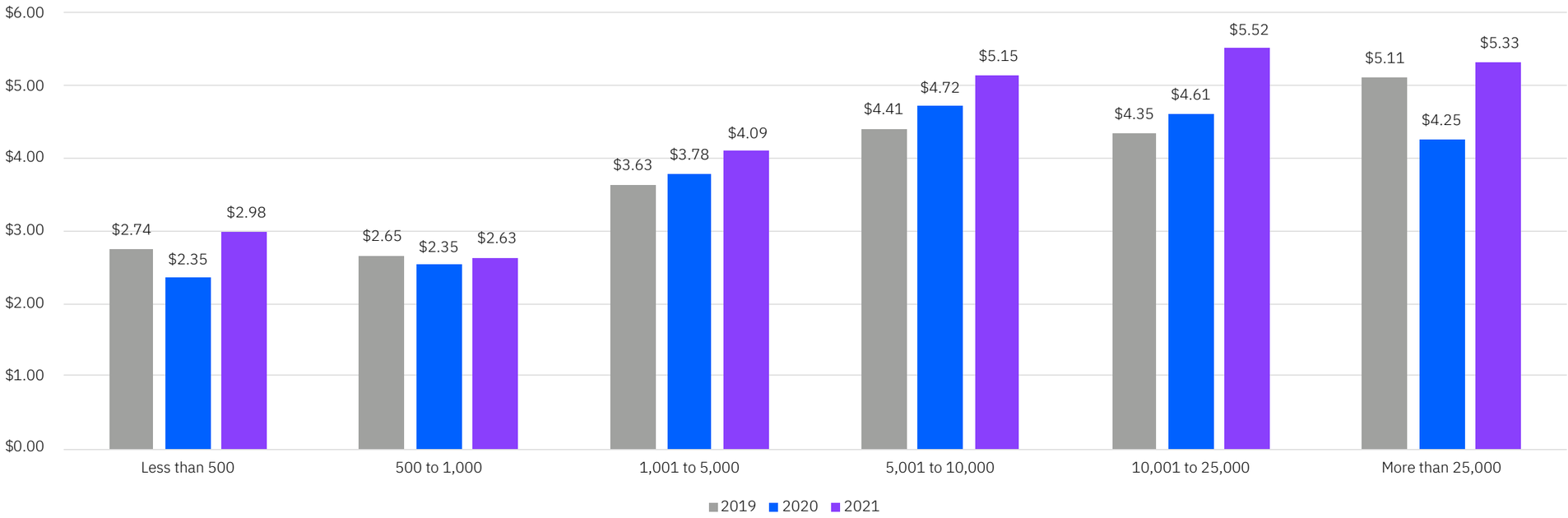
Average total cost of a breach at organizations with over 25,000 employees

Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Geographic and industry samples
Industry definitions
Impact of organization size
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

Figure 38

Average cost of a data breach by employee headcount

Measured in US$ millions



Bigger organizations had the biggest data breach costs.

By organizational size, the costliest size was 10,000-25,000 employees, at an average total cost of $5.52 million, followed by more than 25,000 employees at $5.33 million. Small businesses (less than 500 employees) saw an increase from 2.35 million in 2020 to $2.98 million in 2021, a 26.8% increase. The study represented organizations rather evenly across different sizes: 25% of organizations had less than 1,000 employees; 20% had from 1,001-5,000 employees; 22% had 5,001-10,000 employees; 15% had from 10,001-25,000 employees; and 18% had more than 25,000 employees.

Executive summary

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

Data breach FAQ

Research limitations

About IBM Security and the Ponemon Institute

Take the next steps

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.

Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Research methodology
Data breach FAQ
Research limitations
About IBM Security and the Ponemon Institute
Take the next steps

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 2,000 to 101,000 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 nearly 3,500 separate interviews with individuals at 537 organizations that suffered a data breach between May 2020 and March 2021. 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 537 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 14 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 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 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 65 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 4,477 organizations.

Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Research methodology
Data breach FAQ
Research limitations
About IBM Security and the Ponemon Institute
Take the next steps

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.

Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

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.

Ponemon INSTITUTE

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 Security 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 4.7 trillion events per month in more than 130 countries, IBM holds over 10,000 security patents. To learn more, visit ibm.com/security.

Contact us on Twitter at @IBMSecurity. Join the conversation in the IBM Security Community.

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

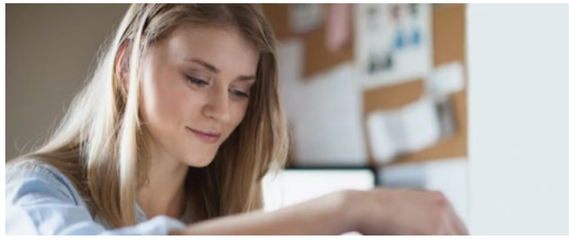
1.800.887.3118
research@ponemon.org

Executive summary
Complete findings
Risk quantification
Security recommendations
Organization characteristics
Research methodology
About IBM Security and the Ponemon Institute
Take the next steps

For more information, contact your IBM Business Partner:

Name
Phone Email
Website

Cybersecurity services
Reduce risk with consulting,
cloud and managed security services



Identity and access management
Connect every user, API and device
to every app securely

Data security
Discover, classify and protect
sensitive enterprise data

Security information and event management
Gain visibility to detect, investigate and respond
to threats

Executive summary

Complete findings

Risk quantification

Security recommendations

Organization characteristics

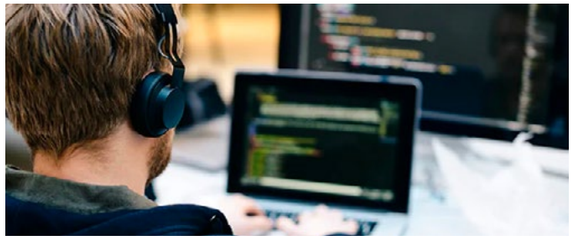
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Security orchestration, automation and response

Accelerate incident response with orchestration and automation



Cloud security

Integrate security into your journey to hybrid multicloud

Zero Trust

Wrap security around every user, device and connection

Executive summary

Complete findings

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

IBM Security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2021

IBM