IBM Security

Cost of a Data Breach Report 2021

IBM

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.

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

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.

- 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.

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.

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.

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

@8672 0 &5 3&5621 ! //< ,%&17,ñ ! #/& 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).

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.

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.

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%.

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.

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

@2 0 3/&7& ñ1%,1(6

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

@2 0 3/&7& ñ1%,1(6

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.

H&< ñ1%,1(

$4.24m

Global average total cost of a data breach

Executive summary

@2 0 3/&7& ñ1%,1(6

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

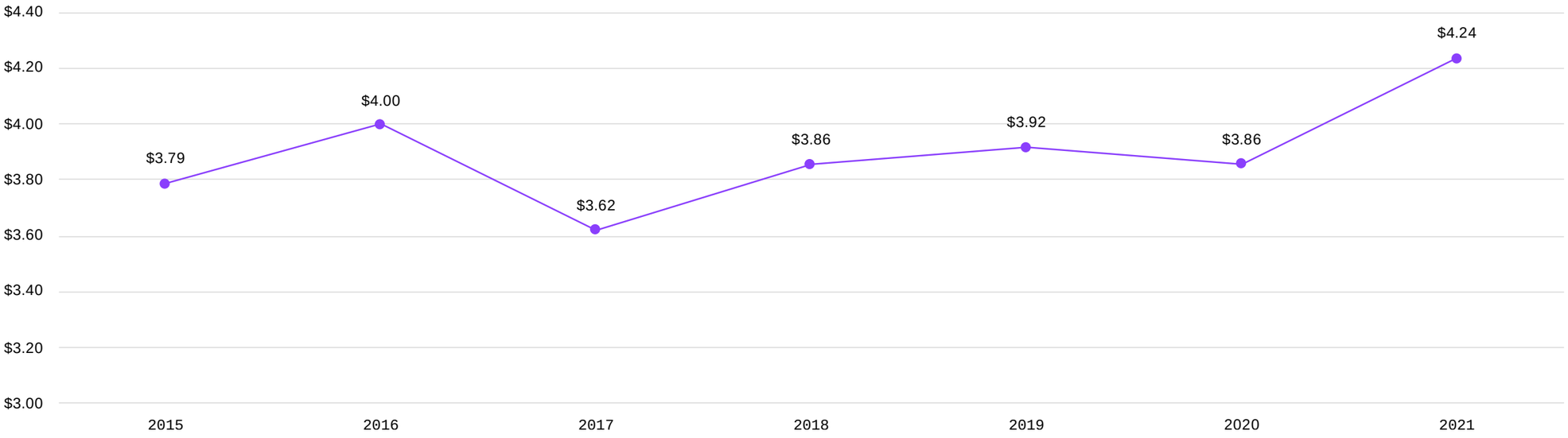
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Average total cost of a data breach

Measured in US$ millions



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

@2 0 3/&7& ñ1%,1(6

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

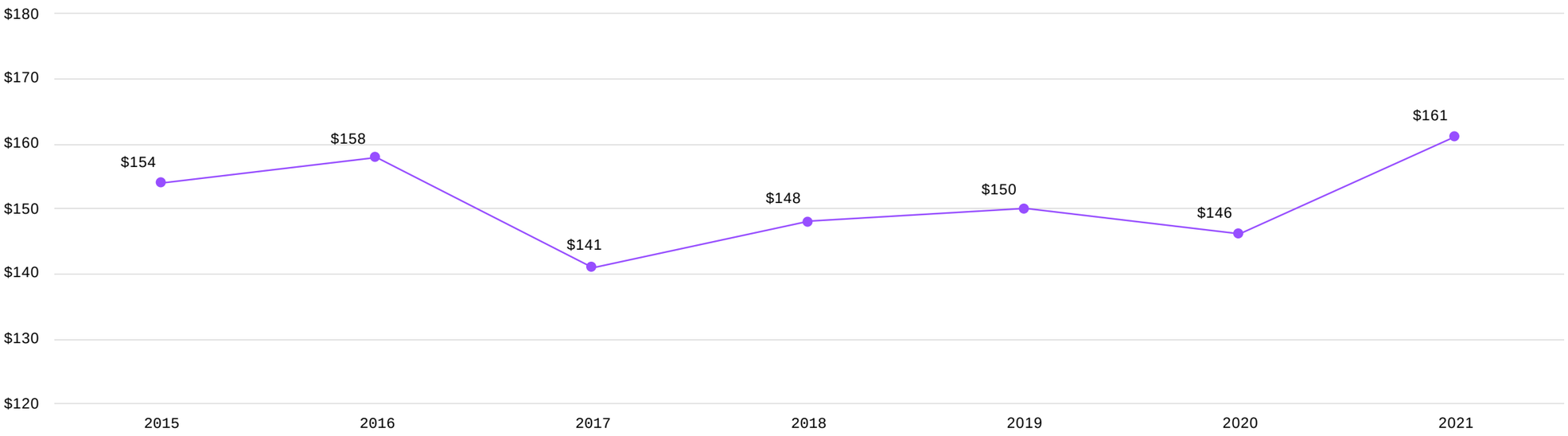
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Average per record cost of a data breach

Measured in US$



*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.

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.

Executive summary

Global findings and highlights

Risk quantification

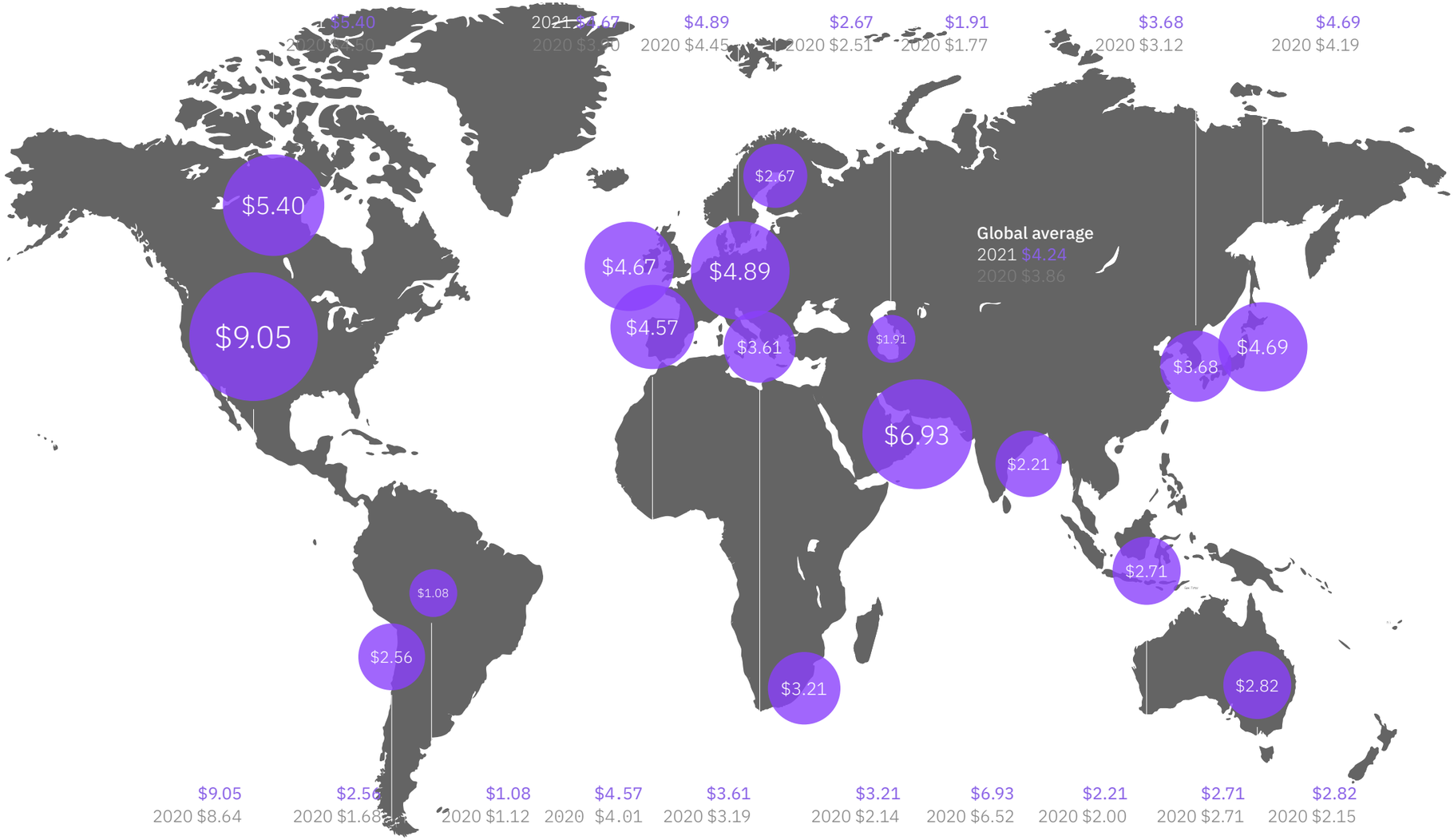
Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps



