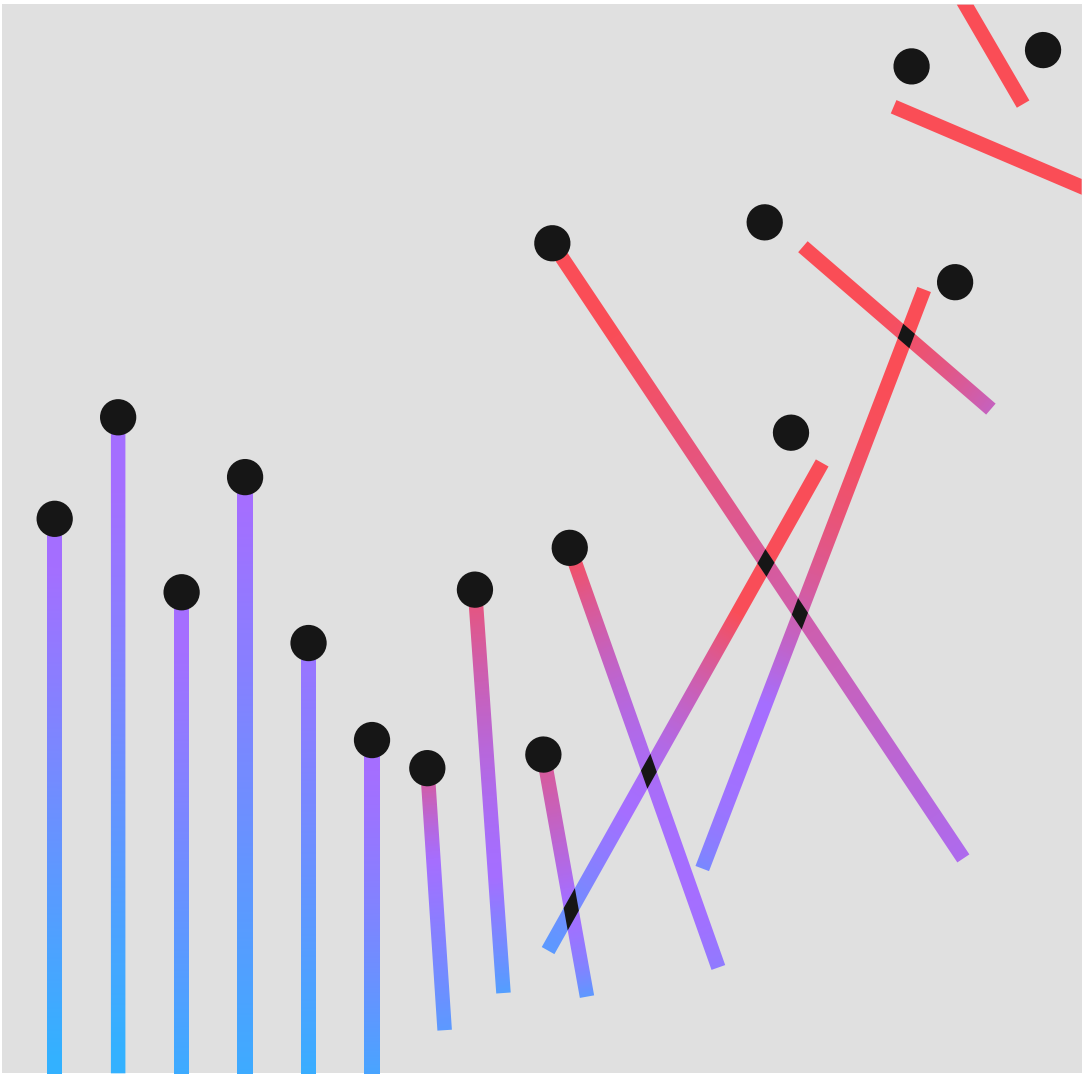
IBM **Security**

Cost of a Data Breach Report 2022



IBM

Contents

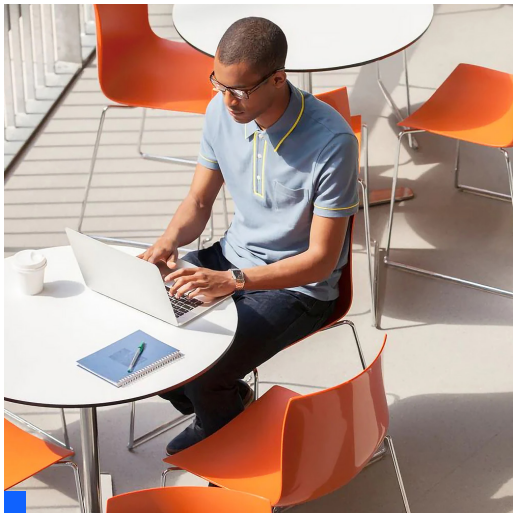
Executive summary

The Cost of a Data Breach Report offers IT, risk management and security leaders a lens into factors that can increase or help mitigate the rising cost of data breaches.

Now in its 17th year, this research — conducted independently by Ponemon Institute, and sponsored, analyzed and published by IBM Security® — studied 550 organizations impacted by data breaches that occurred between March 2021 and March 2022. The breaches occurred across 17 countries and regions and in 17 different industries.

We conducted more than 3,600 interviews with individuals from organizations that were impacted by the data breaches. During the interviews, we asked questions to determine the cost to organizations across different activities related directly to both the immediate and prolonged response to the data breaches.

As in previous years' reports, this year's data provides a view of how dozens of factors impact the costs that keep adding up after a data breach occurs. Additionally, the report examines root causes, short-term and long-term consequences of data breaches, and the mitigating factors and technologies that allowed companies to limit losses.



Significantly, for the first time, the research shows the following insights:

83%

of organizations studied have had more than one data breach.

60%

of organizations' breaches led to increases in prices passed on to customers.

79%

of critical infrastructure organizations didn't deploy a zero trust architecture.

19%

of breaches occurred because of a compromise at a business partner.

45%

of the breaches were cloud-based.

What's new in the 2022 report

With each year's edition, we aim to build upon past research to keep up with changing technology and events. We also try to form a more relevant picture of the risks and strategies for securing data and responding to a breach, from artificial intelligence (AI) to zero trust. Covering some of the technologies most companies focused on in the past year, the 2022 edition of this report has new analysis related to the value of the following:

- Extended detection and response (XDR)
- The use of risk quantification techniques
- Impacts of individual technologies that contribute to a zero trust security framework, such as identity and access management (IAM) and multifactor authentication (MFA)

Furthermore, the report takes a broader look at some leading contributors to higher data breach costs. For the first time, the report looks at the effects of supply chain compromises and the security skills gap.

The report examines areas of security vulnerability from the cloud to critical infrastructure. And we take a deeper dive than past years into the impacts of ransomware and destructive attacks. Also studied is the phenomenon of remote work that continues to be a reality for many organizations past the peak of the COVID pandemic.

As companies experience more breaches and costs continue to climb, this report can serve as a tool to help your teams better manage risk and limit potential losses.
The report is divided into the following five major sections:

- The executive summary with key findings and what's new in the 2022 edition
- In-depth analysis on the complete findings, including breach costs by geographic region and industry
- Security recommendations from IBM Security experts based on this report's results
- Demographics of organizations and industry definitions
- The study's methodology, including how costs were calculated

IBM Security and Ponemon Institute are pleased to present the results of the 2022 Cost of a Data Breach Report.

Key findings

The key findings described here are based on IBM Security analysis of research data compiled by Ponemon Institute.[1]

USD 4.35 million

Average total cost of a data breach

Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022. This figure represents a 2.6% increase from last year, when the average cost of a breach was USD 4.24 million. The average cost has climbed 12.7% from USD 3.86 million in the 2020 report.

83%

Percentage of organizations that have had more than one breach

Eighty-three percent of organizations studied have experienced more than one data breach, and just 17% said this was their first data breach. Sixty percent of organizations studied stated that they increased the price of their services or products because of the data breach.

USD 4.82 million

Average cost of a critical infrastructure data breach

The average cost of a data breach for critical infrastructure organizations studied was USD 4.82 million — USD 1 million more than the average cost for organizations in other industries. Critical infrastructure organizations included those in the financial services, industrial, technology, energy, transportation, communication, healthcare, education and public sector industries. Twenty-eight percent experienced a destructive or ransomware attack, while 17% experienced a breach because of a business partner being compromised.

USD 3.05 million

Average cost savings associated with fully deployed security AI and automation

Breaches at organizations with fully deployed security AI and automation cost USD 3.05 million less than breaches at organizations with no security AI and automation deployed. This 65.2% difference in average breach cost — between USD 3.15 million for fully deployed versus USD 6.20 million for not deployed — represented the largest cost savings in the study. Companies with fully deployed security AI and automation also experienced on average a 74-day shorter time to identify and contain the breach, known as the breach lifecycle, than those without security AI and automation — 249 days versus 323 days. The use of security AI and automation jumped by nearly one-fifth in two years, from 59% in 2020 to 70% in 2022.

1. Cost amounts in this report are measured in US dollars (USD).

USD 4.54 million

Average cost of a ransomware attack, not including the cost of the ransom itself

Eleven percent of breaches in the study were ransomware attacks, an increase from 2021, when 7.8% of breaches were ransomware, for a growth rate of 41%. The average cost of a ransomware attack went down slightly, from USD 4.62 million in 2021 to USD 4.54 million in 2022. This cost was slightly higher than the overall average total cost of a data breach, USD 4.35 million.

19%

Frequency of breaches caused by stolen or compromised credentials

Use of stolen or compromised credentials remains the most common cause of a data breach. Stolen or compromised credentials were the primary attack vector in 19% of breaches in the 2022 study and also the top attack vector in the 2021 study, having caused 20% of breaches. Breaches caused by stolen or compromised credentials had an average cost of USD 4.50 million. These breaches had the longest lifecycle — 243 days to identify the breach, and another 84 days to contain the breach. Phishing was the second most common cause of a breach at 16% and also the costliest, averaging USD 4.91 million in breach costs.

59%

Percentage of organizations that don't deploy zero trust

Just 41% of organizations in the study said they deploy a zero trust security architecture. The other 59% percent of organizations that don't deploy zero trust incur an average of USD 1 million in greater breach costs compared to those that do deploy. Among critical infrastructure organizations, an even higher percentage of 79% doesn't deploy zero trust. These organizations experienced on average USD 5.40 million in breach costs, more than USD 1 million higher than the global average.

USD 1 million

Average difference in cost where remote work was a factor in causing the breach versus when it wasn't a factor

When remote working was a factor in causing the breach, costs were an average of nearly USD 1 million greater than in breaches where remote working wasn't a factor — USD 4.99 million versus USD 4.02 million. Remote work-related breaches cost on average about USD 600,000 more compared to the global average.

45%

Share of breaches that occurred in the cloud

Forty-five percent of breaches in the study occurred in the cloud. Yet breaches that happened in a hybrid cloud environment cost an average of USD 3.80 million, compared to USD 4.24 million for breaches in private clouds and USD 5.02 million for breaches in public clouds. The cost difference was 27.6% between hybrid cloud breaches and public cloud breaches. Organizations with a hybrid cloud model also had shorter breach lifecycles than organizations that solely adopted a public or private cloud model.

USD 2.66 million

Average cost savings associated with an incident response (IR) team and regularly tested IR plan

Nearly three-quarters of organizations in the study said they had an IR plan, while 63% of those organizations said they regularly tested the plan. Having an IR team and an IR plan that was regularly tested led to significant cost savings. Businesses with an IR team that tested its IR plan saw an average of USD 2.66 million lower breach costs than organizations without an IR team and that don't test an IR plan. The difference of USD 3.26 million versus USD 5.92 million represents a 58% cost savings.

29 days

Savings in response time for those with extended detection and response (XDR) technologies

XDR technologies were implemented by 44% of organizations. Those organizations with XDR technologies saw considerable advantages in response times. Those organizations with XDR deployed shortened the breach lifecycle by about a month, on average, compared to organizations that didn't implement XDR. Specifically, organizations took 275 days to identify and contain a breach with XDR deployed versus 304 days without XDR deployed. This figure represents a 10% difference in response times.

12 years

Consecutive years the healthcare industry had the highest average cost of a breach

Healthcare breach costs hit a new record high. The average breach in healthcare increased by nearly USD 1 million to reach USD 10.10 million. Healthcare breach costs have been the most expensive industry for 12 years running, increasing by 41.6% since the 2020 report. Financial organizations had the second highest costs — averaging USD 5.97 million — followed by pharmaceuticals at USD 5.01 million, technology at USD 4.97 million and energy at USD 4.72 million.

USD 9.44 million

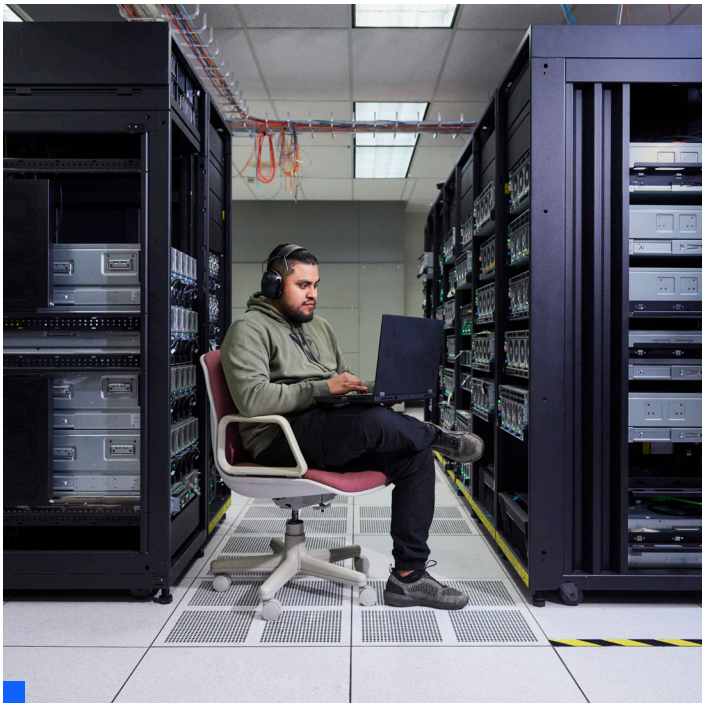
Average cost of a breach in the United States, the highest of any country

The top five countries and regions for the highest average cost of a data breach were the United States at USD 9.44 million, the Middle East at USD 7.46 million, Canada at USD 5.64 million, the United Kingdom at USD 5.05 million and Germany at USD 4.85 million. The United States has led the list for 12 years in a row. Meanwhile, the country with the fastest growth rate over last year was Brazil, a 27.8% increase from USD 1.08 million to USD 1.38 million.

Complete findings

In this section, we provide the detailed findings of this report, in 16 themes. Topics are presented in the following order:

- Global highlights
- Data breach lifecycle
- Initial attack vectors
- Key cost factors
- Security AI and automation
- XDR technologies
- Incident response
- Risk quantification
- Zero trust
- Ransomware and destructive attacks
- Supply chain attacks
- Critical infrastructure
- Cloud breaches and cloud model
- Remote work
- Skills gap
- Mega breaches



USD 4.35 million

Global average total cost of a data breach

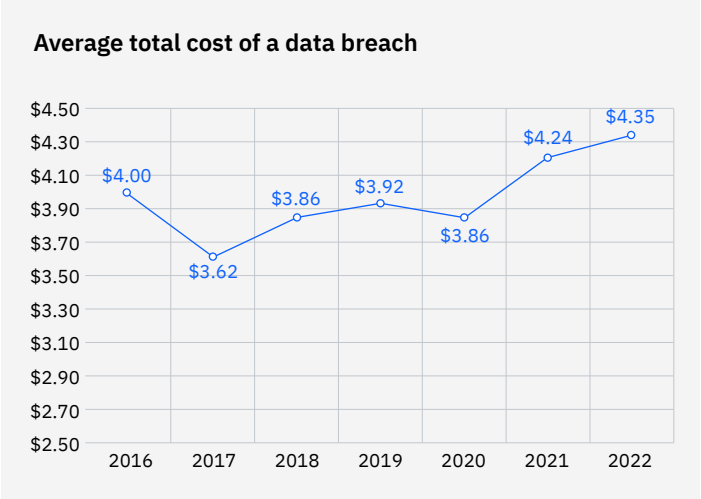


Figure 1: Measured in USD millions

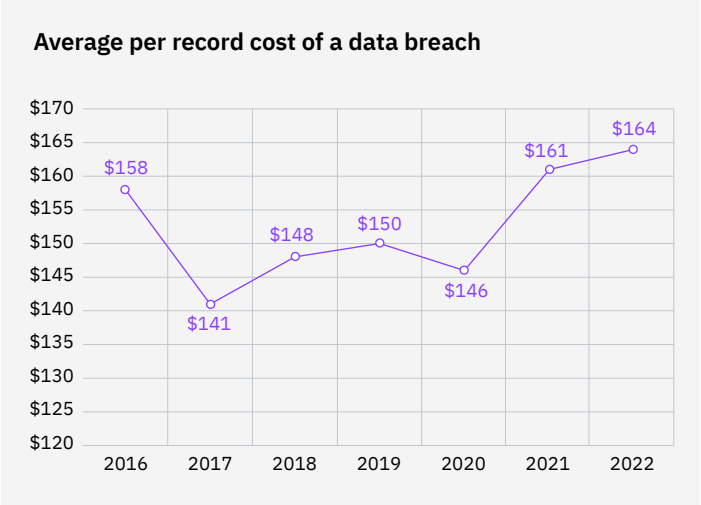


Figure 2: Measured in USD

Global highlights

The Cost of a Data Breach Report is a global report, comprising data from 17 countries and regions and 17 industries. In this section, we look at several key metrics at the level of global average, as well as comparative costs between countries and between industries.

Figure 1: The average cost of a data breach reached a record high in 2022.
The global average total cost of a data breach increased by USD 0.11 million to USD 4.35 million in 2022, the highest it's been in the history of this report. The increase from USD 4.24 million in the 2021 report to USD 4.35 million in the 2022 report represents a 2.6% increase. In the last two years, the average total cost has increased 12.7% from USD 3.86 million in the 2020 report.

Figure 2: The per record cost of a data breach hit a seven-year high.
The global per record cost of a data breach in 2022 was USD 164, a 1.9% increase from USD 161 in 2021. The increase from USD 146 in 2020 is an increase of 12.3%. This study examines breaches sized between 2,200 and 102,000 records. It's not consistent with this research to use the per record cost to calculate the cost of single or multiple breaches above 102,000 records. For more information, see the "Research methodology" section.