Executive summary

@2 0 3/&7& ñ1%,1(6

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

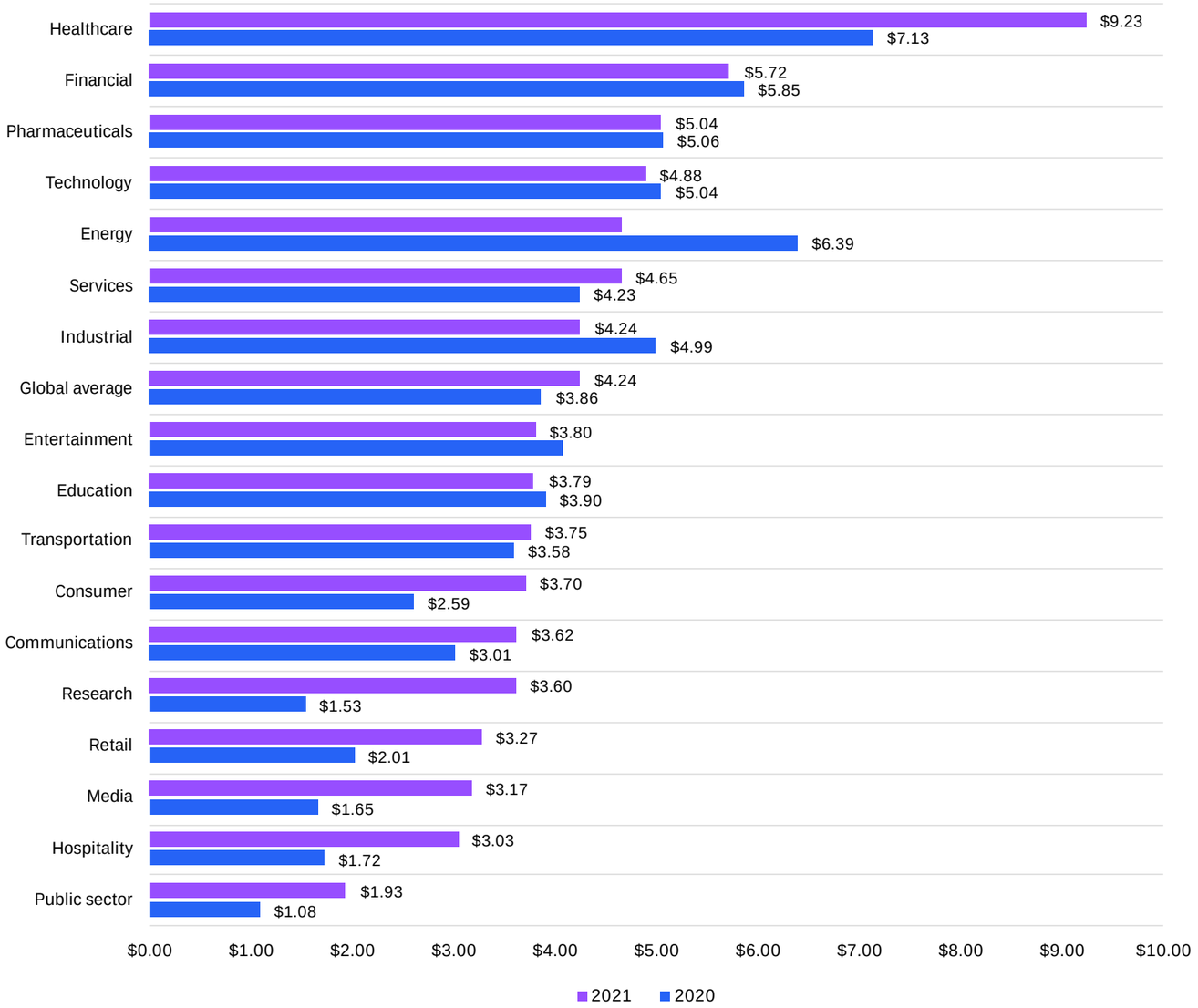
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Average total cost of a data breach by industry

Measured in US$ millions



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

@2 0 3/&7& ñ1%,1(6

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

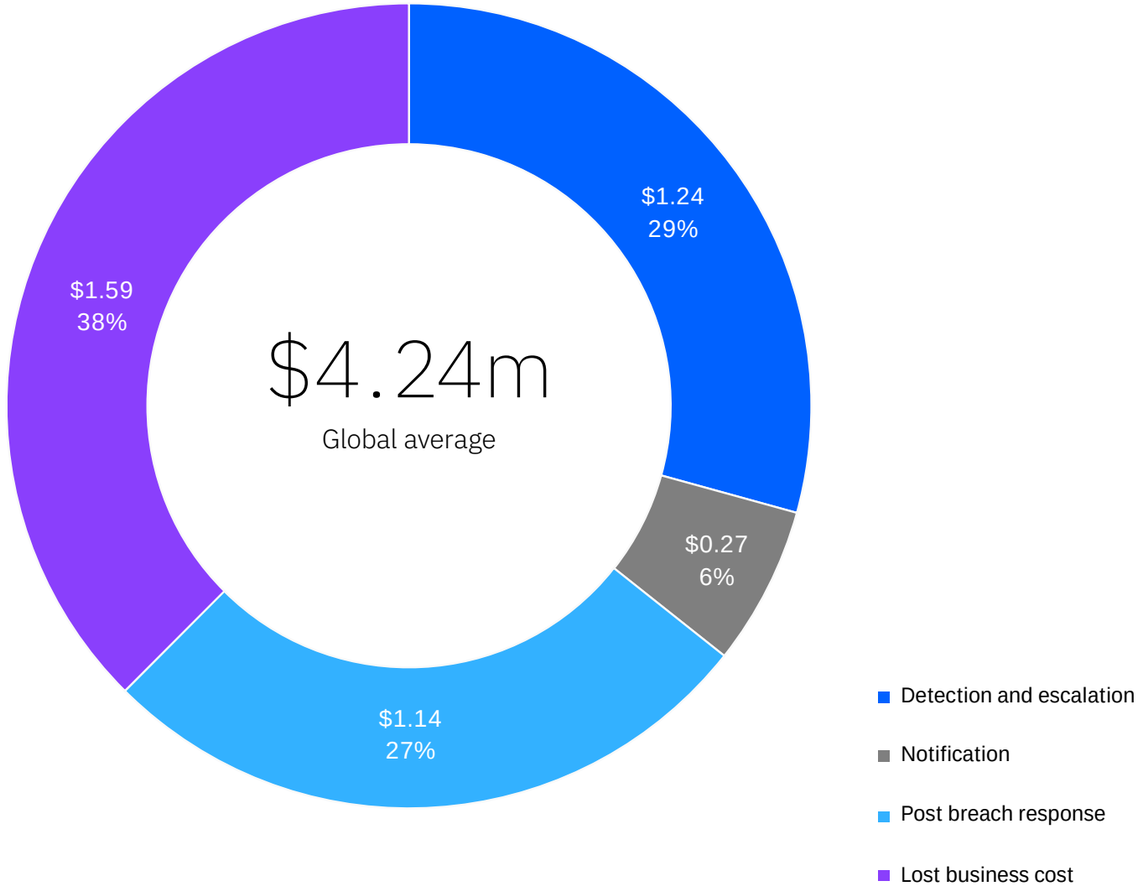
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Average total cost of a data breach divided into four categories

Measured in US$ millions



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

@2 0 3/&7& ñ1%,1(6

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

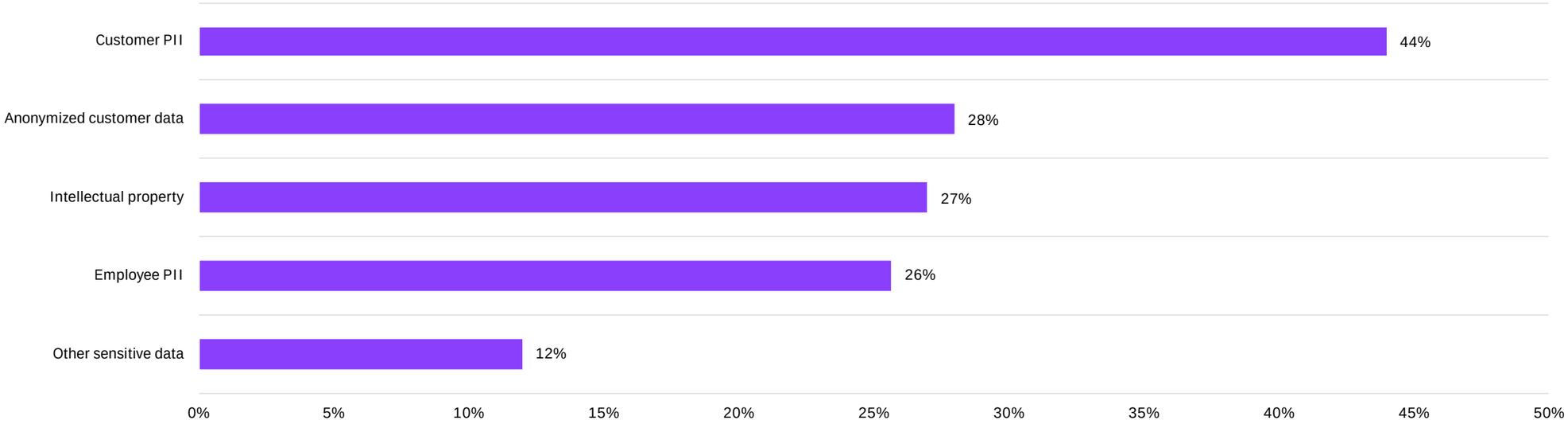
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Types of records compromised

Percentage of breaches involving data in each category



@8672 0 &5 3&5621 ! //< ,%&17,ñ ! #/& ,1'25 0 !7,21 ¤MFF¥

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

@2 0 3/&7& ñ1%,1(6

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

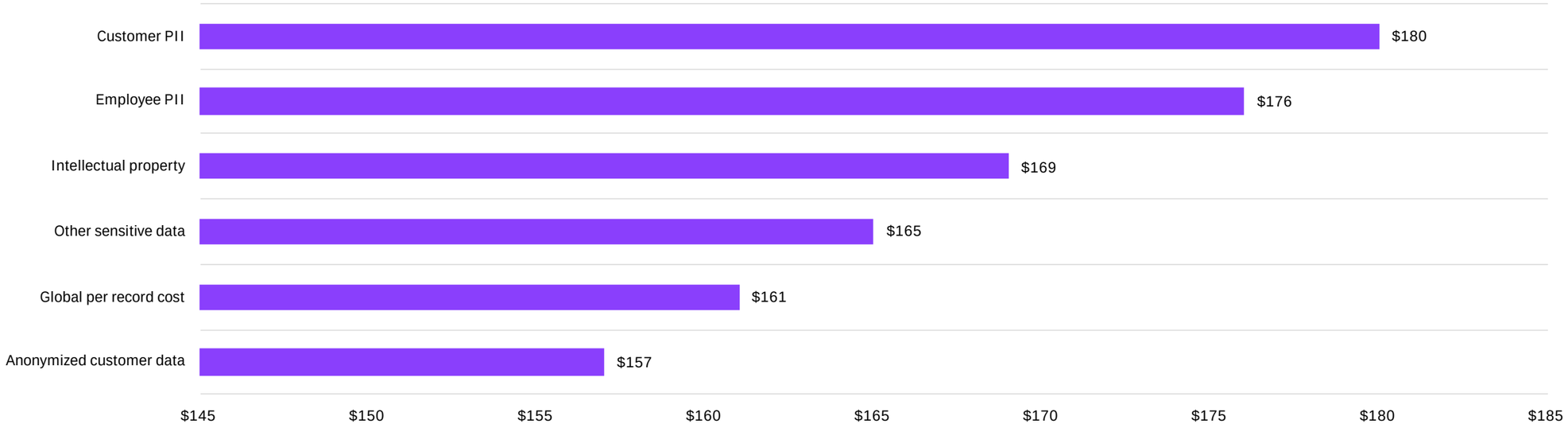
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Average cost per record by type of data compromised

Measured in US$



@8672 0 &5 MFF : ! 6 7+& $267/,&67 7<3& 2' 5&$25%

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

@2 0 3/&7& ñ1%,1(6

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.

H&< ñ1%,1(

$5.01m

Average total cost of a breach caused by business email compromise

Executive summary

@2 0 3/&7& ñ1%,1(6

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

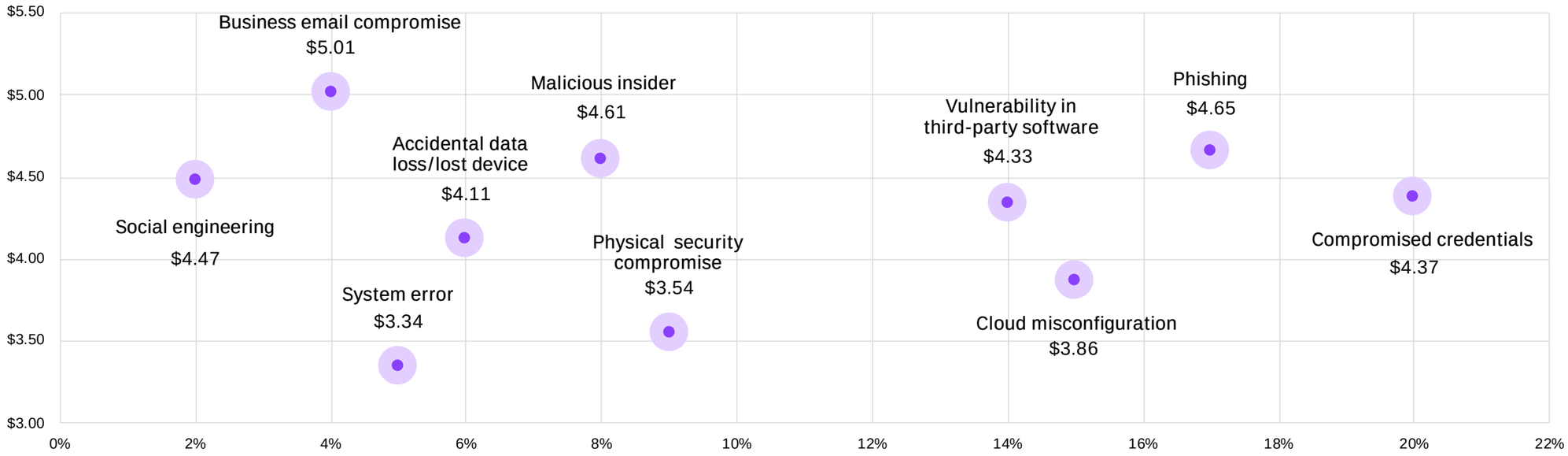
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

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

Measured in US$ millions



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

@2 0 3/&7& ñ1%,1 (6

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.

H&< ñ1%,1 (

$4.87m

Average cost of a breach with a lifecycle over 200 days

Executive summary

@2 0 3/&7& ñ1%,1(6

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

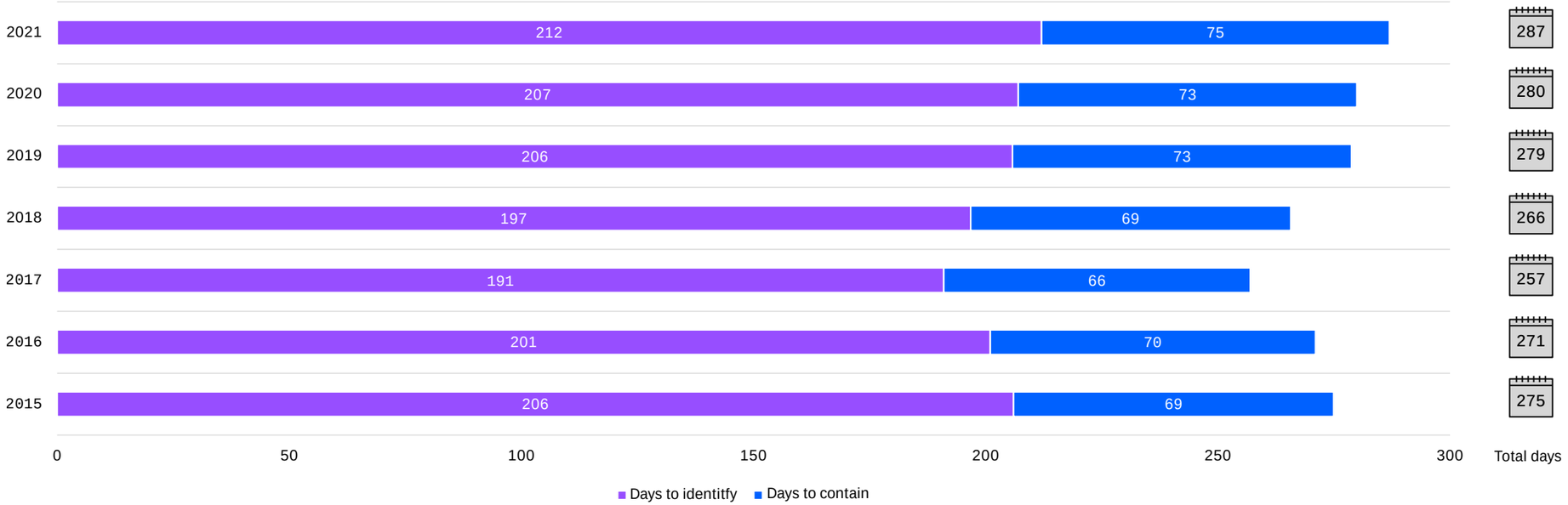
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Average time to identify and contain a data breach