Average cost of a data breach by country or region

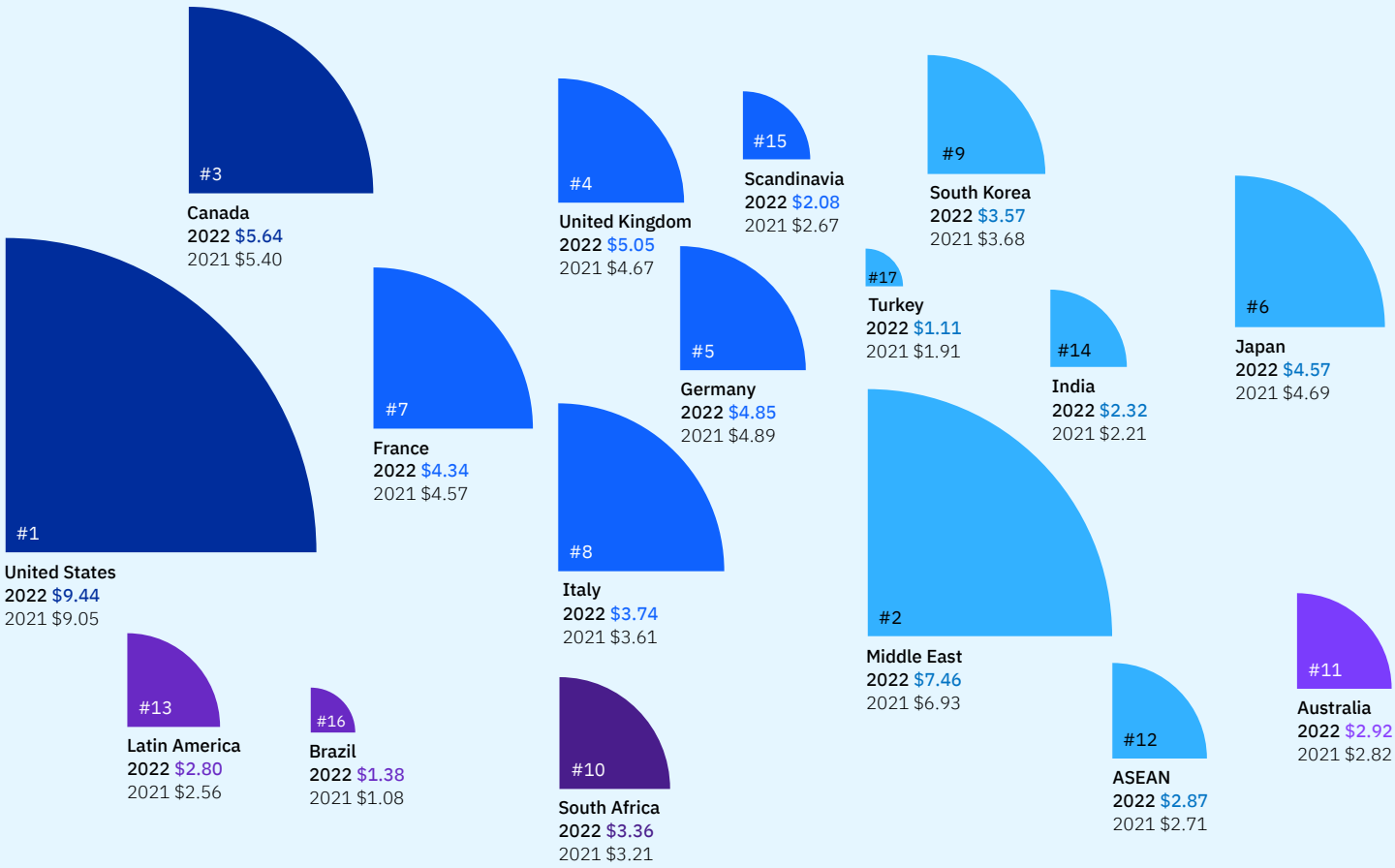


Figure 3: Measured in USD millions

Figure 3: The United States was the costliest country for average total cost of a data breach for the 12th year in a row. The top five countries or regions with the highest average cost of a data breach were:

1. The United States — USD 9.44 million
2. The Middle East — USD 7.46 million
3. Canada — USD 5.64 million
4. The United Kingdom — USD 5.05 million
5. Germany — USD 4.85 million

The United States had the highest average total cost of a data breach at USD 9.44 million, a 4.3% increase of USD 0.39 million, up from USD 9.05 million in 2021. Similar to last year, the Middle East region again had the second highest average total cost of a data breach, increasing from USD 6.93 million in 2021 to USD 7.46 million in 2022. This average cost was an increase of USD 0.53 million, or 7.6%. Canada was again the third highest cost country at USD 5.64 million, an increase of USD 0.24 million or 4.4%. The United Kingdom climbed to number four from eighth out of the 17 countries or regions, surpassing Germany, Japan and France in the ranking. The average total cost of a breach in the United Kingdom was USD 5.05 million, up from USD 4.67 million, an increase of USD 0.38 million, or 8.1%.

Out of the 17 countries or regions studied, six — Germany, Japan, France, South Korea, Scandinavia and Turkey — saw a decrease in the average total cost of a data breach. Brazil, 16th on the list at USD 1.38 million, saw the largest relative cost increase, up USD 0.3 million or 27.8%. Turkey, 17th on the list, saw the largest relative cost decrease, falling from USD 1.91 million to USD 1.11 million, a decrease of USD 0.8 million or 42%. Broad swings in currency valuations, such as occurred in Turkey, can play a role in cost variations from year to year.

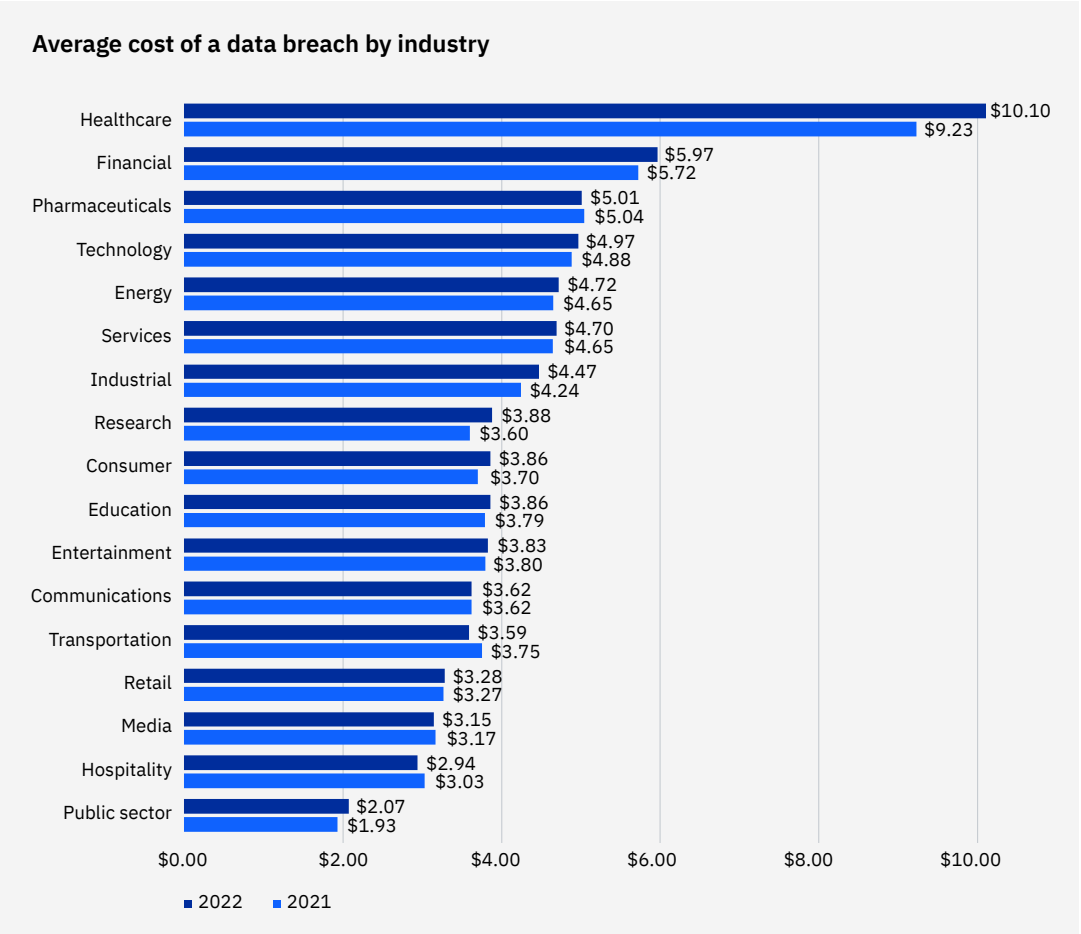


Figure 4: Measured in USD millions

Figure 4: Healthcare was highest cost industry for the 12th year in a row.
The average total cost of a breach in healthcare increased from USD 9.23 million in the 2021 report to USD 10.10 million in 2022, an increase of USD 0.87 million or 9.4%. Healthcare is one of the more highly regulated industries and is considered critical infrastructure by the US government.

Healthcare is one of the more highly regulated industries and is considered critical infrastructure by the US government.

The top five industries by cost were unchanged in the order of ranking from the 2021 report. Following healthcare were the financial, pharmaceuticals, technology and energy industries. The financial industry saw an increase from USD 5.72 million in 2021 to USD 5.97 million in 2022, an increase of USD 0.25 million or 4.4%. The industrial industry, comprised of chemical, engineering and manufacturing organizations, saw an increase from USD 4.24 million to USD 4.47 million in 2022, an increase of USD 0.23 million or 5.4%. The average total cost decreased slightly in four industries — pharmaceuticals, transportation, media and hospitality.

Figure 5: Detection and escalation costs surpassed lost business costs as the largest of four cost categories comprising the cost of a data breach, for the first time in six years. Broken down into four cost categories — lost business, detection and escalation, notification and post breach response — the largest share of data breach costs in 2022 was detection and escalation. Detection and escalation costs increased from USD 1.24 million in 2021 to USD 1.44 million in 2022, an increase of USD 0.2 million or 16.1%. Detection and escalation costs include activities that enable a company to reasonably detect a breach. These costs include forensic and investigative activities; assessment and audit services; crisis management; and communications to executives and boards.

For the first time in at least six years, lost business, at USD 1.42 million in 2022, wasn't the largest share of data breach costs. Lost business costs decreased from USD 1.59 million in 2021, a decrease of 10.7%. Lost business costs include activities that attempt to minimize the loss of customers, business disruption and revenue losses. These costs include business disruption and revenue losses from system downtime; cost of lost customers and acquiring new customers; and reputation losses and diminished goodwill.

Notification costs and post breach response costs remained relatively unchanged from 2021 to 2022. See "How we calculate the cost of a data breach" in the "Research methodology" section for definitions of each of the four cost categories.

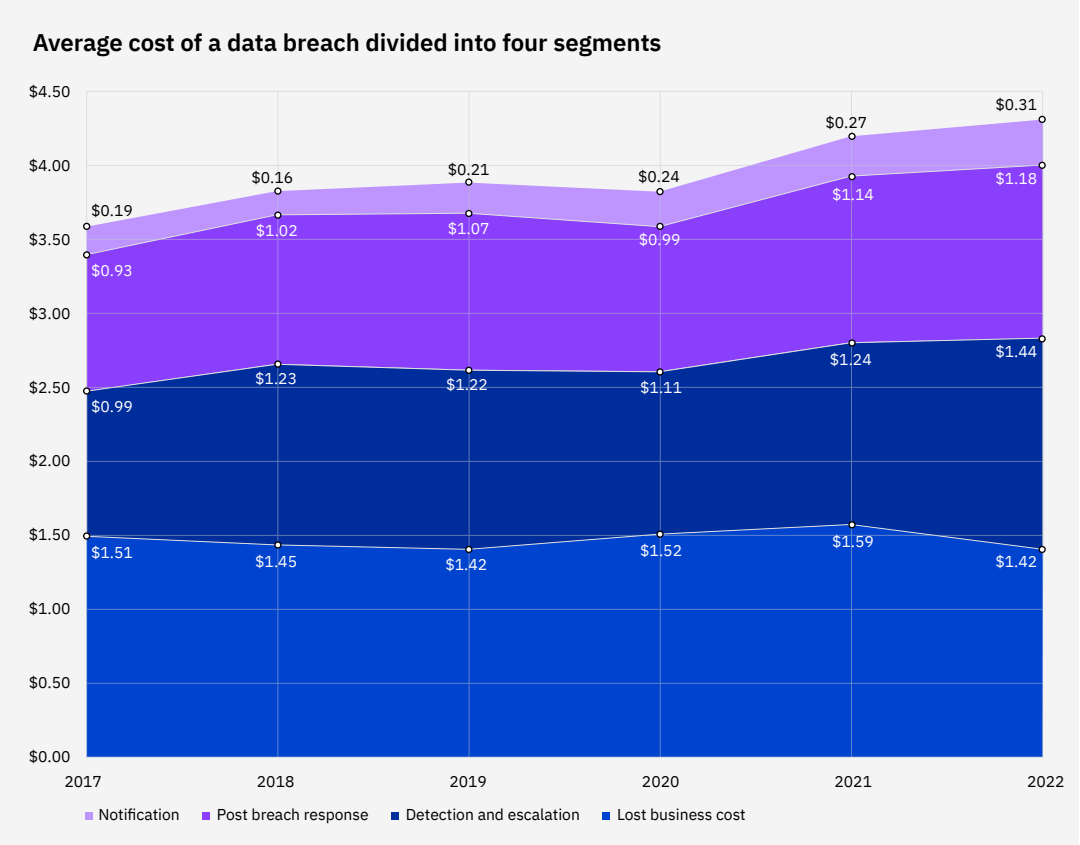


Figure 5: Measured in USD millions

Was this your first data breach?

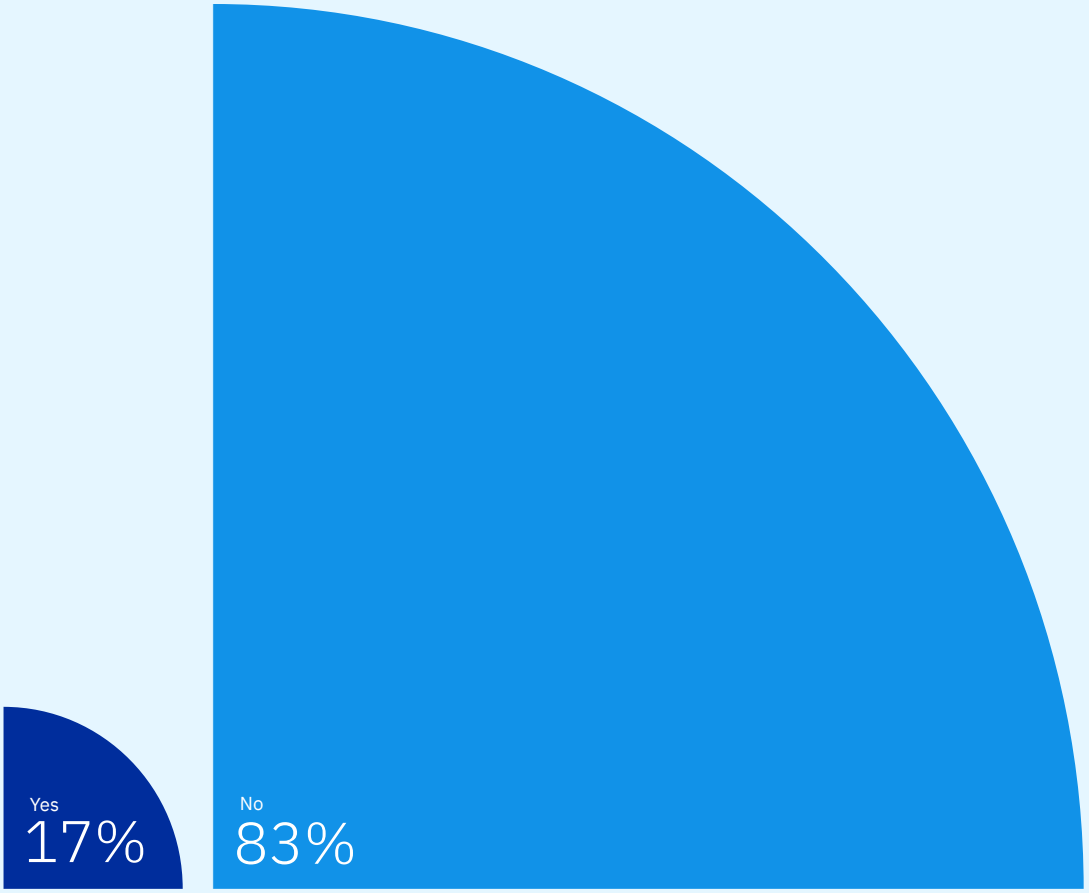


Figure 6

Figure 6: Most organizations in the study have experienced more than one data breach.
Of the 550 organizations in the study, just 17% said this was their first data breach. Eighty-three percent said this wasn't their first data breach. With security teams handling more incidents every year and considering the impact of remote work on security, it's likely the recurrence of breaches is climbing.

Figure 7: A majority of organizations in the study said they increased the price of their products and services as a result of the data breach.
In response to the question, 60% said they increased prices, and 40% said they didn't increase prices.

Did the data breach result in your organization increasing the price of products and services?

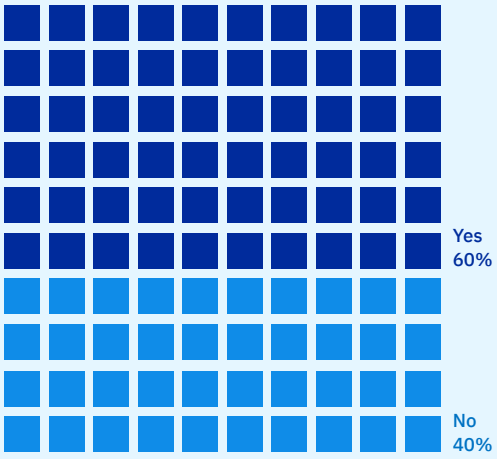


Figure 7

277 days

Average time to identify and contain a data breach

Data breach lifecycle

The time elapsed between the first detection of the breach and its containment is referred to as the data breach lifecycle. The time to identify a breach describes the time it takes to detect that an incident has occurred. The time to contain a breach refers to the time it takes for an organization to resolve a situation when it's been detected and ultimately restore service. These metrics can be used to determine the effectiveness of an organization's incident response and containment processes.

Figure 8: The mean or average time to identify and contain a data breach fell from 287 days in 2021 to 277 days in 2022, a decrease of 10 days or 3.5%.
In 2022 it took an average of 207 days to identify the breach and 70 days to contain the breach. In 2021 it took an average of 212 days to identify the breach and 75 days to contain the breach. The 277-day average in 2022 means that if a breach occurred on January 1, it would take until October 4 of that year to identify and contain the breach. The 277-day average is consistent with the average over the past seven years, with a maximum difference of 11% between the lowest total, 257 days in 2017, and the highest total, 287 days in 2021.

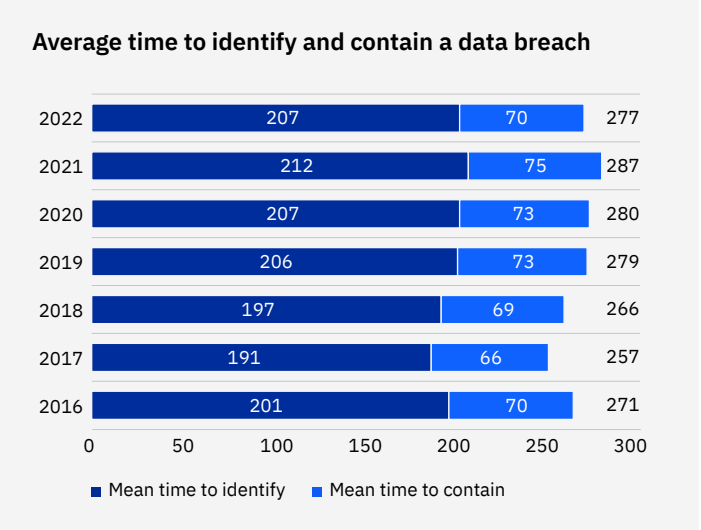


Figure 8: Measured in days

Figure 9: A shorter data breach lifecycle continues to be associated with lower data breach costs.
A data breach lifecycle of less than 200 days was associated with an average cost of USD 3.74 million in 2022, compared to USD 4.86 million for breaches with a lifecycle of greater than 200 days. This difference represents an average cost savings of USD 1.12 million, or 26.5%, for breaches with the shorter than 200-day lifecycle.

The cost gap between a lifecycle longer than 200 days and a lifecycle shorter than 200 days was smaller in 2022 than in 2021, when it was USD 1.26 million. The cost gap in 2022 — USD 1.12 million — is the same size as the cost gap in 2020. The cost gap has grown slightly over the past seven years, while the average cost of a data breach has also grown incrementally. The 2021 cost gap of USD 1.26 million was the largest of the past seven years.