Measured in days



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

@2 0 3/&7& ñ1%,1(6

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

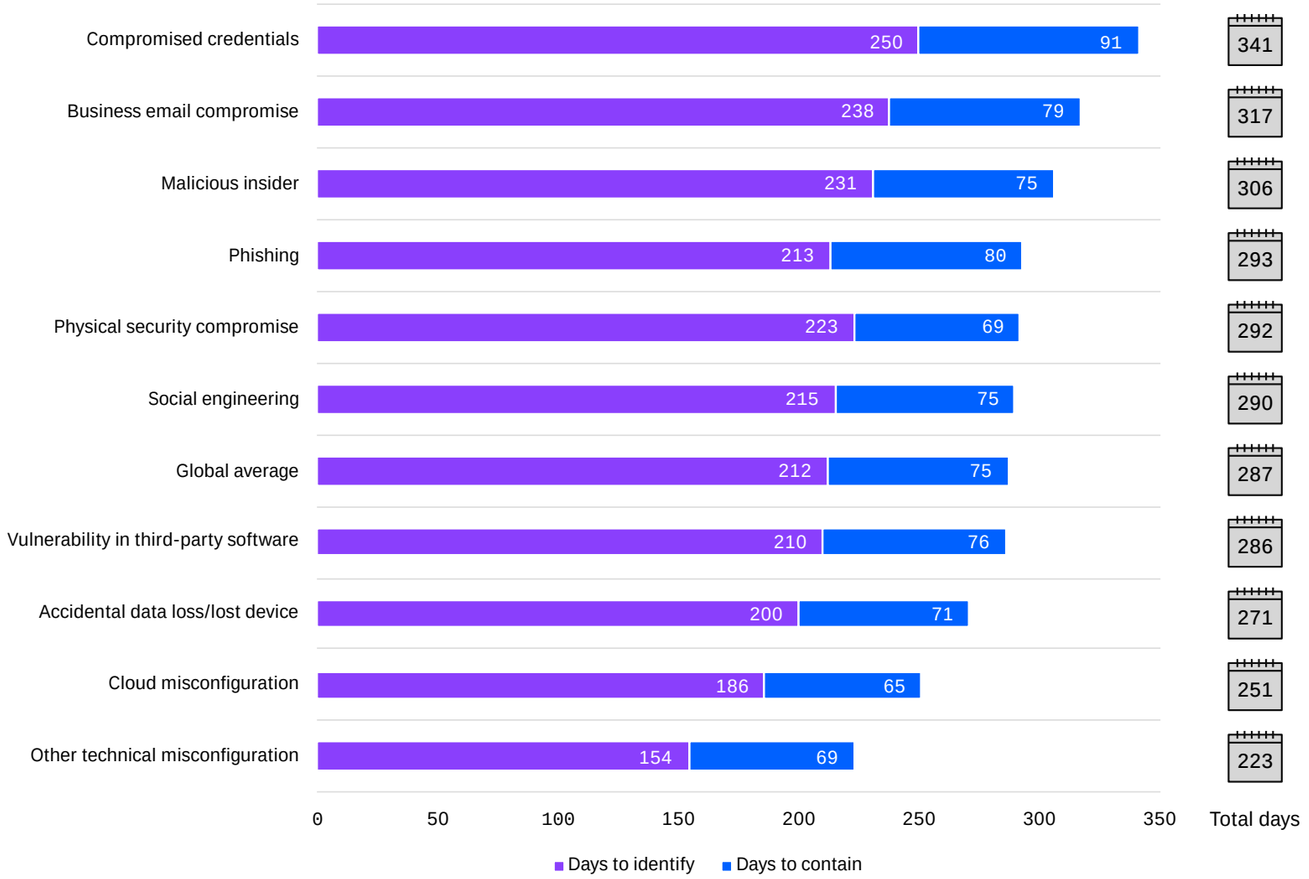
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

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

Measured in days



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

@2 0 3/&7& ñ1%,1(6

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

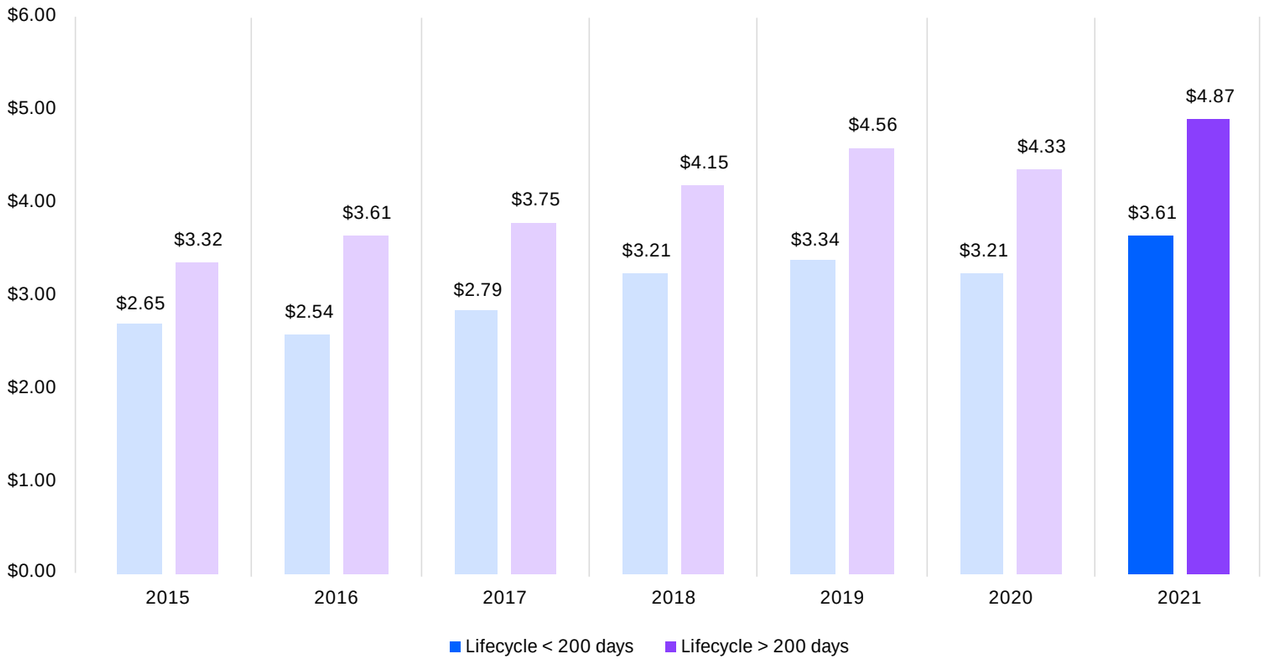
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

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

Measured in US$ millions



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

@2 0 3/&7& ñ1%,1(6

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

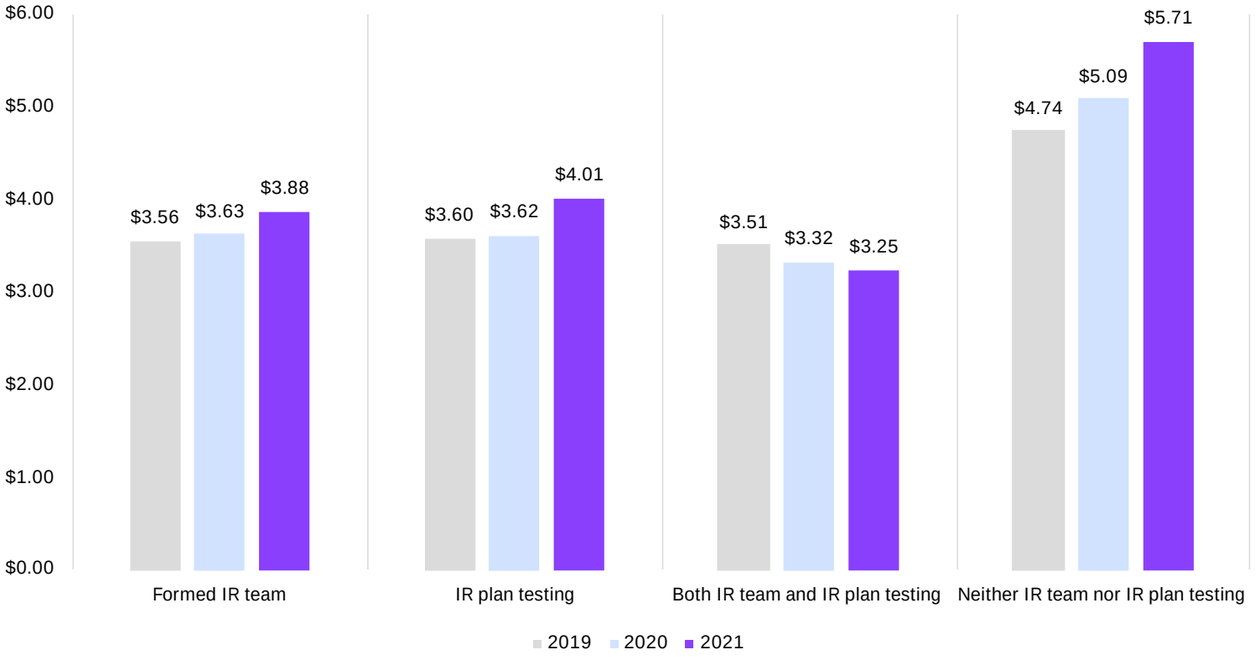
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

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

Measured in US$ millions



F1$,%&17 5&63216& 7&! 0 6 !1% ,1$,%&17 5&63216& 3/!1

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

@2 0 3/&7& ñ1%,1(6

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.

H&< ñ1%,1(

$5.65m

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

Executive summary

@2 0 3/&7& ñ1%,1(6

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

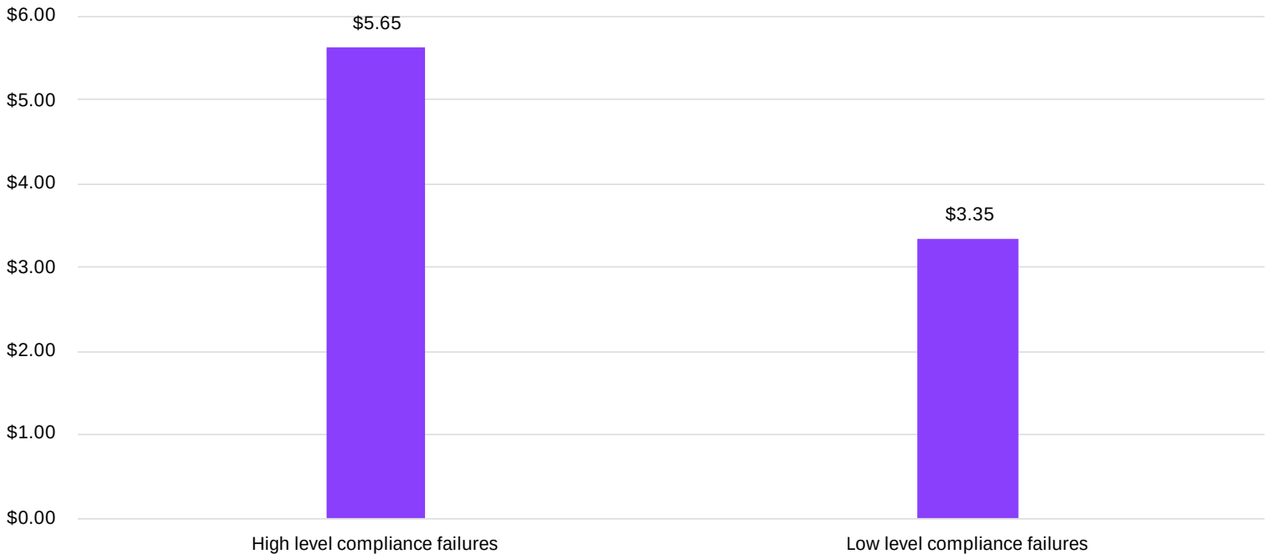
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

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

Measured in US$ millions



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

@2 0 3/&7& ñ1%,1(6

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

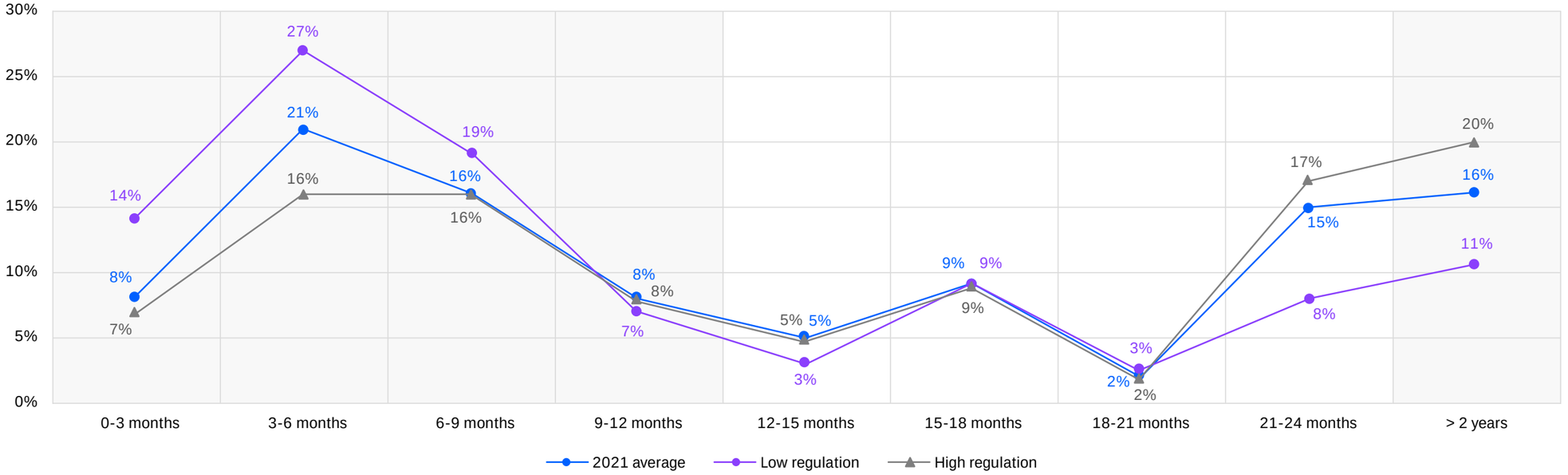
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

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

Percentage of total costs accrued in three month intervals



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

@2 0 3/&7& ñ1%,1 (6

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.

H&< ñ1%,1 (

$5.04m

Average cost of a breach at organizations without zero trust deployed

Executive summary

@2 0 3/&7& ñ1%,1(6

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

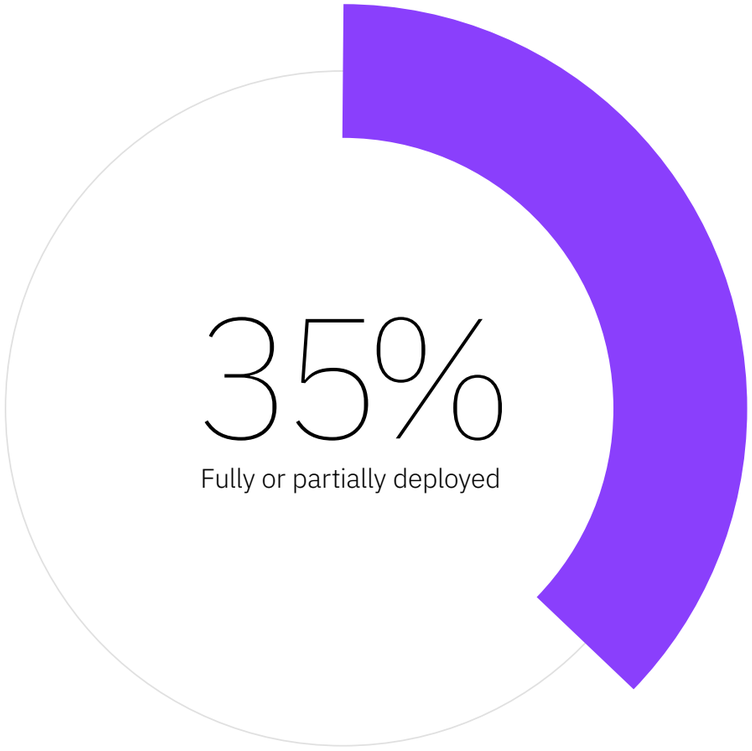
Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Has your organization deployed zero trust?