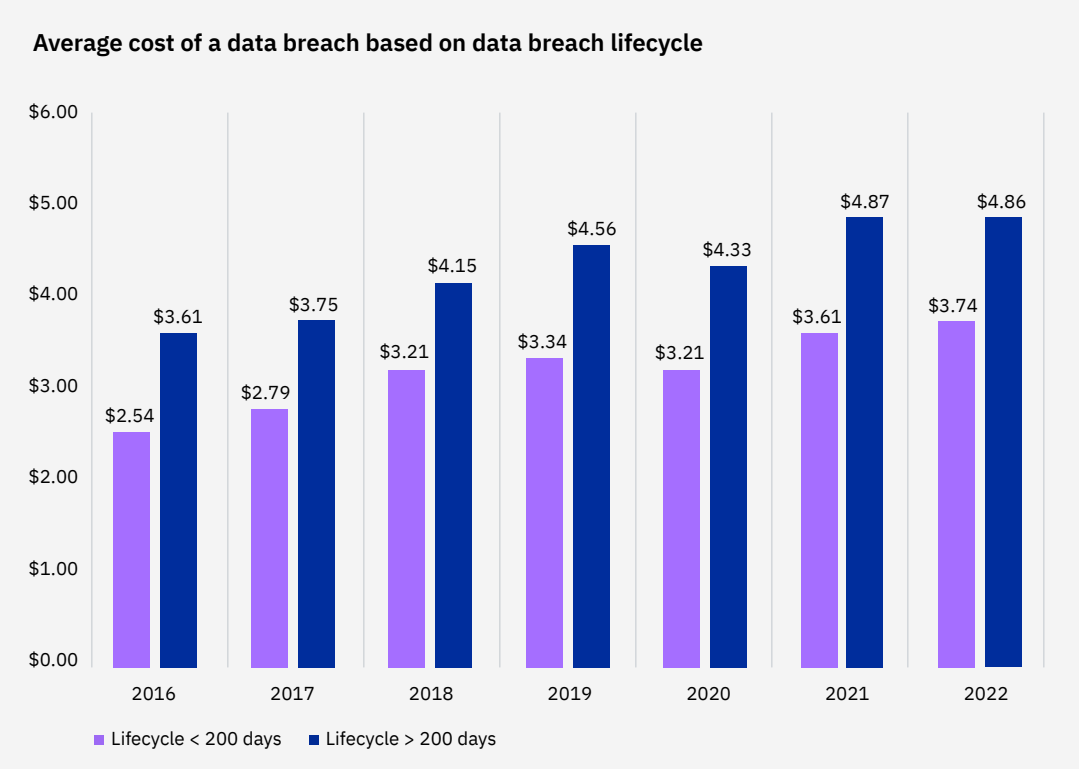


Figure 9: Measured in USD millions. Sum of days to identify and days to contain equals the breach lifecycle.

Figures 10a and 10b: Data breaches in high data protection regulatory environments, such as the healthcare, financial, energy, pharmaceuticals and education industries, tended to see costs accrue in later years following the breach.
The difference between low and high regulatory environments showed up in a pronounced way two years or more after the data breach — the "longtail" costs. In highly regulated industries, an average of 24% of data breach costs were accrued more than two years after the breach occurred. This result compares to an average of 8% of costs accrued more than two years after a breach in low regulatory environments.

In low regulatory environments, data breach costs tended to accrue in the first three to six months — where an average of 24% of data breach costs accrued. In the overall average for 2022, 52% of costs were incurred in the first 12 months, 29% in the second year after the breach and 19% more than two years after the breach. For highly regulated industries, 45% of costs accrued in the first year, 31% in the second year and 24% more than two years after the breach.

In the analysis of industries in the high regulation categories, we concluded that regulatory and legal costs may have contributed to higher costs in the years following a breach.

Note: This analysis was comprised of a subset of 218 companies with historical data from previous breaches.

Time elapsed	Percentage of total cost		
	2022 average	Low	High
1st year	52%	66%	45%
2nd year	29%	26%	31%
2+ years	19%	8%	24%

Figure 10a

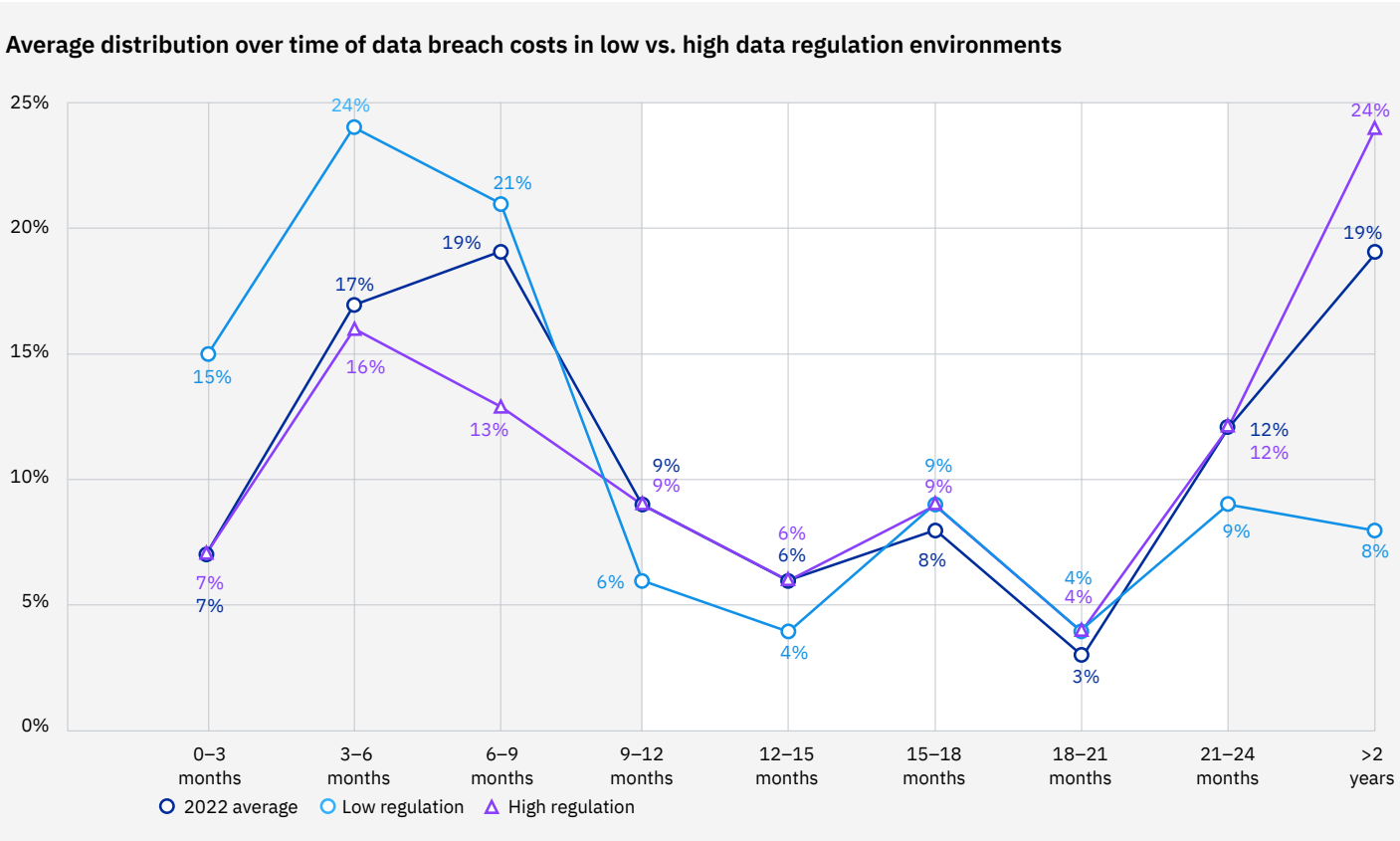


Figure 10b: Percentage of total costs accrued in three-month intervals

USD 4.91 million

Average cost of data breach with a phishing initial attack vector

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 stolen or compromised credentials. This section also compares the average time it takes to identify and contain breaches based on their initial attack vector.

Figure 11: The most common initial attack vector in 2022 was stolen or compromised credentials, responsible for 19% of breaches in the study, at an average cost of USD 4.50 million. In 2022, the most common initial attack vectors were compromised credentials at 19% of breaches, phishing at 16% of breaches, cloud misconfiguration at 15% of breaches and vulnerability in third-party software at 13% of breaches. The 2021 report saw the same order of the top four initial attack vectors.

The costliest initial attack vector in 2022 on average was phishing at USD 4.91 million. Following phishing was business email compromise at USD 4.89 million and 6% of breaches, vulnerability in third-party software at USD 4.55 million and compromised credentials at USD 4.50 million.

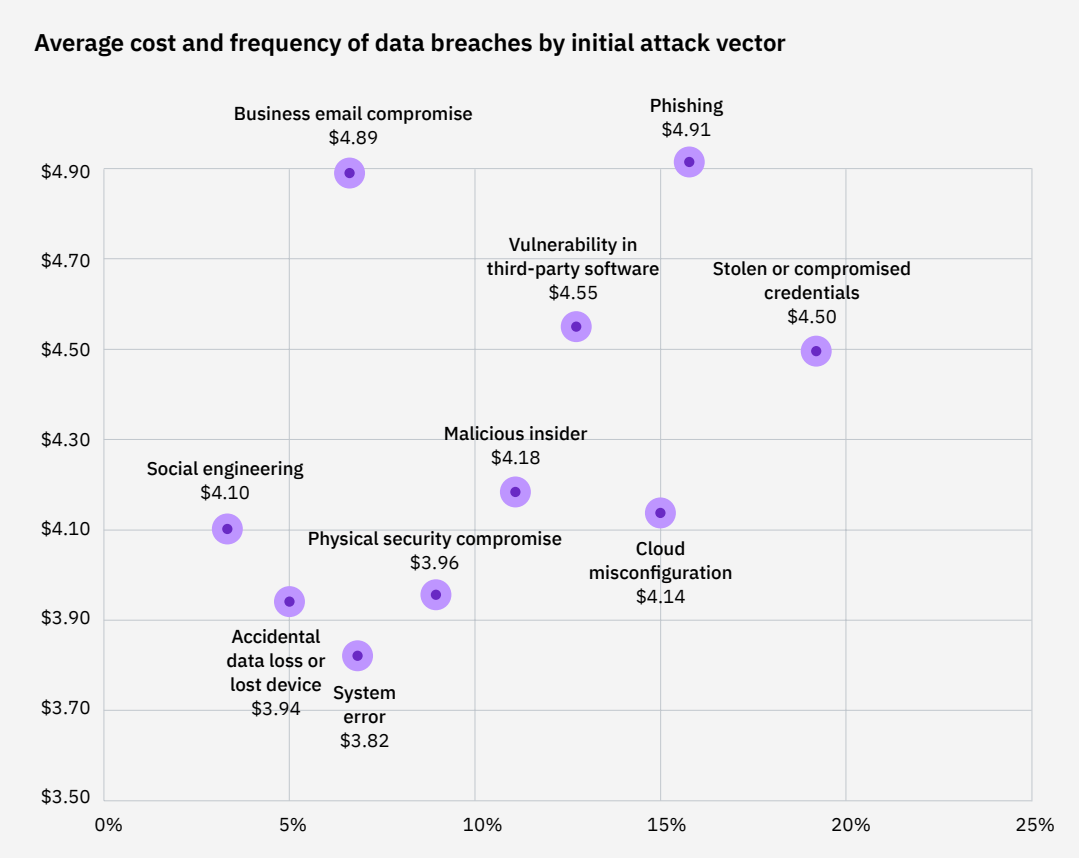


Figure 11: Measured in USD millions

Figure 12: Attack vectors with longer mean times to identify and contain, such as phishing or business email compromise, were also among the most expensive types of breaches. Stolen or compromised credentials were the initial attack vector with the longest mean time to identify and contain the breach, at 327 days. That time is 16.6% greater than the overall mean time to identify and contain a data breach. Compromised credentials were also the most common — 19% — initial attack vector leading to data breaches in the study.

Breaches caused by business email compromise had the second highest mean time to identify and contain, at 308 days. Business email compromise was also the second costliest initial attack vector, with breaches costing an average of USD 4.89 million. Breaches caused by phishing had the third highest mean time to identify and contain, at 295 days, and had the highest average cost by initial attack vector, at USD 4.91 million. Vulnerability in third-party software had the fourth highest mean time to identify and contain a breach, with an average that was above the overall average — 284 days versus 277 days.

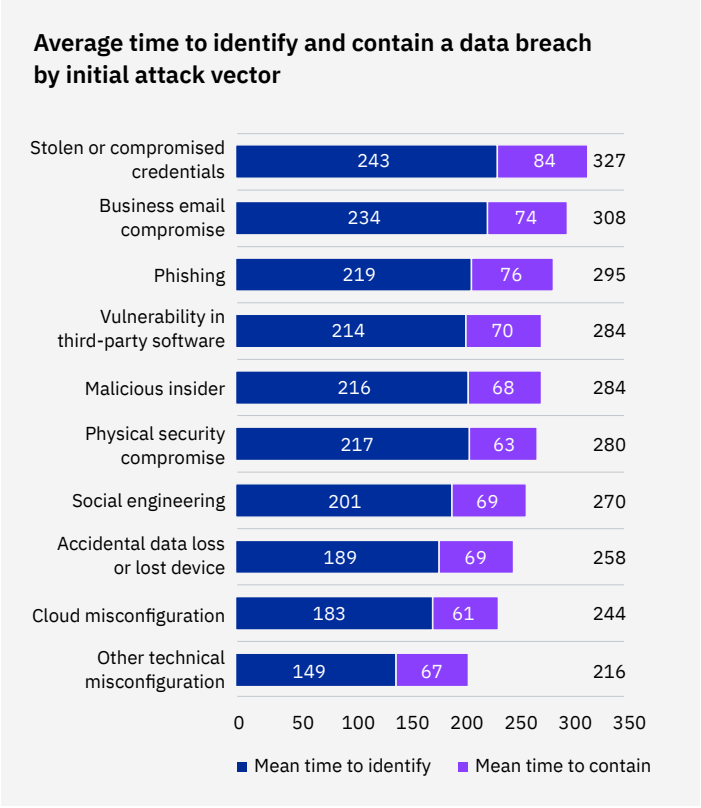


Figure 12: Measured in days

USD 5.57 million

Average cost of a breach for organizations with high levels of compliance failures

Key cost factors

This section looks at a multitude of factors that influence the cost of a data breach, including various types of security technologies and practices. A special analysis of 28 cost factors examines their impact on the mean cost of a data breach. We look at how these 28 factors were associated with either lower-than-average breach costs stemming from a cost mitigating influence, or a higher-than-average cost of a breach resulting from a cost amplifying influence.

The following cost factors are new to the report this year: IAM; XDR technologies; MFA; and crisis management teams.

These cost factors aren't additive, so it's not consistent with this research to add multiple cost factors together to calculate the cost of a breach.

Figure 13 shows the impact of 28 factors on the average cost of a data breach.
The chart shows the average cost difference of breaches at organizations with these cost-influencing factors compared to the mean cost of a data breach of USD 4.35 million. The chart is divided into those factors that are associated with a lower-than-average breach cost, which are cost mitigators, and those factors that are associated with a higher-than-average breach cost, or cost amplifiers.

AI platforms, a DevSecOps approach and use of an incident response (IR) team were the three factors associated with the highest cost decrease compared to the mean cost of a breach. For example, breaches at organizations with AI platforms had an average cost that was USD 300,075 less than the mean cost of a data breach of USD 4.35 million — which is approximately USD 4.05 million.

On the other hand, security system complexity, occurrence of cloud migration when the organization is in the process of migrating to the cloud and compliance failures were the three factors associated with the highest net increase in the average cost. For example, breaches at organizations with security system complexity had an average cost of USD 290,655 more than the mean cost of a data breach of USD 4.35 million — which is approximately USD 4.64 million.

For the first time, this year's report measured the impact of the following four new cost factors: IAM; XDR technologies; MFA; and crisis management teams. Each of these factors was associated with lower-than-average breach costs, led by IAM.

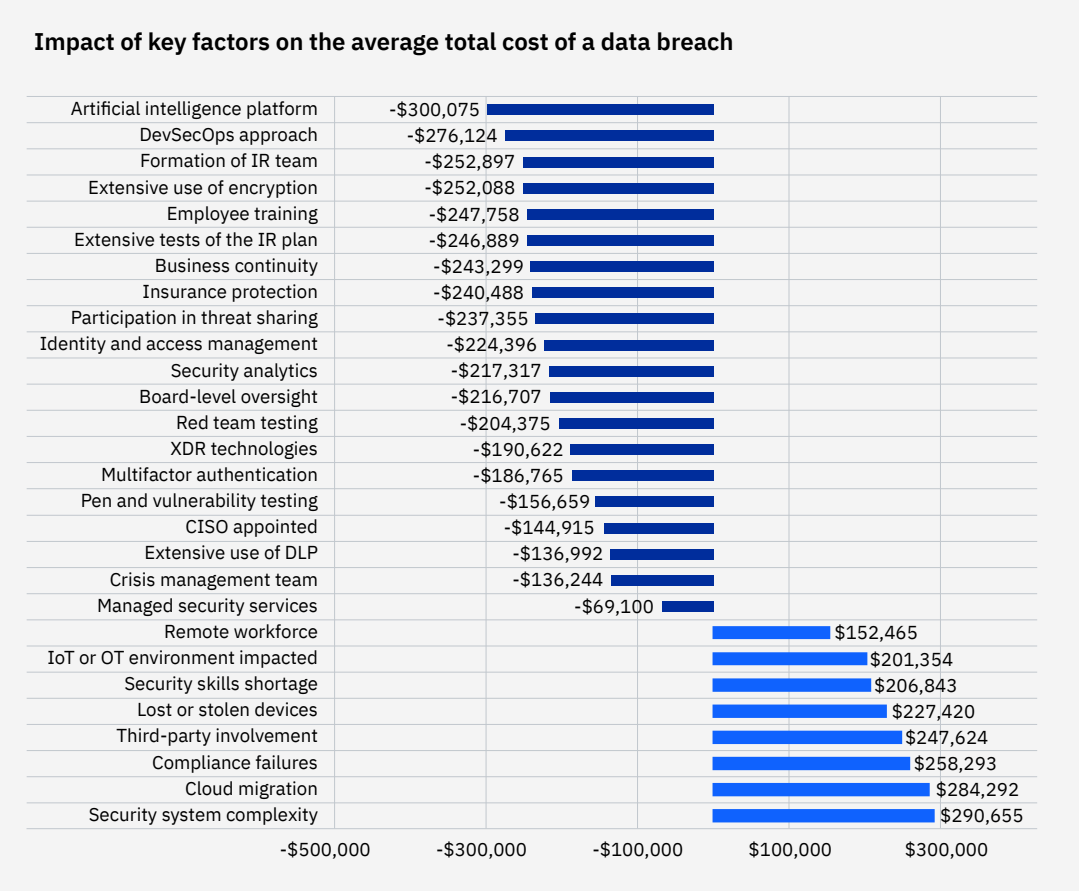


Figure 13: Measured in USD

Figure 14 looks at the three cost factors — out of 28 measured — with the greatest level of impact in potentially amplifying the average cost of a data breach.
This chart compares organizations with a high level of the cost factor to those with a low level of the cost factor. There was a difference of USD 2.47 million, or 58%, between high levels and low levels of security system complexity. A difference of USD 2.27 million, or 50.5%, occurred between high levels and low levels of cloud migration. There was a difference of USD 2.26 million, or 50.9%, between high levels and low levels of compliance failures. These data points showed that having high levels of these cost factors present was also associated with a significantly higher than average cost of a data breach. Organizations with a high level of cloud migration had a USD 5.63 million average cost that was USD 1.28 million higher than the average cost of a data breach, a difference of 25.7%.

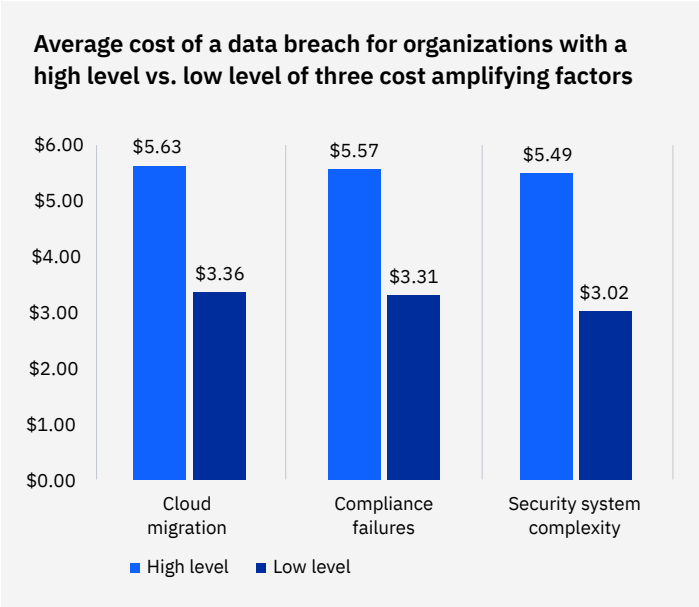


Figure 14: Measured in USD millions

Figure 15 looks at the three cost factors — out of 28 measured — with the greatest level of impact in potentially mitigating the cost of a data breach.
The chart compares organizations with a high level of the cost factor to those with a low level of the cost factor. Those organizations with high levels of use of security platforms that use AI had an average cost of a breach that was USD 2.39 million, or 55.3%, lower than those with low levels of use of an AI platform. Organizations with high levels of use of an IR team had an average cost of a breach that was USD 2.12 million, or 44.9%, lower than those with a low level of use of an IR team. Those organizations with a high level of use of a DevSecOps approach had an average cost of a breach that was USD 1.17 million, or 26.7%, lower than those with a low level of use of DevSecOps. Organizations with high levels of these cost factors present had a significantly lower than average cost of a data breach. Those organizations with high level use of an AI platform had an average cost of USD 3.13 million that was USD 1.22 million lower than the overall average cost of a data breach, a 32.6% difference.