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

Executive summary

Impact of zero trust

Risk quantification

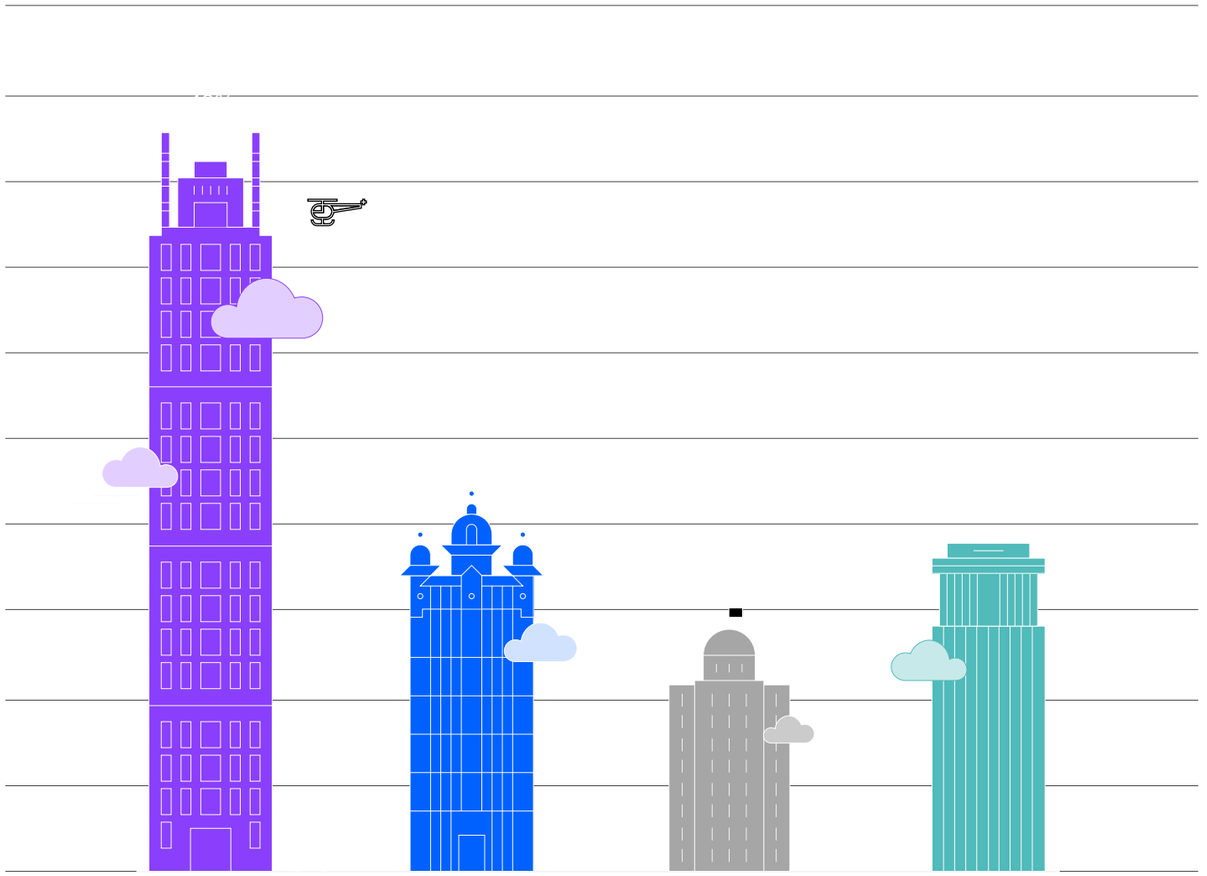
Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps



Executive summary

@2 0 3/&7& ñ1%,1(6

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

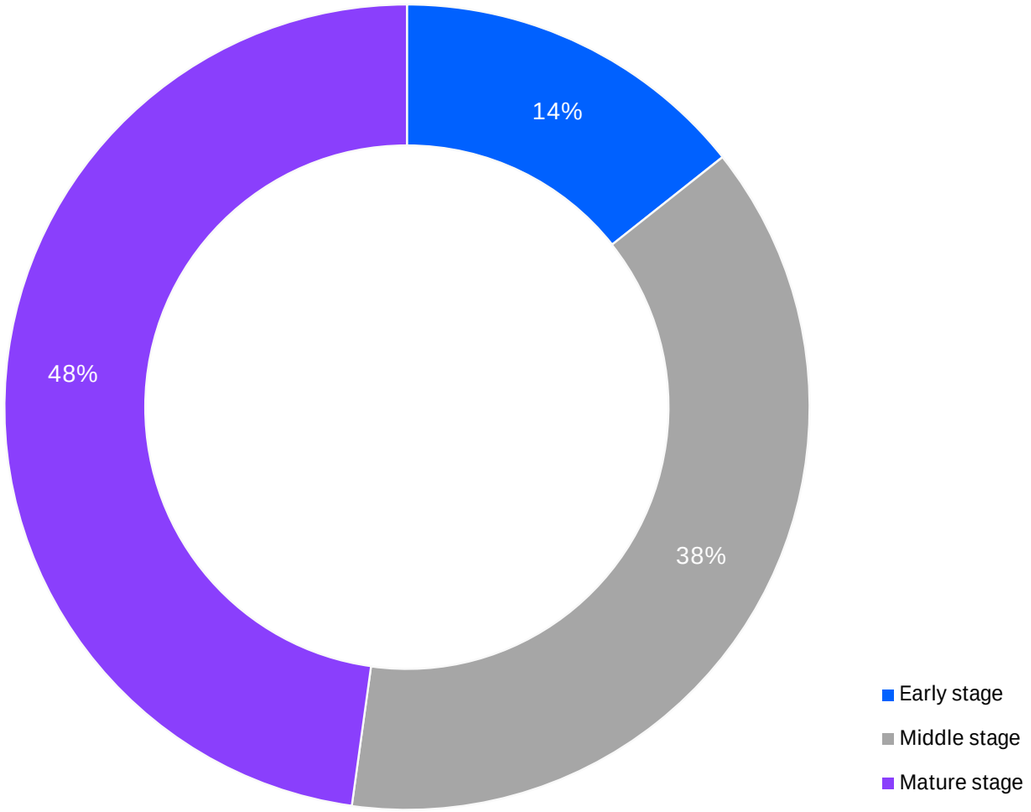
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Zero trust maturity level

Percentage of organizations per maturity stage



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

@2 0 3/&7& ñ1%,1(6

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

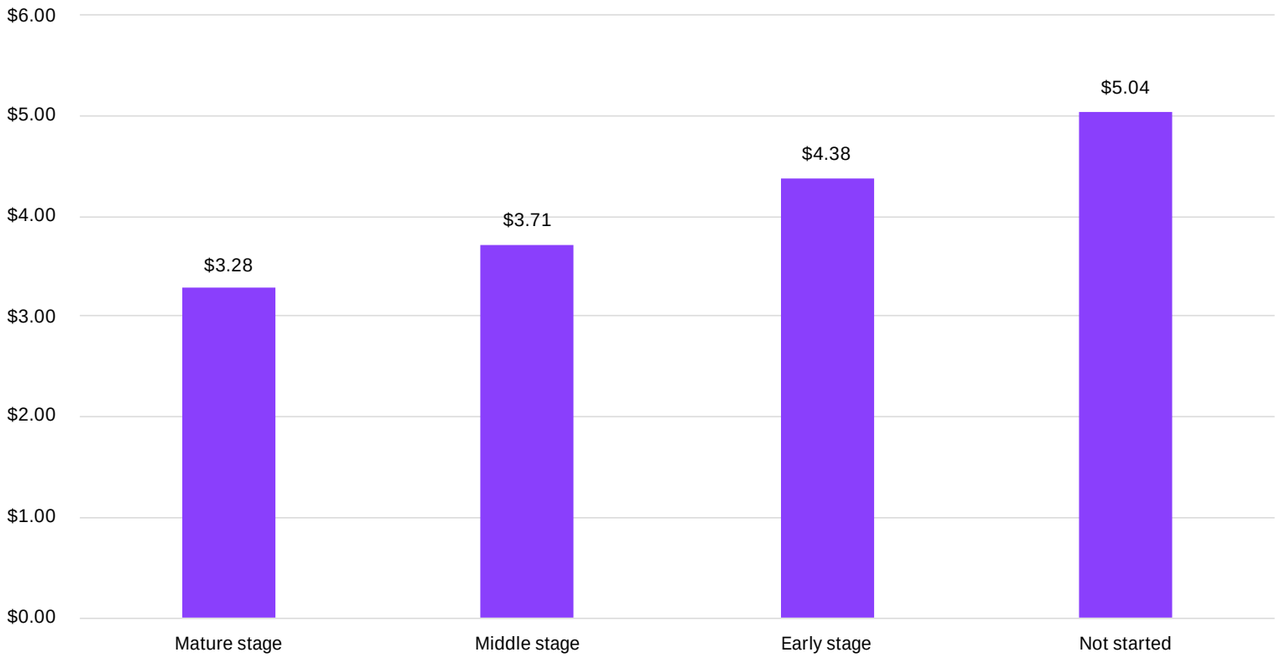
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

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

Measured in US$ millions



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

@2 0 3/&7& ñ1%,1(6

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

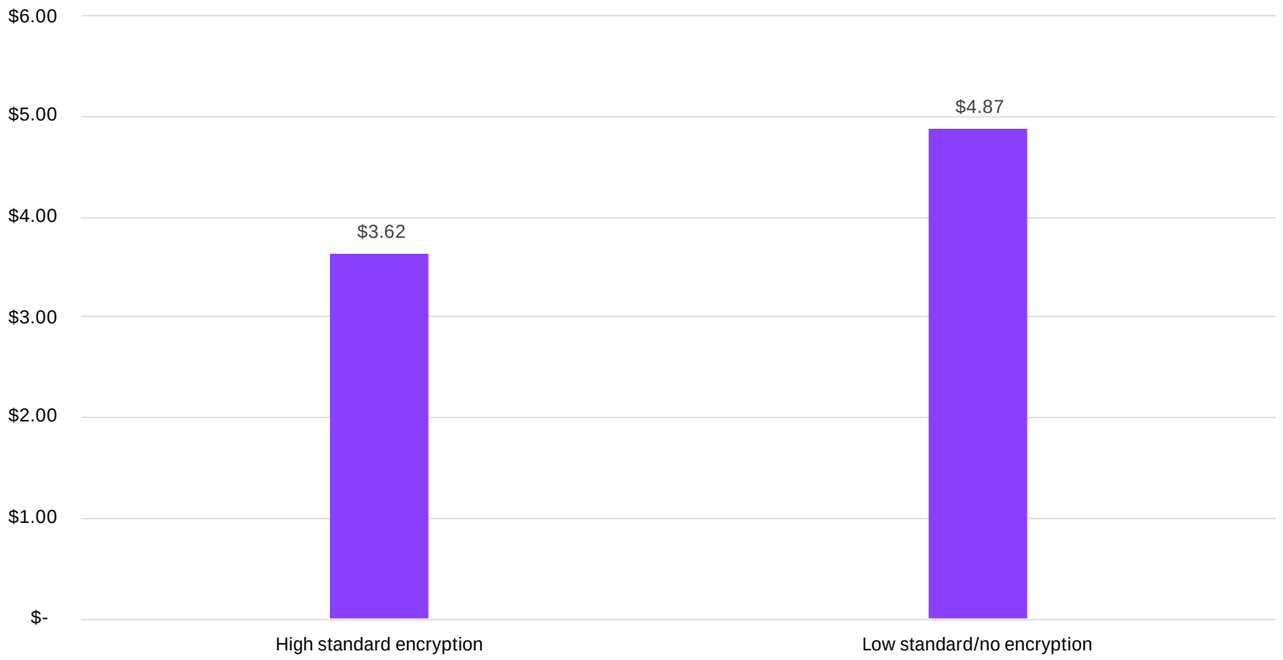
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Impact of encryption on average cost of a data breach

Measured in US$ millions



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

@2 0 3/&7& ñ1%,1 (6

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.

H&< ñ1%,1 (

$2.90m

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

Executive summary

Security AI and automation

Risk quantification

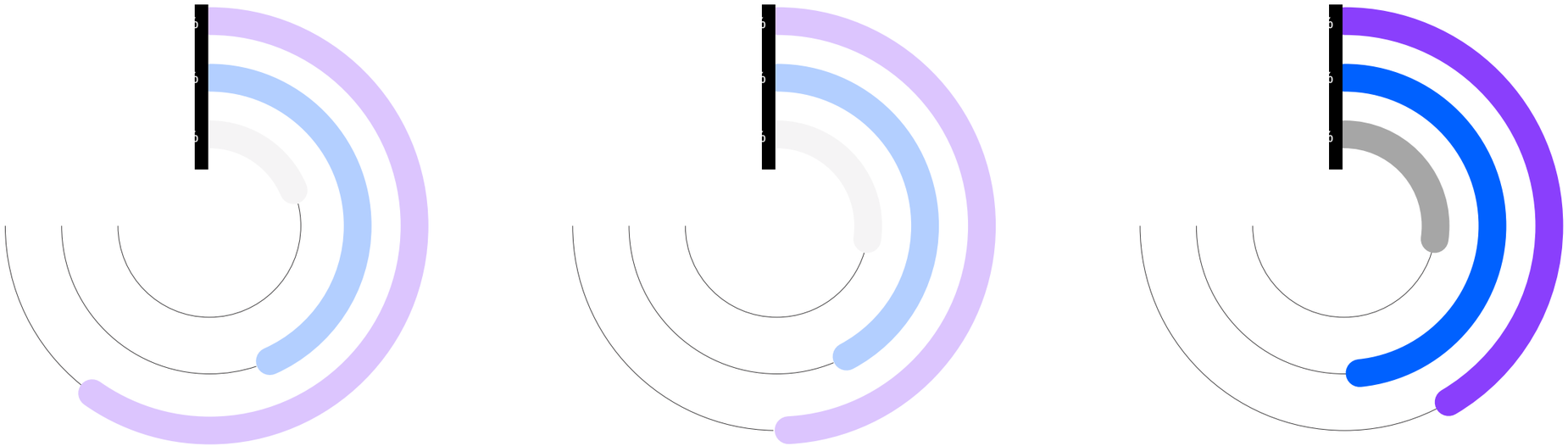
Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps



Executive summary

@2 0 3/&7& ñ1%,1(6

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

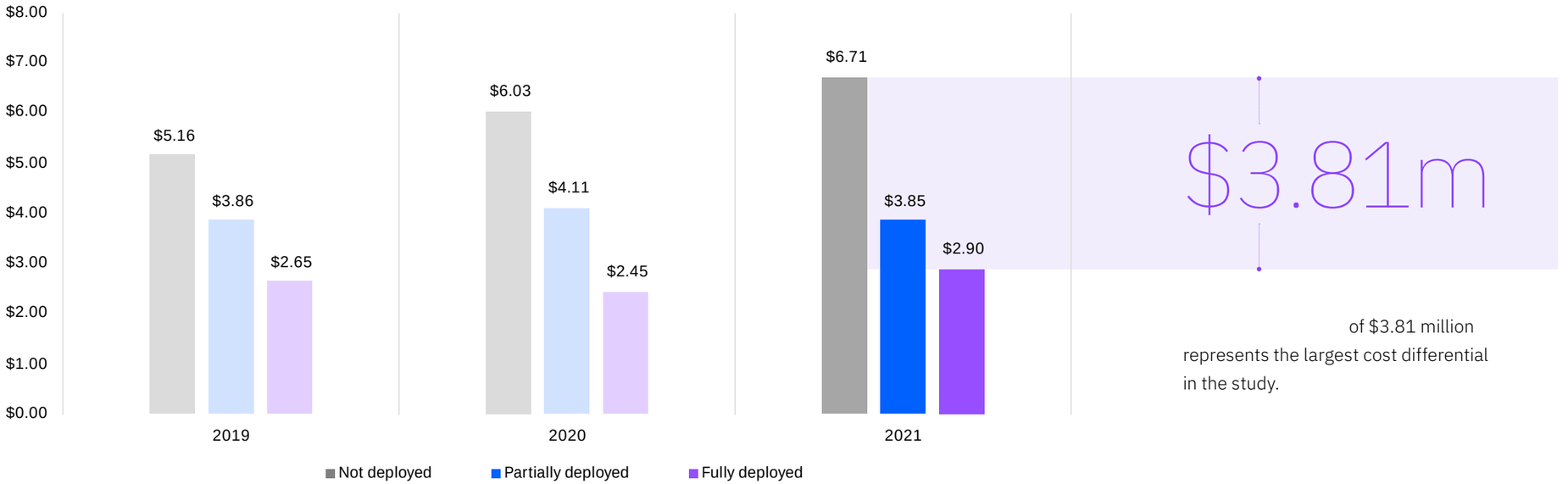
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Average cost of a data breach by security automation deployment level