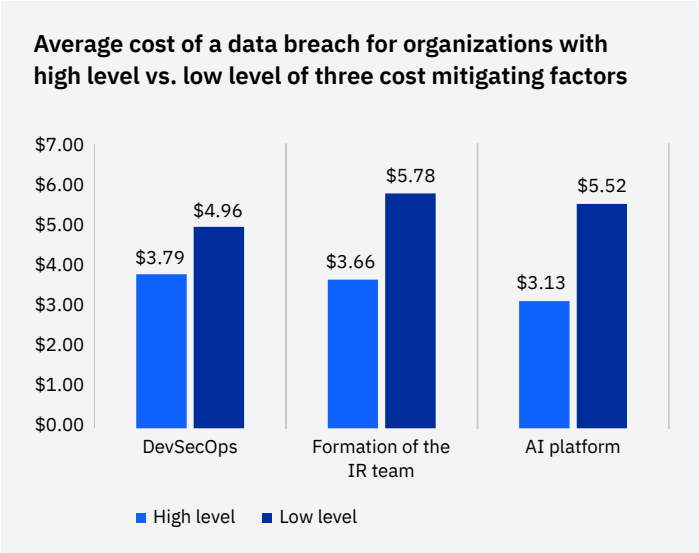


Figure 15: Measured in USD millions

USD 3.05 million

Average savings from fully deployed security AI and automation versus no security AI and automation

Security AI and automation

This was the fifth year we examined the relationship between data breach cost and security AI and automation. In this context, security AI and 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 AI, 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, nonintegrated systems, without data shared between them.

Figure 16: The share of organizations with fully or partially deployed security AI and automation increased by five percentage points, from 65% to 70%, between 2021 and 2022.
Fully deployed security AI and automation increased by six percentage points, from 25% to 31%, between 2021 and 2022 and by 10 percentage points, from 21% to 31%, between 2020 and 2022. The share of organizations with no security AI and automation deployed decreased from 35% in 2021 to 30% in 2022 and has decreased from 41% in 2020, a difference of 11 percentage points.

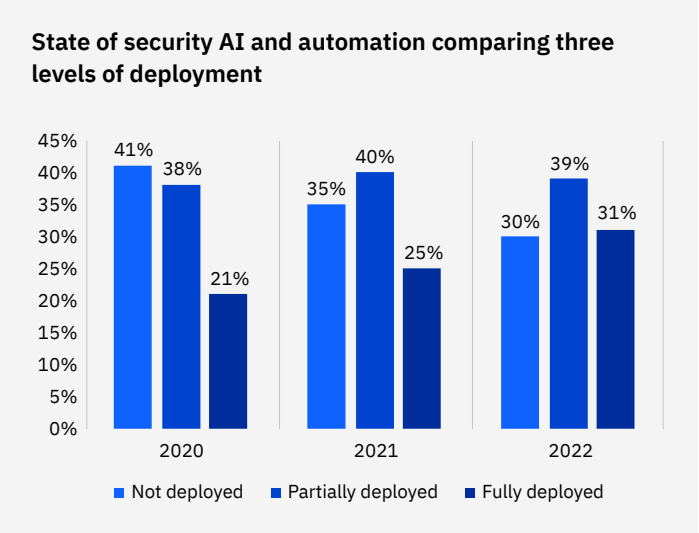


Figure 16: Percentage of organizations per deployment level

Figure 17: Fully deployed security AI and automation was associated with average breach costs that were USD 3.05 million lower than with no security AI and automation deployed, a difference of 65.2%, the largest cost savings in the study.

Organizations with fully deployed security AI and automation had an average total cost of a data breach of USD 3.15 million. This average total cost compared to USD 6.20 million for organizations without security AI and automation deployed. The difference between average cost of a breach with fully deployed security automation and no security AI and automation deployed was smaller in 2022 than in 2021, when the gap was USD 3.81 million, or in 2020, when the savings was USD 3.58 million.

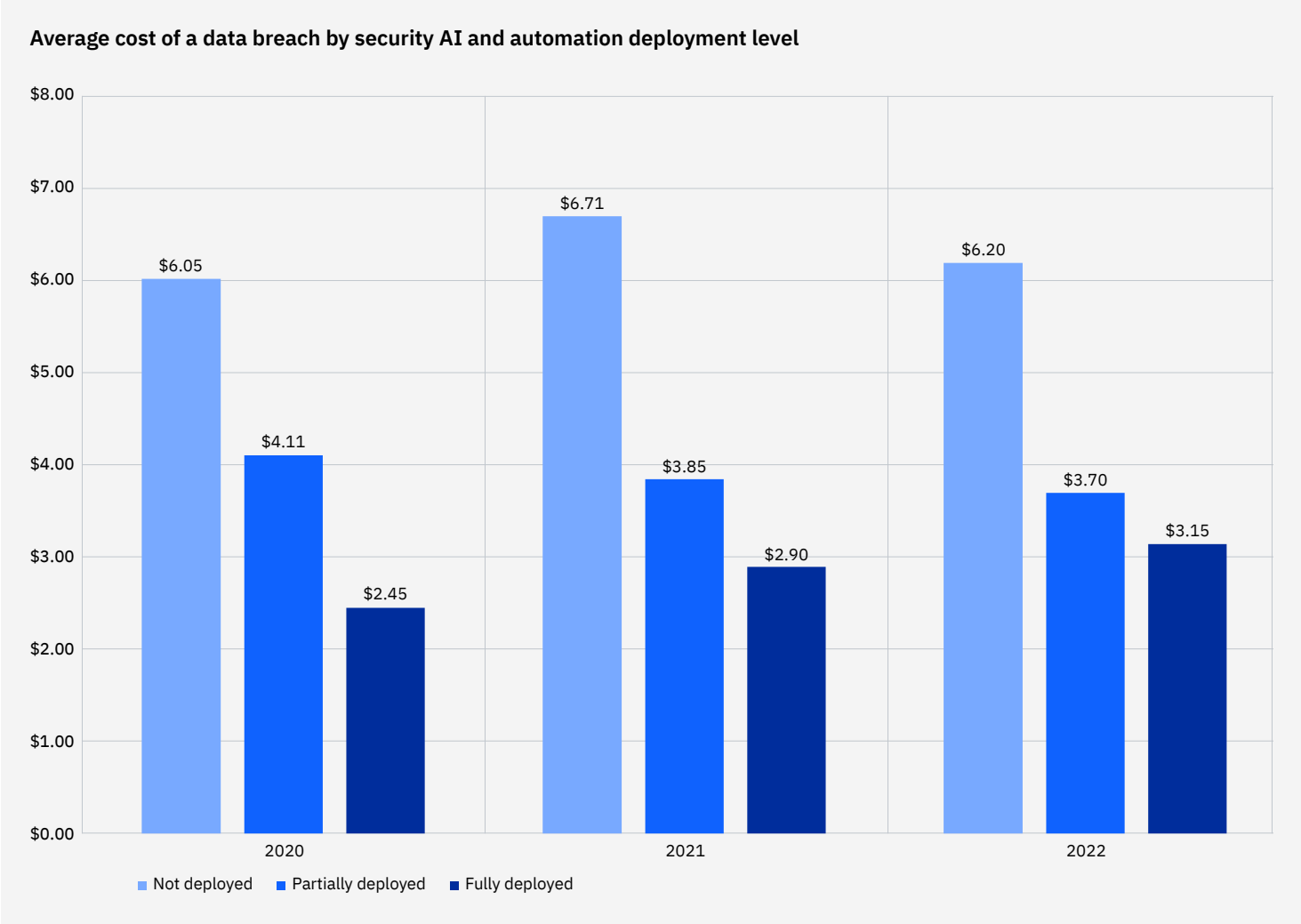


Figure 17: Measured in USD millions

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

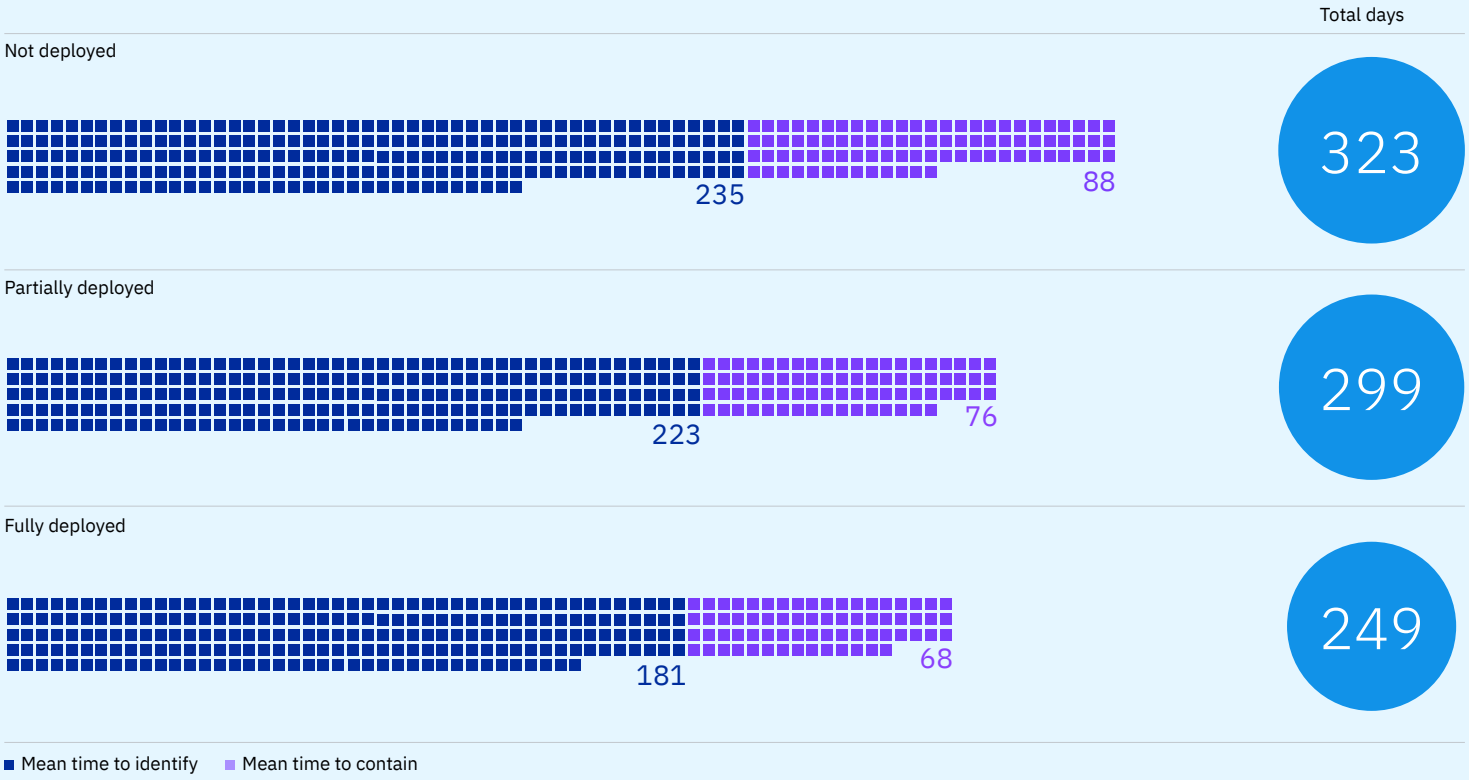


Figure 18: Measured in days

Figure 18: Organizations with fully deployed security AI and automation were able to detect and contain a breach much more quickly than organizations with no security AI and automation deployed.
Organizations with fully deployed security AI and automation took an average of 181 days to identify and 68 days to contain the data breach, for a total lifecycle of 249 days. Those organizations with no security AI and automation deployed took an average 235 days to identify and 88 days to contain a breach, for a total lifecycle of 323 days, which was 74 days longer than organizations with fully deployed security AI and automation. The average time to identify and contain a breach was a total of 299 days with partially deployed security AI and automation.

29 days

Organizations with XDR technologies identified and contained a breach 29 days faster than those without XDR

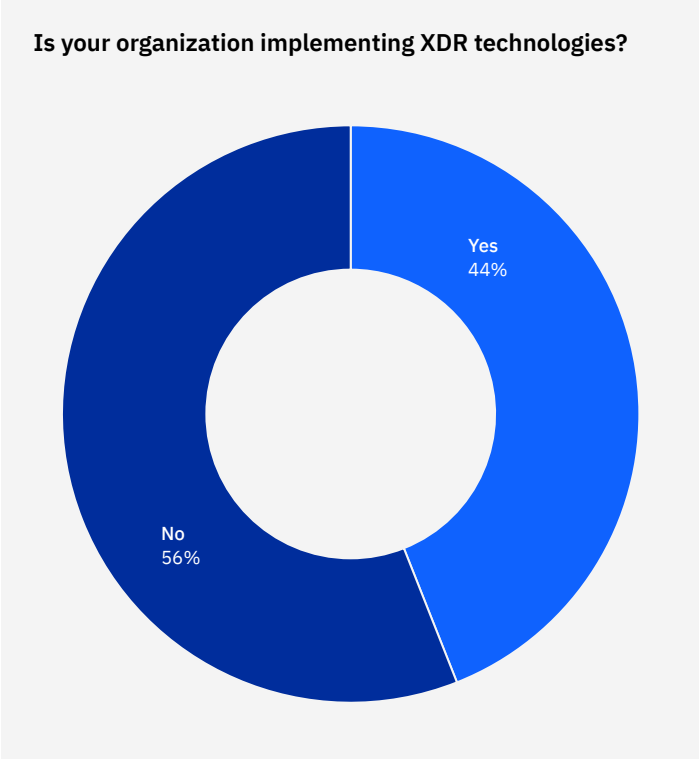


Figure 19

XDR technologies

For the first time, the study examined the effects of XDR technologies on the cost of a data breach. This section looks at the prevalence of XDR in the organizations studied, plus its impact on average total cost and the average time to contain data breaches.

Significantly, XDR impacted average breach costs with a savings of 9.2%. While these savings may appear humble at first sight, the true impact comes in the amount of time organizations saved in breach duration when they use XDR — nearly one month. Extra time to identify and contain a breach can add a lot to the overall cost of a breach and its consequences.

Figure 19: XDR capabilities were commonly used but not yet by a majority of organizations.
According to the survey of 550 organizations in the study, 44% are implementing XDR technologies, while 56% aren't implementing XDR technologies.

Figure 20: The use of XDR technologies was associated with a lower-than-average cost of a data breach.
Those organizations that are implementing XDR technologies experienced an average cost of a data breach of USD 4.15 million. Organizations that weren't implementing XDR technologies experienced an average cost of a data breach of USD 4.55 million. This cost was above the global average and USD 0.40 million more than breaches at organizations implementing XDR technologies, a difference of 9.2%.

Figure 21: The average time to identify and contain a data breach was significantly lower with XDR technologies.
Breaches at organizations with XDR technologies deployed took an average of 275 days to identify and contain the breach, which was 29 days less than breaches at organizations without XDR technologies deployed, at 304 days. That represents a 10% difference in mean time to identify and contain a breach between organizations with XDR technologies and those with no XDR technologies.

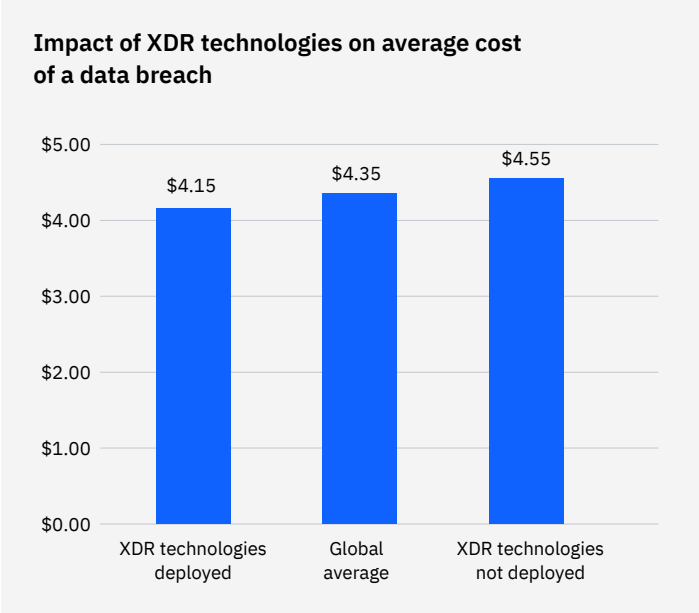


Figure 20: Measured in USD millions

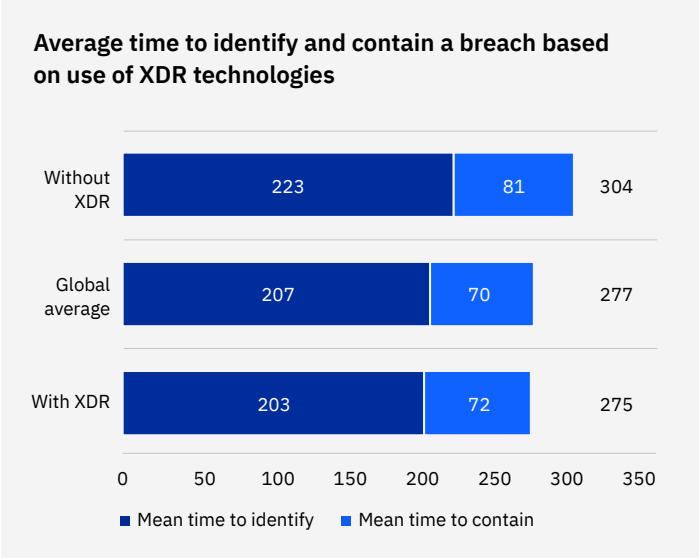


Figure 21: Measured in days

USD 2.66 million

Average breach cost savings at organizations with an IR team that tested an IR plan versus those with no IR team and had not tested an IR plan

Incident response

In previous years, this research has shown that the use of IR teams and testing of an IR plan significantly reduced the average cost of a data breach. In this year's analysis, we again looked at how IR teams, capabilities and processes impacted the cost of a breach.

Figure 22: A majority of organizations in the study had IR plans and testing of IR plans on a regular basis. Nearly three-quarters of organizations in the study said they had an IR plan, with 73% saying they did have an IR plan and 27% saying they didn't have a plan. At organizations with an IR plan, 63% said they regularly tested the IR plan, with 37% saying they didn't regularly test the IR plan.

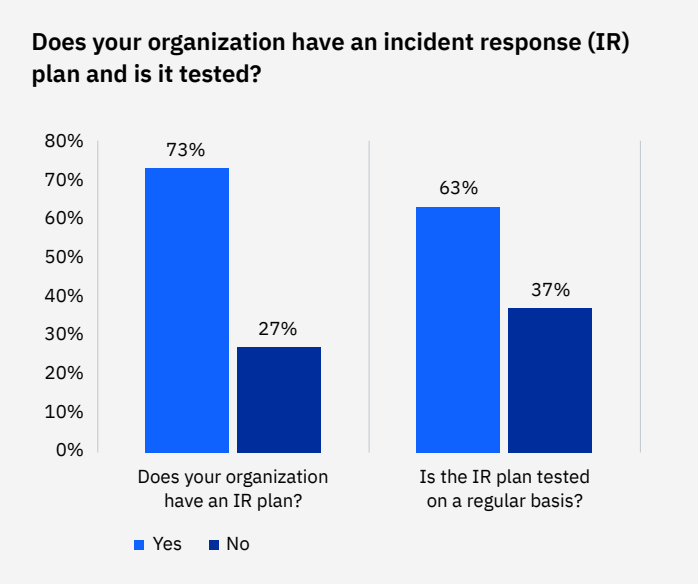


Figure 22

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

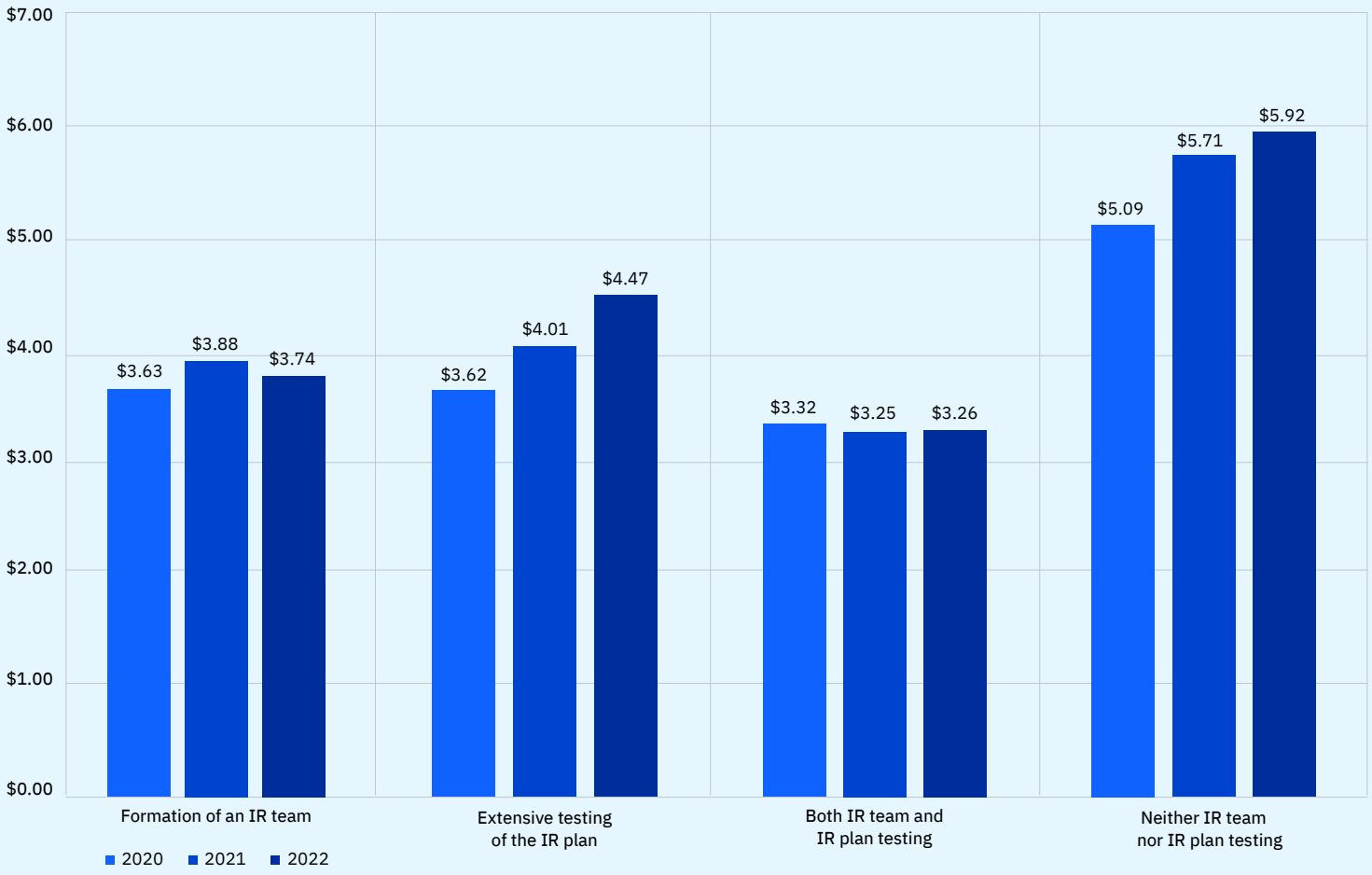


Figure 23: Measured in USD millions

Figure 23: IR teams and extensive IR plan testing continued to mitigate data breach costs in 2022.
The gap between the average data breach cost at organizations with both IR teams and IR plan testing and those with neither IR teams or IR plan testing continued to grow between the 2020 report and the 2022 report. Breaches at organizations with IR capabilities saw an average cost of a breach of USD 3.26 million in 2022, compared to USD 5.92 million at organizations without IR capabilities. This average cost was a difference of USD 2.66 million, or 58%. Those savings were an increase over 2021, when the average cost of a breach at organizations with IR capabilities saved USD 2.46 million, and in 2020, when the cost difference was USD 1.77 million. This finding indicates a growing cost-saving effectiveness of IR capabilities.

USD 2.10 million

Cost savings of breaches at organizations that use risk quantification techniques versus those that don't

Does your organization prioritize risks, threats and impacts based on risk quantification techniques?

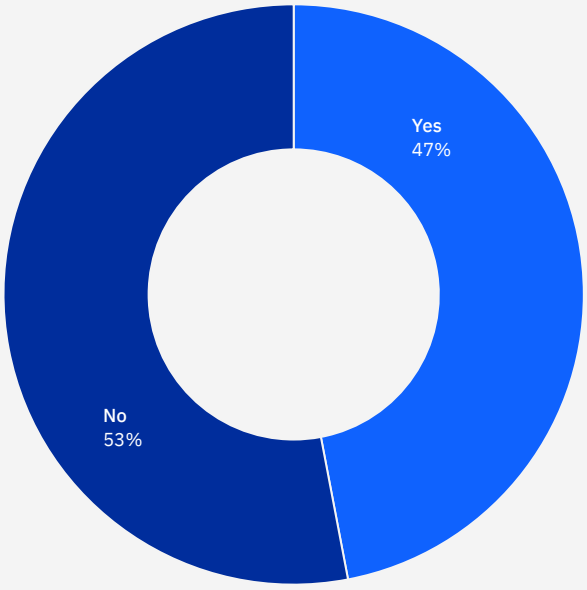


Figure 24

Risk quantification

Risk quantification looks at impacts, including financial impacts, availability of data and data integrity. Using risk quantification can highlight financial loss types by impact, including the following examples: loss of productivity; cost of response or recovery; reputation impact; and fines and judgments.

Chief information security officers (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, can clarify potential security gaps and how to reduce overall risk by quantifying security risk into financial terms.

This section looks at how many organizations are using risk quantification techniques to prioritize risks, threats and impacts and reviews the average cost impact of risk quantification techniques.

Figure 24: Less than half, 47%, said they prioritize risks, threats and impacts based on risk quantification techniques. Meanwhile, out of the 550 organizations studied, 53% don't prioritize risks, threats and impacts based on risk quantification techniques.

Figure 25: Risk quantification had a considerable effect on data breach costs, saving up to USD 2.10 million on average. Organizations that prioritized risks, threats and impacts based on risk quantification techniques had an average breach cost of USD 3.30 million. That cost was USD 2.10 million less than those that didn't use risk quantification, at USD 5.40 million, a savings of 48.3%. Risk quantification was associated with breach costs that were more than USD 1 million lower than the global average of USD 4.35 million.

Impact of risk quantification techniques on average cost of a data breach

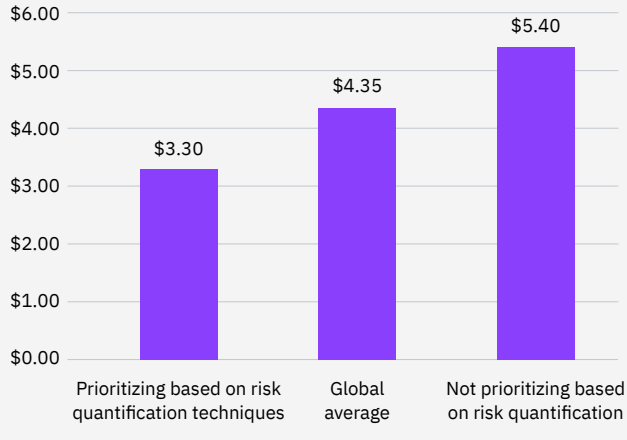


Figure 25: Measured in USD millions

USD 1.51 million

Average breach cost savings associated with a mature zero trust deployment versus early adoption of zero trust

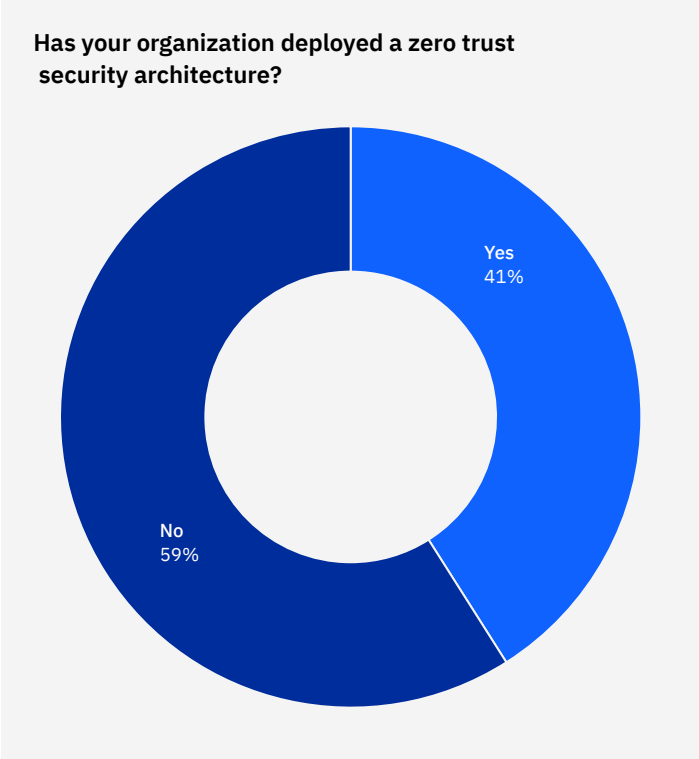


Figure 26

Zero trust

For a second year, this study examined the prevalence and financial impact of data breaches based on deployment of a zero trust security framework. The zero trust 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. As the data in this section shows, zero trust has a net positive impact on data breach costs.

Figure 26: In the 2022 study, 41% of organizations said they have deployed a zero trust security architecture, while 59% said they haven't.
This finding compares to the 2021 report when 35% said they had partially or fully deployed a zero trust architecture.

Figure 27: Organizations with zero trust deployed saved nearly USD 1 million in average breach costs compared to organizations without zero trust deployed.
The average cost of a data breach was USD 4.15 million at organizations with zero trust deployed, while the cost of a breach was an average USD 5.10 million at organizations without zero trust deployed. The difference was USD 0.95 million, representing a 20.5% savings for organizations with zero trust deployed.

Figure 28: Having a mature zero trust deployment was associated with breach costs that were more than USD 1.5 million lower than breaches at organizations with early adoption of zero trust.
Organizations with mature stage deployment of their zero trust security architecture, when zero trust is applied consistently across all domains, had an average data breach cost of USD 3.45 million. In midstage, when zero trust was applied in many areas of the organization, the average cost of a data breach was USD 3.96 million. For early adoption stage organizations that were beginning to implement a few practices, the average cost of a data breach was USD 4.96 million. This cost was USD 1.51 million more than breaches at mature organizations, a difference of 35.9%.

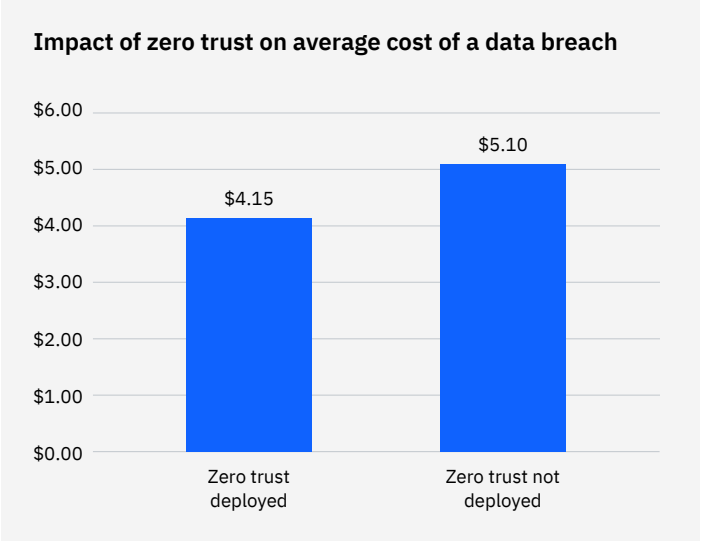


Figure 27: Measured in USD millions

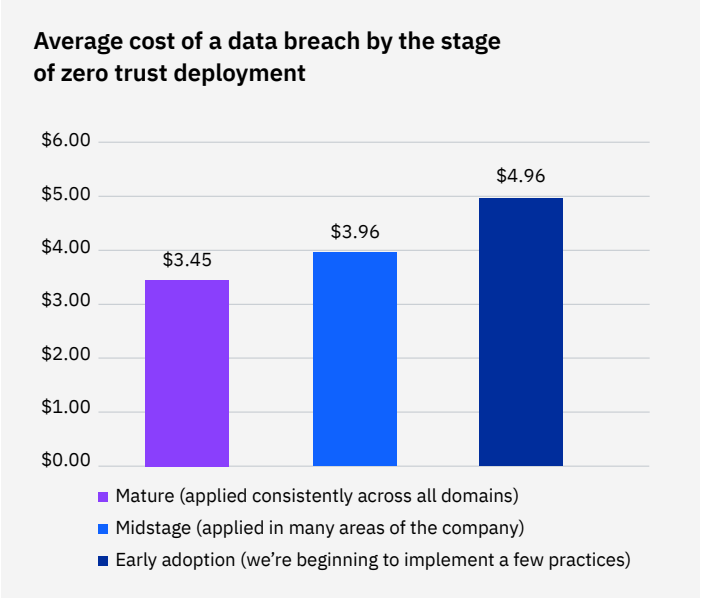


Figure 28: Measured in USD millions

49 days

Ransomware breaches took 49 days longer than average to identify and contain.

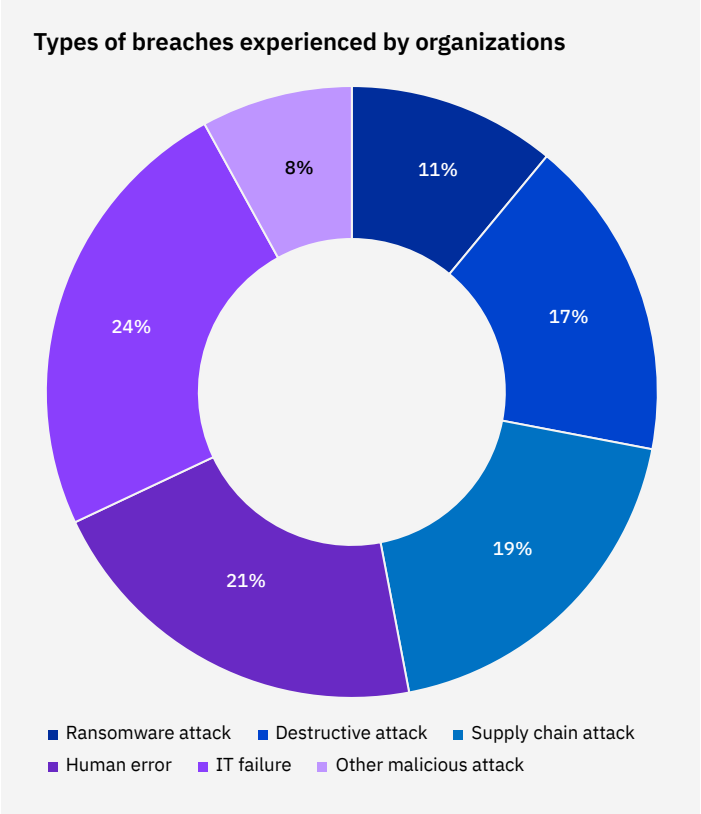


Figure 29

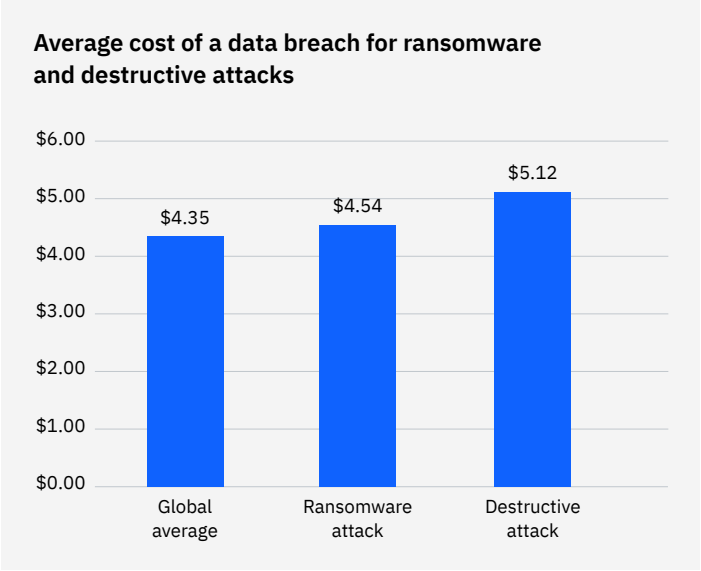


Figure 30: Measured in USD millions

Ransomware and destructive attacks

This was the second year that we examined the cost of ransomware and breaches. We also added destructive malware breaches to this year's study. Compared to last year, ransomware breach costs have declined slightly, from USD 4.62 million to USD 4.54 million. However, the frequency of ransomware breaches has increased — from 7.8% of breaches in the 2021 report to 11% in the 2022 study.

This year we looked at the lifecycle of these breaches, as well as what impact paying a ransom had on the non-ransom cost of the breach. Note: This study doesn't include the cost of the ransom itself in calculating the cost of a ransomware attack.

Figure 29: Ransomware was responsible for 11% of breaches, while destructive attacks were responsible for 17% of breaches.
Another 19% of breaches were caused by supply chain attacks, which were breaches caused due to a business partner being initially compromised. Human errors, meaning breaches caused unintentionally through negligent actions of employees or contractors, were responsible for 21% of breaches.

IT failures, which were caused by a disruption or failure in an organization's computer systems that led to data loss, were responsible for 24% of breaches. Such failures included errors in source code, or a process failure such as automated communication errors. The remaining 8% of breaches were other malicious attacks.

Figure 30: The average cost of a ransomware attack — not including the cost of the ransom itself — was USD 4.54 million, slightly higher than the overall average total cost of a data breach of USD 4.35 million.
The average cost of a destructive or wiper attack was USD 5.12 million, which was USD 0.77 million more than the overall average, a difference of 16.3%.

Figure 31: The average time to identify and contain a ransomware or destructive attack was significantly higher than average.
A ransomware attack took 237 days to identify and 89 days to contain, for a total lifecycle of 326 days. A destructive attack took 233 days to identify and 91 days to contain, for a total lifecycle of 324 days. Compared to the overall average lifecycle of 277 days, organizations took 49 days longer to identify and contain a ransomware attack, a difference of 16.3%. Additionally, organizations took 47 days longer to identify and contain a destructive attack, a difference of 15.6%.

Figure 32: The average cost of a ransomware breach was higher for those that didn't pay the ransom.
The cost of the ransom wasn't included in the calculation of the cost of a ransomware breach. A ransomware breach's cost was based on activities, such as detection of the attack and loss of business due to system downtime. For those organizations that didn't pay the ransom, the average cost of the breach was USD 5.12 million. For organizations that did pay the ransom, the cost of the breach was USD 4.49 million. The difference in average cost was USD 0.63 million, or 13.1%.