Measured in US$ millions



$3.81m

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

>F !1% !872 0 !7,21k

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

@2 0 3/&7& ñ1%,1(6

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

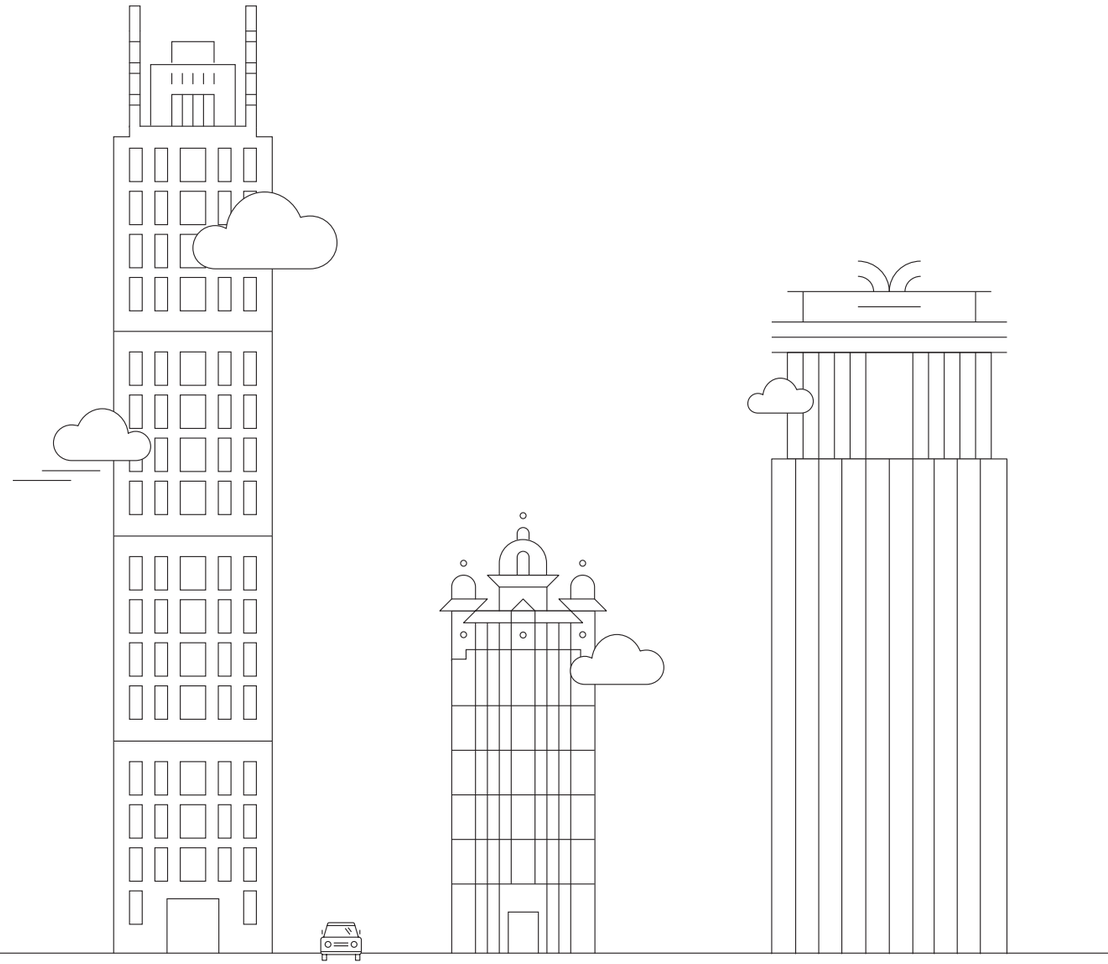
Organizations with fully deployed security AI and automation were able to detect and contain a breach must more quickly than organizations with no security AI/automation deployed.

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 →



Security AI and automation

Risk quantification

Security recommendations

Organization characteristics

Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Executive summary

@2 0 3/&7& ñ1%,1(6

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

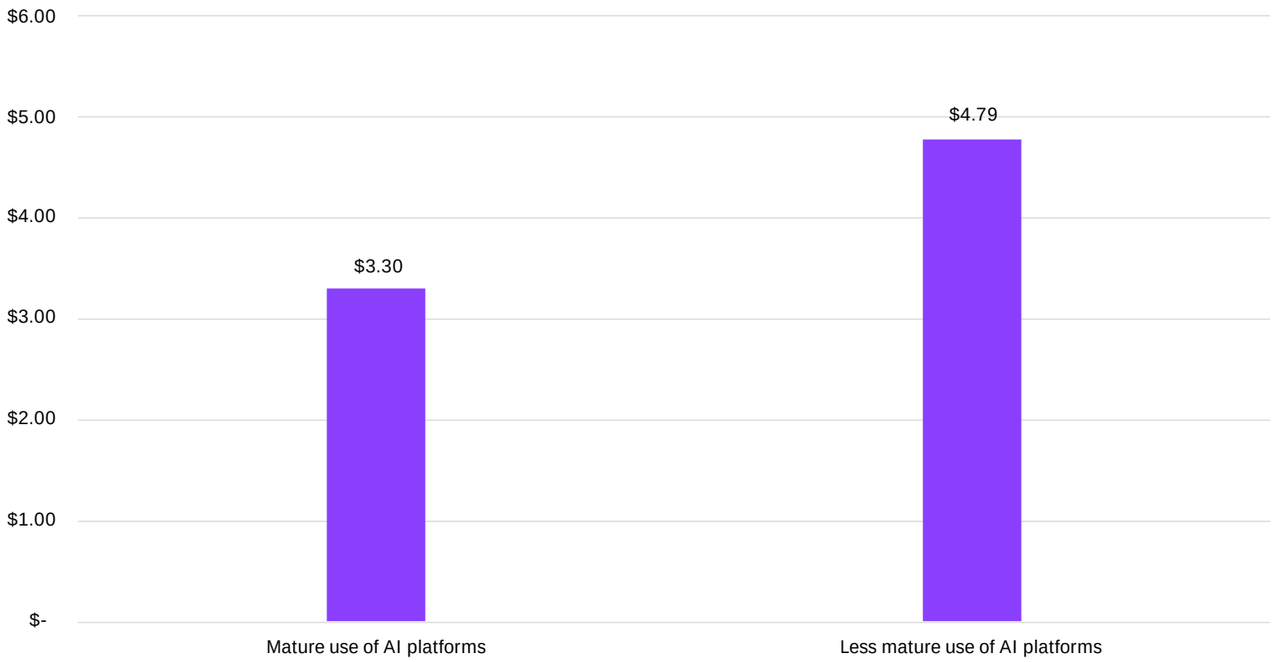
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Impact of AI platforms on average cost of a data breach

Measured in US$ millions



L5(!1,=!7,216 : ,7+ ! 0 !785& 86& 2' >F 3/!7'25 0 6 +!% ! 6,(1,ñ$!17/< /2 : &5 !9&5! (& $267k

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

@2 0 3/&7& ñ1%,1(6

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

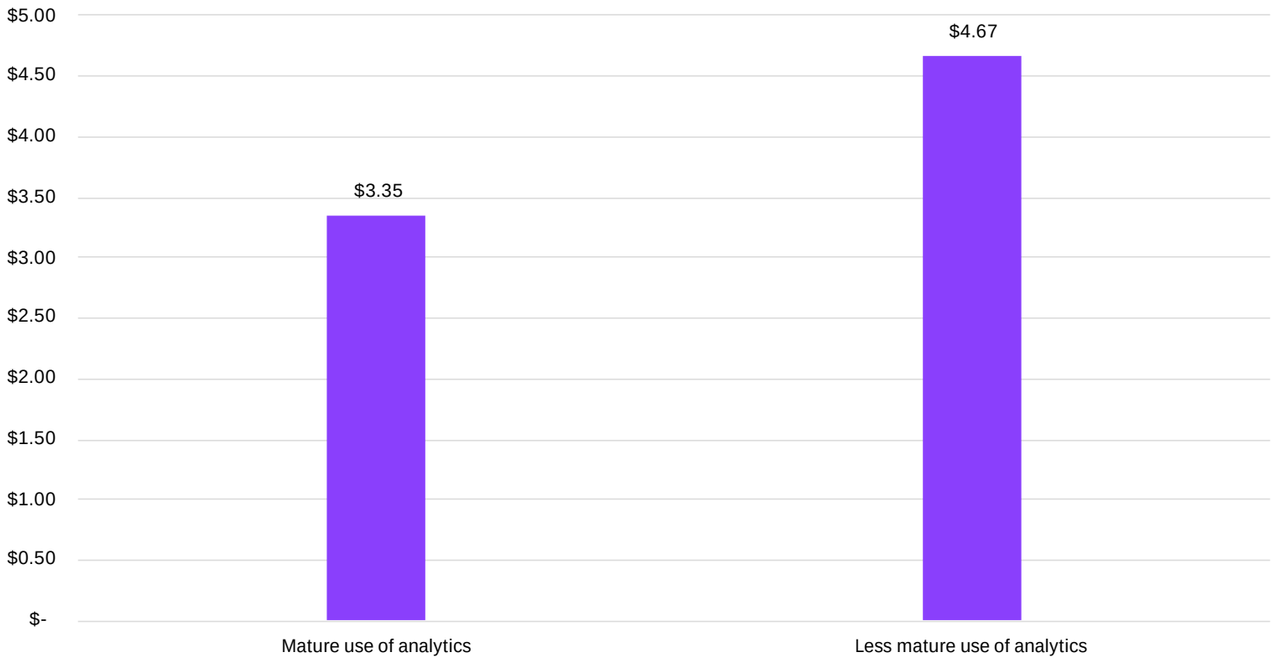
Research methodology

About IBM Security and the Ponemon Institute

Take the next steps

Impact of security analytics on average cost of a data breach

Measured in US$ millions



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

@2 0 3/&7& ñ1%,1(6

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 system complexity on average cost of a data breach

Measured in US$ millions

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%.