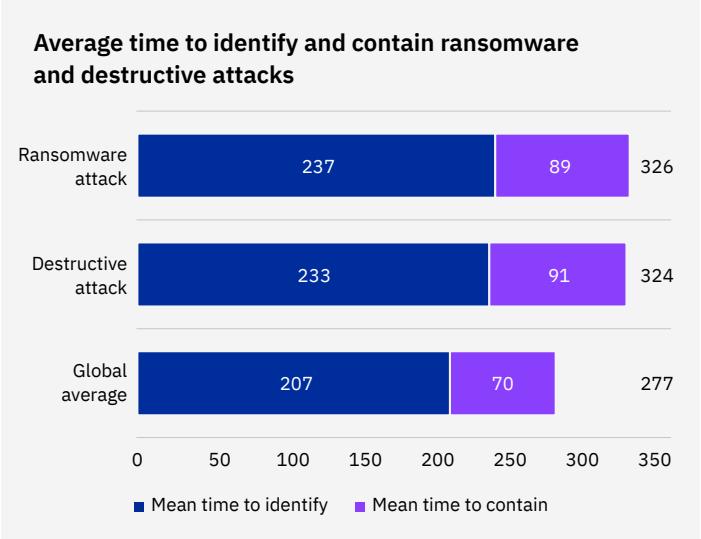


Figure 31: Measured in days

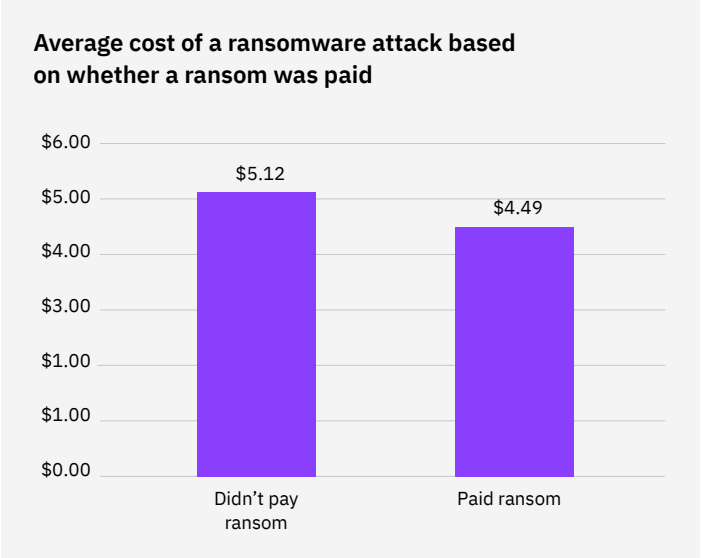


Figure 32: Measured in USD millions. Cost of ransom isn't included in this calculation.

26 days

A supply chain breach took on average 26 days longer to identify and contain than the global average

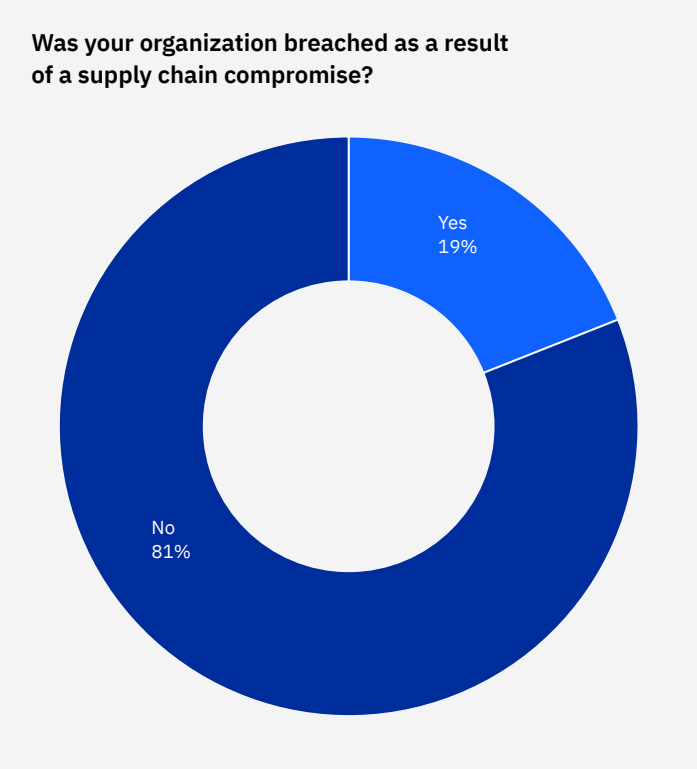


Figure 33

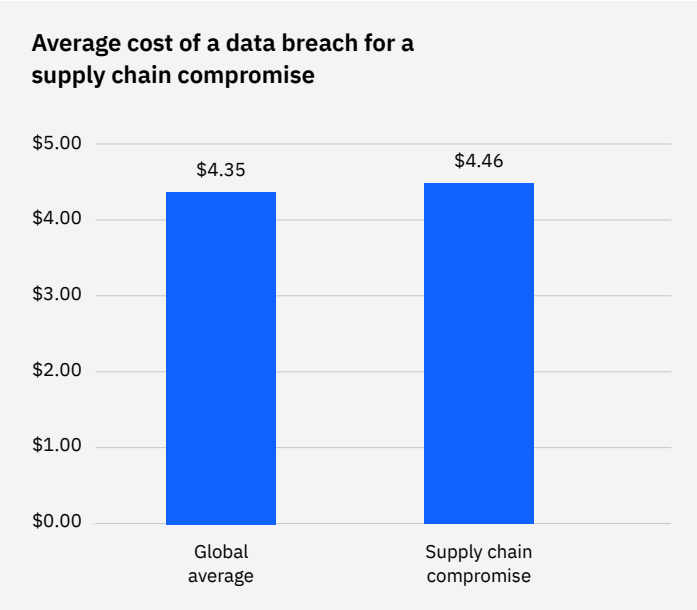


Figure 34: Measured in USD millions

Supply chain attacks

With a number of major supply chain attacks taking place in recent years, this year's report marked the first year that we examined data breaches in the context of supply chain attacks. A supply chain compromise is a breach resulting from a compromise of a business partner such as a supplier. As the research found, nearly one-fifth of breaches were caused by a supply chain compromise, and these compromises made breaches more expensive and resulted in longer lifecycles.

Figure 33: About one-fifth of breaches in the study were the result of a supply chain compromise.
Nineteen percent of organizations said yes, they were breached as a result of a supply chain compromise, and 81% said no.

Figure 34: The average total cost of a supply chain compromise was USD 4.46 million.
That cost was greater than the overall average cost of a data breach of USD 4.35 million, a difference of USD 0.11 million or 2.5%.

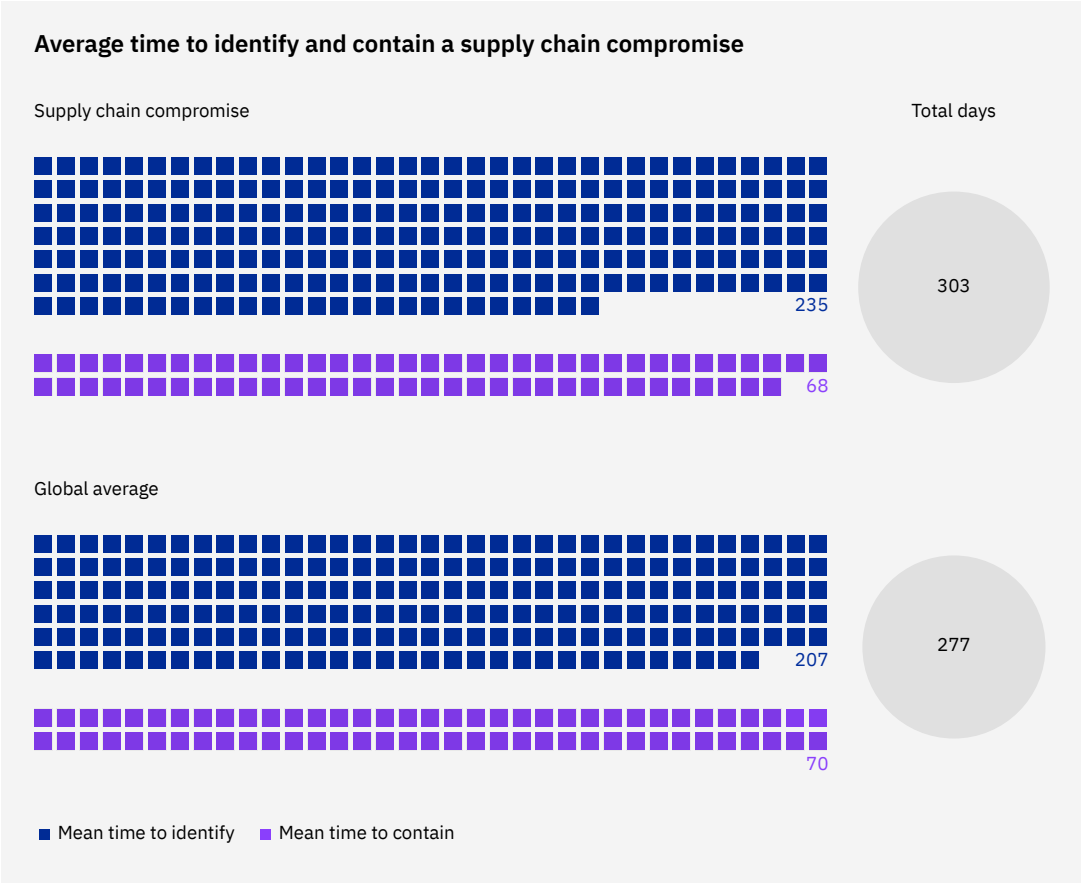


Figure 35: Measured in days

Figure 35: A supply chain compromise had a longer lifecycle than the global average.
Organizations took an average of 235 days to identify and 68 days to contain a supply chain compromise, for a total lifecycle of 303 days. The average lifecycle was 26 days longer than the overall average data breach lifecycle of 277 days, a difference of 9%.

79%

Share of critical infrastructure industries that didn't adopt a zero trust security approach

Critical infrastructure

This report marked the first year that we studied the cost and containment of data breaches in the context of critical infrastructure industries. Based on classification by the US Cybersecurity and Infrastructure Security Agency (CISA), critical infrastructure industries in this study included financial services, industrial, technology, energy, transportation, communication, healthcare, education and public sector.

One revelation of this analysis was that critical infrastructure industries had a much lower prevalence of zero trust security approaches than the global average. Critical infrastructure industries without zero trust strategies deployed had significantly higher data breach costs than average.

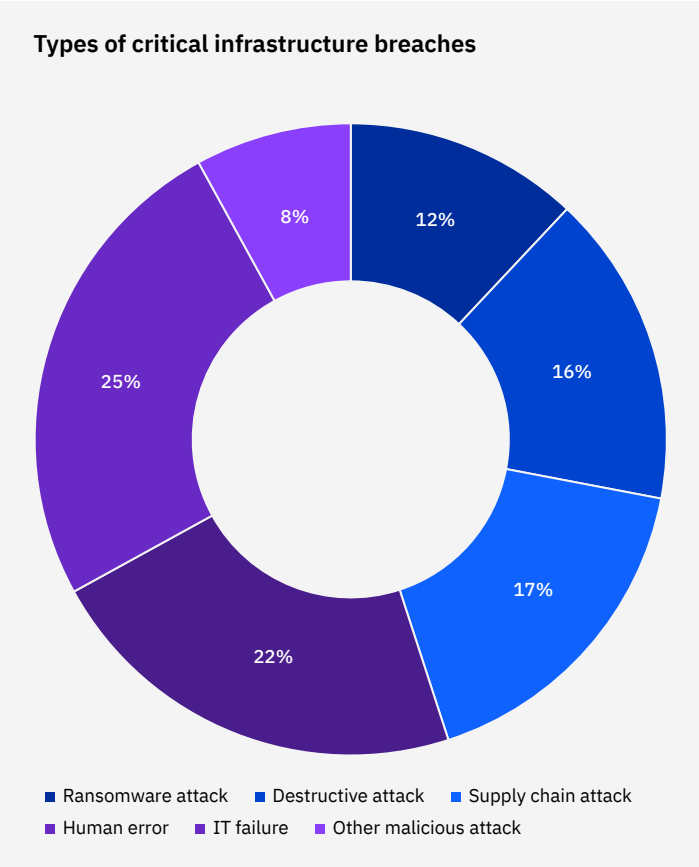


Figure 36

Figure 36: Ransomware and destructive attacks were responsible for more than a quarter of breaches in critical infrastructure industries.
Ransomware attacks accounted for 12% of critical infrastructure breaches, while destructive attacks were behind 16% of critical infrastructure breaches, for a combined 28%. Another 17% of breaches on these industries were supply chain attacks where a third-party business partner was the attack vector. Meanwhile, breaches caused by human error or IT failures accounted for 22% and 25%, respectively. The remaining 8% of critical infrastructure breaches were other malicious attacks.

Figure 37: The average cost of a data breach in critical infrastructure organizations was USD 4.82 million.
Critical infrastructure organizations had an average cost of a data breach USD 0.99 million higher than USD 3.83 million for organizations in noncritical infrastructure industries, a difference of 22.9%. Noncritical infrastructure industries included those organizations in pharmaceuticals, services, entertainment, consumer goods, media, hospitality, retail and research.

Figure 38: Critical infrastructure industries identified and contained data breaches more quickly than other industries.
The lifecycle of a data breach in critical infrastructure industries took fewer days than the global average or noncritical infrastructure industries. The mean time to identify in critical infrastructure industries was 204 days, compared to 211 days for other industries. The mean time to contain for critical infrastructure industries was 69 days, compared to 71 days for other industries. The combined average of 273 days to identify and contain a breach in critical infrastructure was four days shorter than the overall global average of 277 days. Additionally, the combined average for critical infrastructure industries was nine days shorter than the 282 days average for other industries.

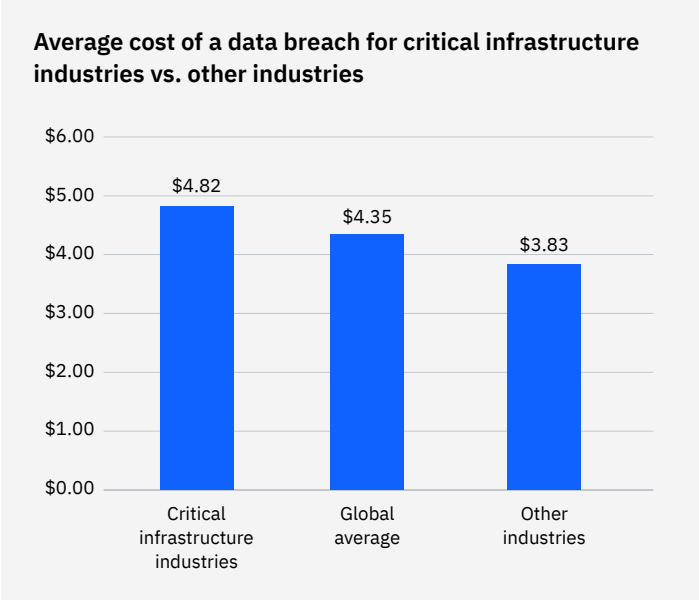


Figure 37: Measured in USD millions

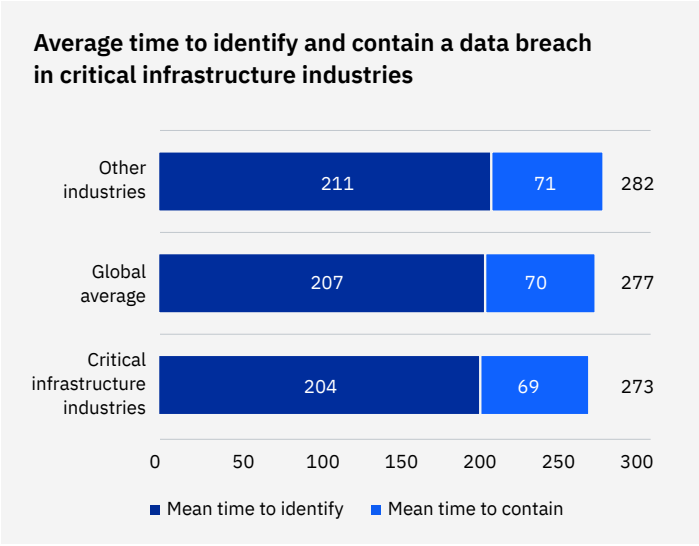


Figure 38: Measured in days

Figure 39: Only one-fifth of critical infrastructure organizations had deployed a zero trust approach to security — half as many as the overall global average.
Twenty-one percent of critical infrastructure organizations had deployed a zero trust approach, while 79% had not. That percentage compares to the overall global average of 41% of organizations with a zero trust strategy.

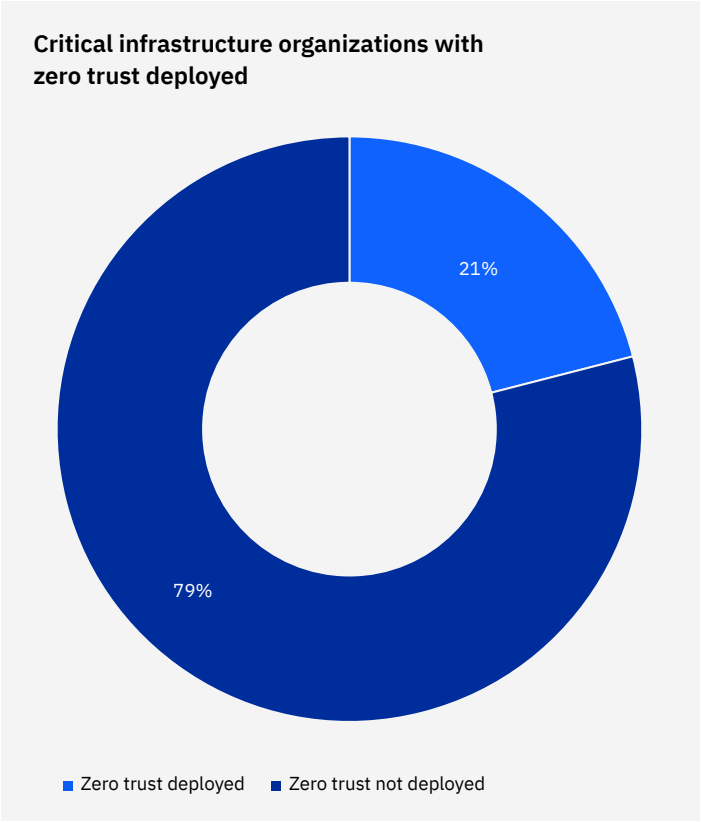


Figure 39

Figure 40: Organizations in critical infrastructure industries that implemented a zero trust approach to security had an average cost of a data breach of USD 4.23 million.
At those critical infrastructure organizations that didn't deploy a zero trust approach, the average cost of a breach was USD 5.40 million. The result was a difference of USD 1.17 million, or 24.3%, more than those that did implement a zero trust strategy.

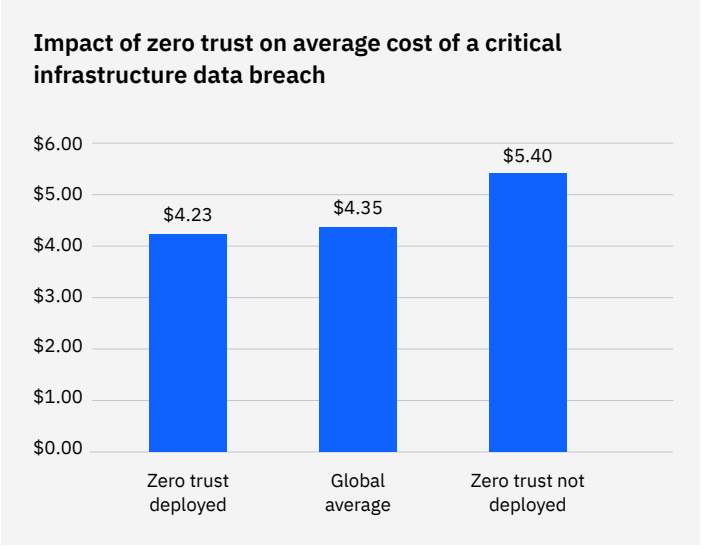


Figure 40: Measured in USD millions

43%

Share of organizations that were in early stages or had not started applying security practices to safeguard their cloud environments

Cloud breaches and cloud model

For a second year in this report, we've taken a close look at the impact of cloud model and maturity of cloud security on the cost of a data breach. The research found that 45% of breaches occurred in the cloud, but those in the public cloud cost considerably more than breaches at organizations with a hybrid cloud model. However, analysis of the research also shows that organizations still need a mature cloud security posture, regardless of cloud model.

Figure 41: A plurality of study participants had a hybrid cloud IT operating model, with 45% indicating they had a hybrid cloud model.
Meanwhile, 28% said their IT model was fully on-premises, and 27% said their IT model was completely cloud-based.

Figure 42: Nearly half of organizations experienced a data breach in the cloud.
Forty-five percent said the data breach occurred in the cloud, whereas 55% said the data breach didn't occur in the cloud.

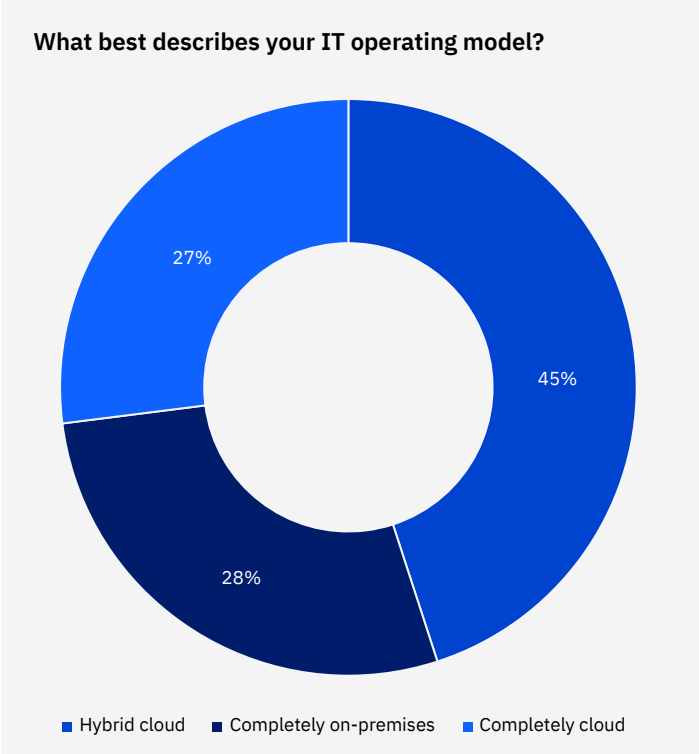


Figure 41

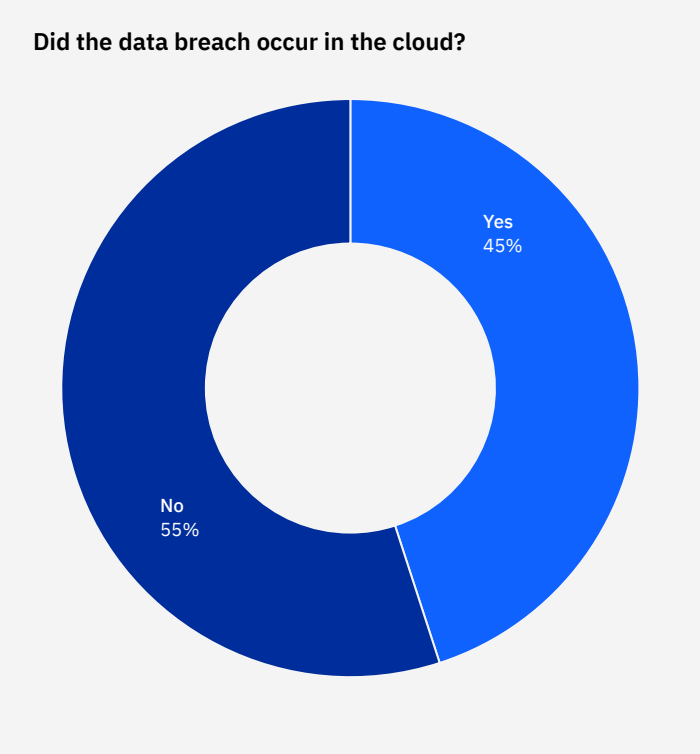


Figure 42

State of security maturity in the cloud environment

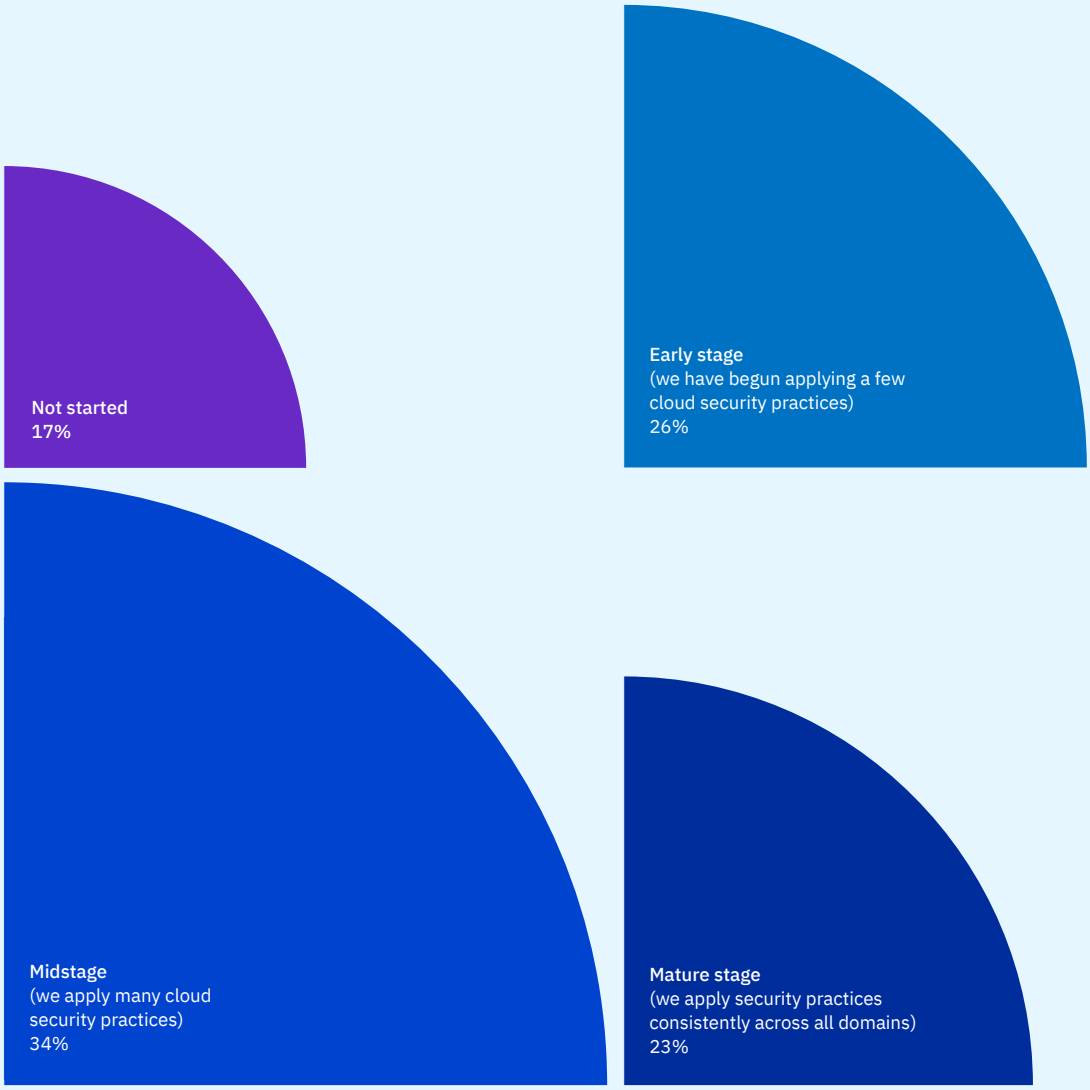


Figure 43

Figure 43: Nearly half, or 43%, of organizations had not started or were in early stages of applying practices to secure their cloud environments.
Meanwhile, 34% were at the midstage and were applying many cloud security practices, and 23% were in the mature stage and were applying security practices consistently across all domains. Another 26% of organizations said that they were in the early stage, meaning that they had begun applying a few cloud security practices. Finally, 17% of organizations said that they had not started their journey in securing their cloud environments.

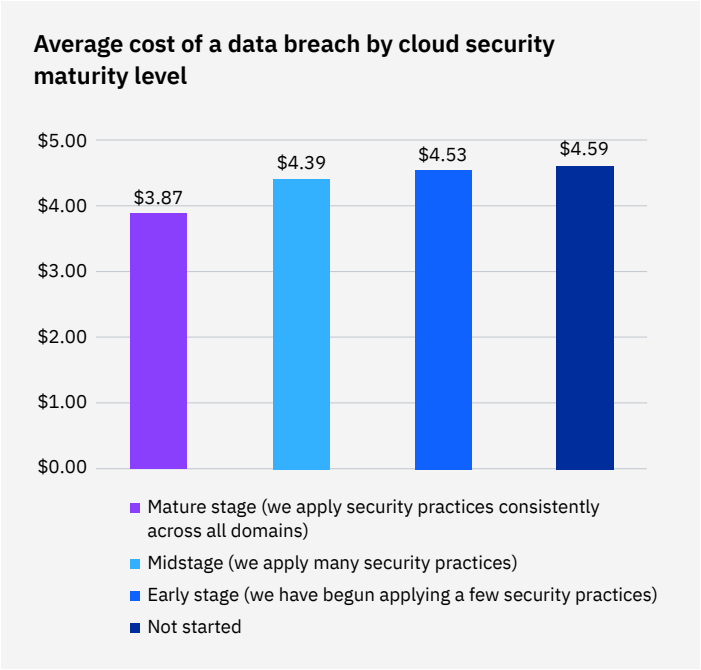


Figure 44: Measured in USD millions

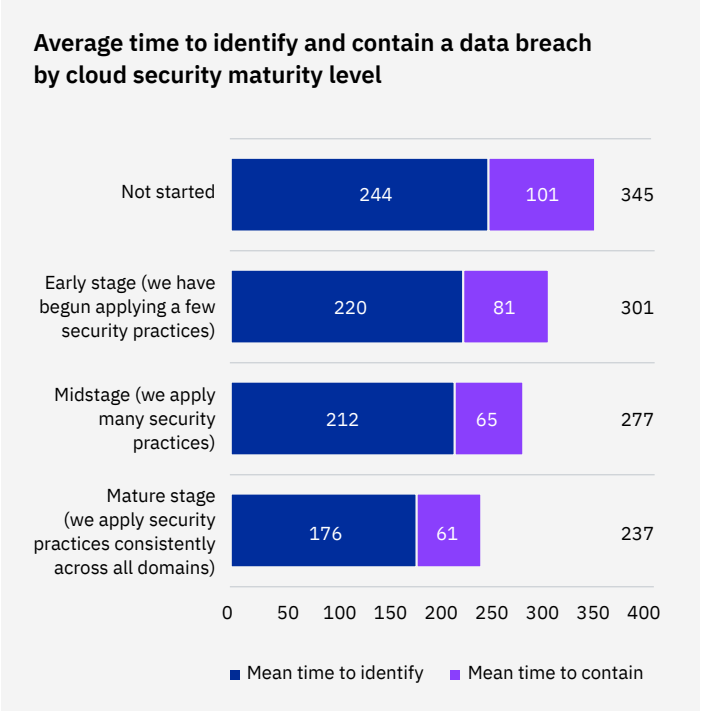


Figure 45: Measured in days

Figure 44: Organizations with mature cloud security had a lower-than-average cost of a data breach.
At mature organizations, breach costs were on average USD 0.66 million less than organizations in the early stages of securing their cloud environments. Breaches at mature-stage organizations cost an average of USD 3.87 million, compared to USD 4.39 million at midstage organizations, USD 4.53 million at early-stage organizations and USD 4.59 million at organizations that had not started their cloud security journey. The cost difference between mature stage and early stage represented a 15.7% savings for mature stage organizations. Note: Breach costs in this analysis refer to any type of breach, not just cloud-based breaches.

Figure 45: Organizations in the mature stage of securing their cloud environments were able to identify and contain the data breach much more quickly than organizations in the early stage.
Mature stage organizations took an average of 176 days to identify and 61 days to contain a breach, or 237 days combined. This lifecycle was 40 days less than the global average of 277 days and 64 days less than early-stage organizations — more than two months, or a 23.8% difference. Those organizations who had not started their cloud security journey took much longer to identify and contain the breach. The average for those organizations was 345 days, more than 100 days longer than mature-stage organizations. For midstage organizations, the average time to identify and contain the data breach was 277 days, the same as the overall global average.

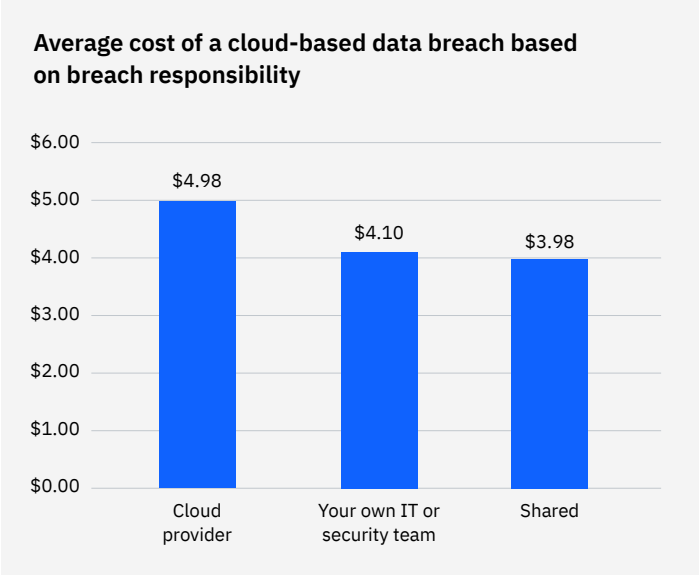


Figure 46: Measured in USD millions

Figure 46: Breaches that were deemed the responsibility of the cloud provider had the highest average total cost of a breach based on cloud provider.
Breaches that were the responsibility of the cloud provider had an average total cost of USD 4.98 million. Breaches deemed the responsibility of the organization's own IT or security team cost an average of USD 4.10 million. Those breaches that were the shared responsibility of the cloud provider and the organization's IT or security team cost an average of USD 3.98 million. This shared responsibility average cost is USD 1 million less than for those breaches where the cloud provider had responsibility, a difference of 22.3%.

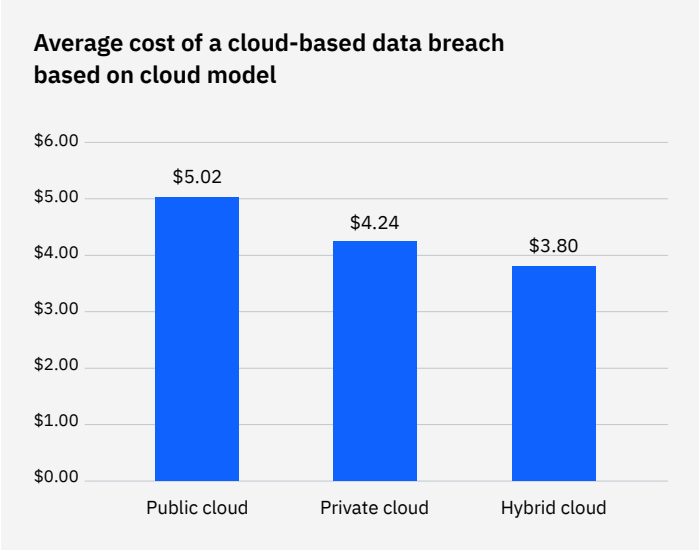


Figure 47: Measured in USD millions

Figure 47: Breaches in the public cloud were costliest.
Breaches in a public cloud cost an average USD 5.02 million, whereas breaches within a private cloud cost an average USD 4.24 million. Within a hybrid cloud model, breaches cost an average USD 3.80 million, about USD 1.2 million less costly than breaches within a public cloud, for a difference of 27.7%.

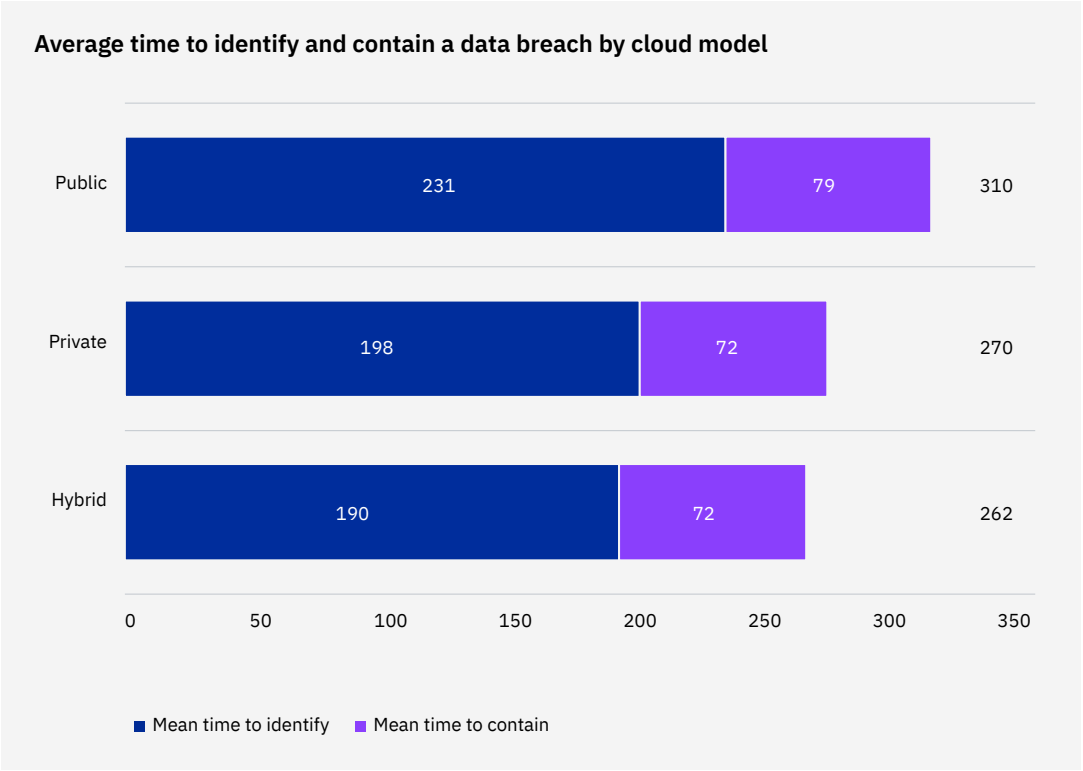


Figure 48: Measured in days

Figure 48: Organizations with a hybrid cloud model were able to identify and contain a breach significantly faster on average than those with public or private cloud models.
The average time to identify and contain a breach with a hybrid cloud model was 262 days. This lifecycle was 15 days less than the global average of 277 days and eight days less than private cloud. Breaches at organizations with a public cloud model took an average of 310 days to identify and contain the breach. This lifecycle was 48 days longer than hybrid cloud, or a difference of 16.8%. Note: Since hybrid cloud implementations vary, this analysis included on-premises breaches, not just purely cloud-based breaches.

USD 1 million

Breach costs where remote working was a factor in causing the breach were about USD 1 million more than breaches where remote work wasn't a factor

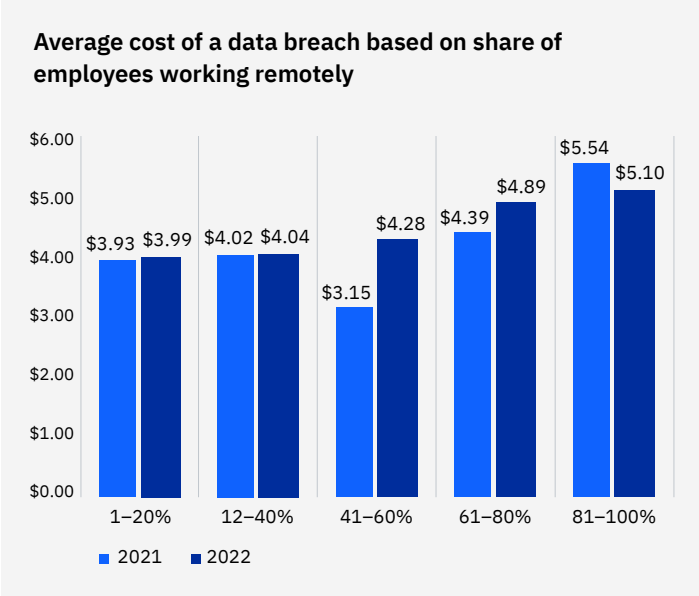


Figure 49: Measured in USD millions

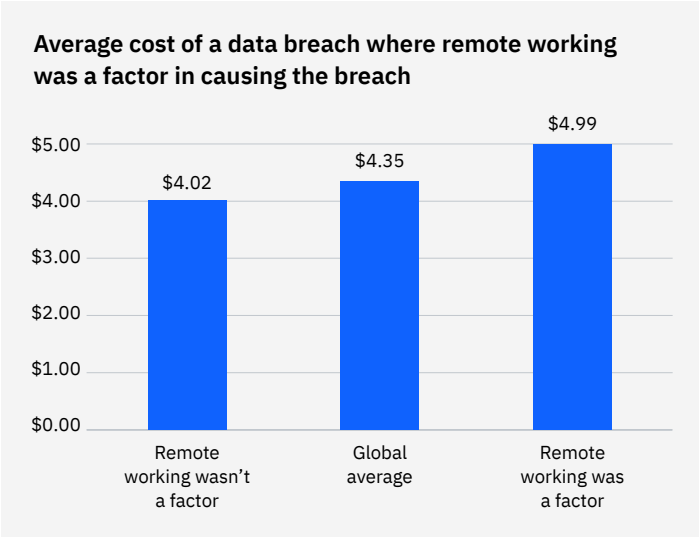


Figure 50: Measured in USD millions

Remote work

This is the third time this report has been published since the start of the COVID-19 pandemic. In the context of the pandemic, starting with last year's report, we've examined the impacts of work-from-home arrangements on data breach costs. Remote working has had considerable effects on the cost of a breach when remote work was a factor in causing the breach, such as a remote-working employee having credentials stolen. The study also found that breach costs were highest for organizations with most of their employees working remotely.

Figure 49: There was a strong correlation between remote working and cost of a data breach, where more employees working remotely was associated with higher data breach costs.
For those organizations with the largest share of employees working remotely — 81% to 100% — the average cost of a data breach was USD 5.10 million. That cost was a slight decrease in this category from last year. For organizations with the smallest share of employees working remotely — less than 20% — the average cost was USD 3.99 million. The difference between highest and lowest share of employees working remotely was USD 1.11 million, a difference of 24.4%.

Figure 50: The average total cost of a data breach was nearly USD 1 million greater when remote work was a factor in causing the data breach.
Organizations that indicated remote work was a factor in the breach experienced an average cost of a data breach of USD 4.99 million. In contrast, the average cost of a data breach was USD 4.02 million when remote work wasn't a factor in causing the breach, a difference of USD 0.97 million or 21.5%. When remote work was a factor, the cost was also USD 0.64 million more than the overall global average, a difference of 13.7%.

USD 550,000

Average data breach cost savings of a sufficiently staffed organization versus insufficiently staffed

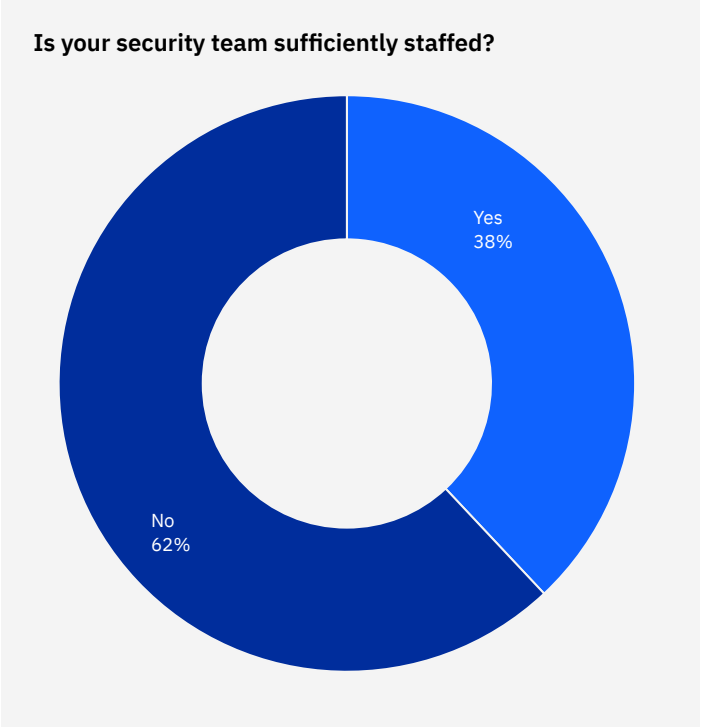


Figure 51

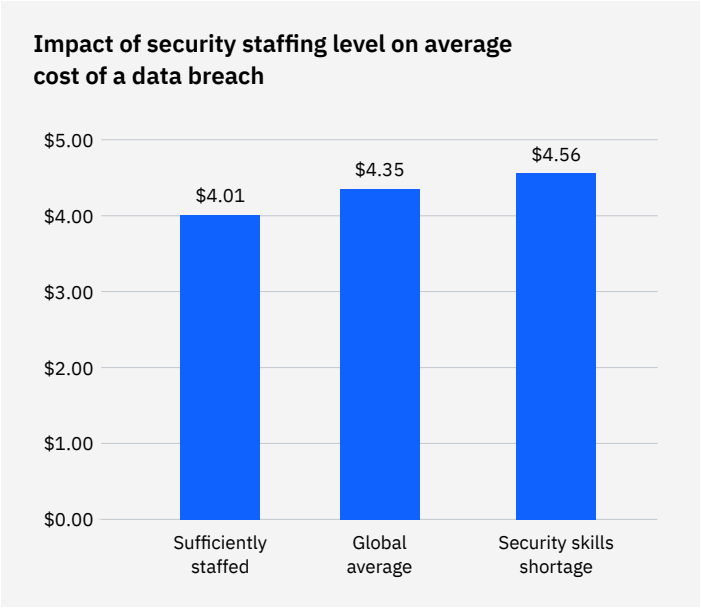


Figure 52: Measured in USD millions

Skills gap

Many organizations struggled to fill positions on their security teams. Those organizations that said they were sufficiently staffed saw considerable cost savings in terms of data breach costs, compared to those without enough employees to staff their teams. This was the first year of this report that we took a deeper look at the security skills gap.

Figure 51: There was a widespread security skills shortage among organizations in the study.
Only a little more than one-third of organizations had sufficiently staffed security teams. Just 38% of organizations said their security teams were sufficiently staffed to meet their security management needs, while 62% said they weren't sufficiently staffed.

Figure 52: Organizations that said their security teams had a skills shortage had a higher-than-average cost of the data breach.
At organizations with a sufficiently staffed security team, the average cost of a data breach was lower than average. The average cost of a data breach at sufficiently staffed organizations was USD 4.01 million. In contrast, the average cost of a data breach was USD 4.56 million at organizations with insufficiently staffed security teams, a difference of USD 0.55 million, or 12.8%.

USD 387 million

Average total cost for breaches of 50 million to 60 million records

Mega breaches

Mega breaches — those with more than 1 million compromised records — aren't normal experiences for most businesses. But mega breaches have an outsized impact on consumers and industries.

This study included 13 companies that experienced a data breach involving the loss or theft of 1 million to 60 million records. The study of the mega breaches involved a distinct methodology from the other 550 breaches in this study, each of which had no more than 102,000 lost records. For a full explanation of the research methodology, see the "Data breach FAQ" at the end of this report.

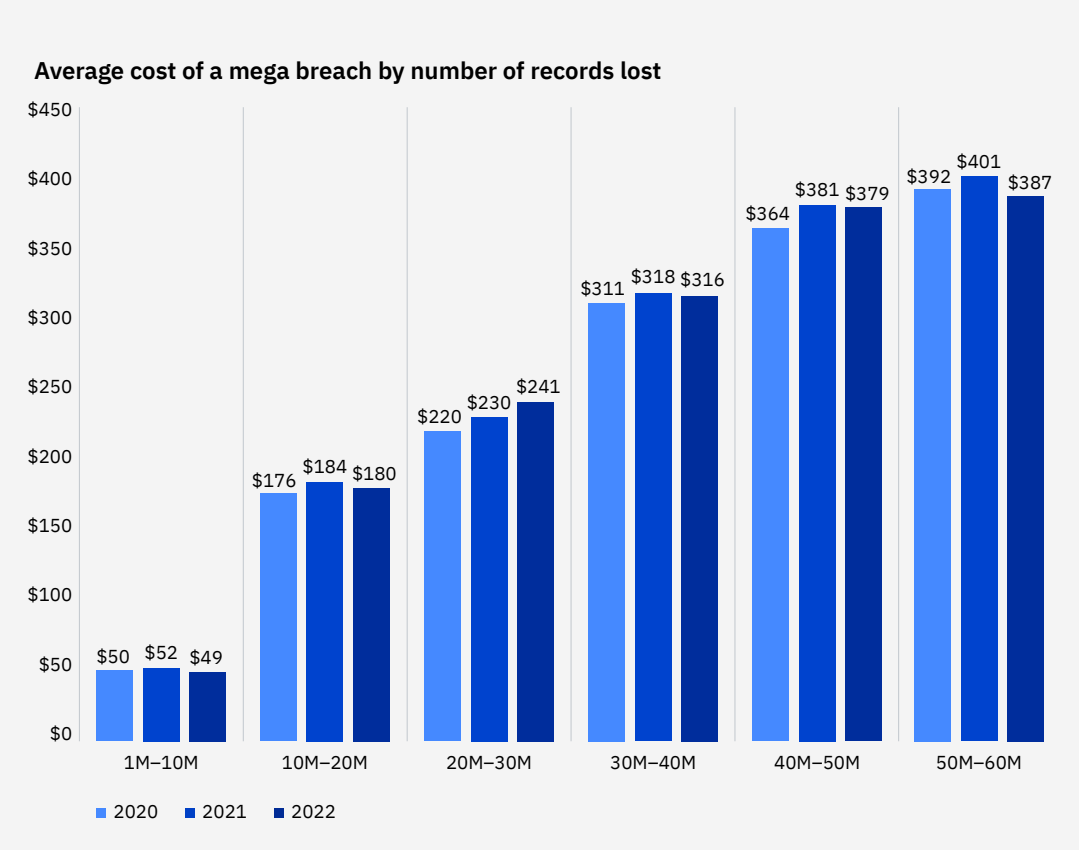


Figure 53: Measured in USD millions

Figure 53: In 2022, the average cost of a mega breach decreased slightly.
Mega breach costs saw a decrease from 2021 in six of seven breach size cohorts. The cost of the largest mega breaches of 50 million to 60 million records decreased from USD 401 million in 2021 to USD 387 million, a drop of USD 14 million or 3.6%. The cohort for 20 million to 30 million records was the only cohort where the average increased from last year. In that cohort, the average total cost of a mega breach increased from USD 230 million to USD 241 million, an increase of USD 11 million or 4.8%.

Recommendations to help minimize financial impacts of a data breach

In this section, IBM Security outlines steps organizations can take to help reduce the financial cost and reputational consequences of a data breach. These recommendations include successful security approaches taken by organizations in the study.

Adopt a zero trust security model to help prevent unauthorized access to sensitive data.
Results from the study showed that while just 41% of organizations had implemented a zero trust security approach, they had a potential breach cost saving of USD 1.5 million with a mature deployment. As organizations incorporate remote work and hybrid multicloud environments, a zero trust strategy can help protect data and resources by limiting their accessibility and requiring context.

Security tools that can share data between disparate systems and centralize data security operations can help security teams detect incidents across complex hybrid multicloud environments. You can gain deeper insights, mitigate risks and accelerate response with an open security platform that can advance your zero trust strategy. At the same time, you can use your existing investments while leaving your data where it is, helping your team become more efficient and collaborative.

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. Mature cloud security practices were associated with breach cost savings of USD 720,000 compared to no cloud security practices. Use data classification schema and retention programs to help bring visibility into and reduce the volume of sensitive information that's vulnerable to a breach. Protect sensitive information using data encryption and fully homomorphic encryption. Using an internal framework for audits, evaluating risk across the enterprise and tracking compliance with governance requirements can help improve your ability to detect a data breach and escalate containment efforts.

Invest in security orchestration, automation and response (SOAR) and XDR to help improve detection and response times.
Along with security AI and automation, XDR capabilities can help significantly reduce average data breach costs and breach lifecycles. According to the study, organizations with XDR deployed shortened the breach lifecycle by 29 days on average compared to organizations that didn't implement XDR, with a cost savings of USD 400,000. SOAR and security information and event management (SIEM) software, managed detection and response services and XDR can help your organization accelerate incident response with automation, process standardization and integration with your existing security tools.

Use tools that help protect and monitor endpoints and remote employees.
In the study, breaches where remote work was a factor in causing the breach cost nearly USD 1 million more than breaches where remote work wasn't a factor. Unified endpoint management (UEM), endpoint detection and response (EDR) and identity and access management (IAM) products and services can help provide security teams with deeper visibility into suspicious activity. This oversight involves bring your own devices (BYOD) and company laptops, desktops, tablets, mobile devices and IoT, including endpoints the organization doesn't have physical access to. UEM, EDR and IAM speed investigation and response time to isolate and contain the damage in breaches where remote work was a factor.

Create and test incident response playbooks to increase cyber resilience.
Two of the most effective ways to mitigate the cost of a data breach are forming an incident response (IR) team and extensive testing of the IR plan. Breaches at organizations with IR teams that regularly test their plan saw USD 2.66 million in savings compared to breaches at organizations with no IR team or testing of the IR plan. Organizations can respond quickly to contain the fallout from a breach by establishing a detailed cyberincident playbook. Routinely test that plan through tabletop exercises or run a breach scenario in a simulated environment such as a cyber range.

Adversary simulation exercises, also known as red team exercises, can enhance the effectiveness of IR teams by uncovering attack paths and techniques they might miss and identifying gaps in their detection and response capabilities. An attack surface management solution can help organizations improve their security posture by locating previously unknown exposure points through simulations of an authentic attack experience.

Recommendations for security practices are for educational purposes and don't guarantee results.

Organization demographics

This year’s study comprised 550 organizations of various sizes, geographies and industries. This section shows the breakdown of organizations in the study by geography and industry and includes definitions used for classifying the organizations by industry.

17 years

The United States has been a part of the study for the longest time at 17 years

Geographic demographics

The 2022 study was conducted in 17 countries or regional samples.

Global study at a glance

Countries	2022 sample	Percent	Years studied	Currency
United States	64	12%	17	USD
India	49	9%	11	INR
United Kingdom	43	8%	15	GBP
Brazil	43	8%	10	BRL
Germany	38	7%	14	EUR
Japan	35	6%	11	JPY
France	33	6%	13	EUR
Middle East[1]	31	6%	9	SAR
South Korea	30	5%	5	KRW
Australia	26	5%	13	AUD
Canada	25	5%	8	CAD
Italy	24	4%	11	EUR
ASEAN[2]	23	4%	6	SGD
Latin America[3]	23	4%	3	MXN
South Africa	21	4%	7	ZAR
Scandinavia[4]	20	4%	4	NOK
Turkey	20	4%	5	TRY
Total	**550**	**100%**		

1. Middle East is a sample of companies located in Saudi Arabia and the United Arab Emirates
2. ASEAN is a sample of companies located in Singapore, Indonesia, Philippines, Malaysia, Thailand and Vietnam
3. Latin America is a sample of companies located in Mexico, Argentina, Chile and Colombia
4. Scandinavia is a sample of companies located in Denmark, Sweden, Norway and Finland

Figure 54

The largest samples of industries were in these sectors.

16% Financial

12% Services

12% Industrial

11% Technology

Industry demographics

This year's study was conducted in 17 industries, the same industries that have been included in the study for multiple years.

Distribution of the sample by industry

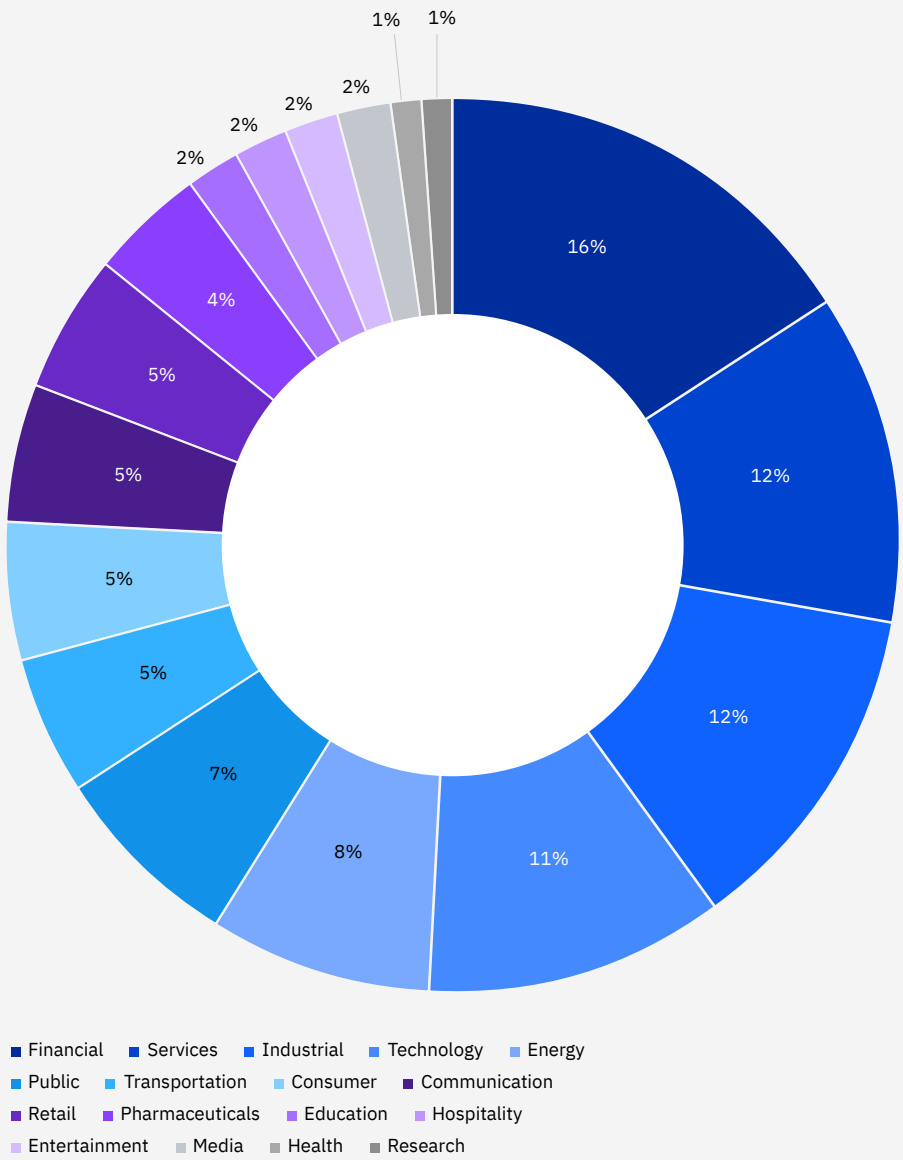


Figure 55

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 processing, 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, research and development

Public
Federal, state and local government agencies and non-governmental organizations (NGOs)

Research methodology

To preserve confidentiality, the benchmark instrument didn't capture any company-specific information. Data collection methods excluded actual accounting information and 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 respondents to provide a second estimate for indirect and opportunity costs, separately.

To ensure a manageable size for benchmarking, we carefully limited items to only cost activity centers that we considered crucial to measuring data breach costs. Based on discussions with experts, the final set of items included a fixed set of cost activities. After collecting benchmark information, we re-examined each instrument carefully for consistency and completeness.

We limited the scope of data breach cost items to known cost categories that applied to a broad set of business operations that handle personal information. Our belief was that a study focused on business process — not data protection or privacy compliance activities — would yield better quality results.

This research used activity-based costing, which identifies activities and assigns a cost according to actual use.

How we calculate the cost of a data breach

To calculate the average cost of a data breach, this research excluded very small and very large breaches. Data breaches examined in the 2022 study ranged in size between 2,200 and 102,000 compromised records. We used a separate analysis to examine the costs of very large mega breaches, which is explained further in the "Data breach FAQ" section of the report.

This research used 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.

Detection and escalation
Activities that enable a company to reasonably detect the breach, including the following:
- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards

Notification
Activities that enable the company to notify data subjects, data protection regulators and other third parties, including the following:
- Emails, letters, outbound calls or general notice to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement of outside experts

Post breach response
Activities to help victims of a breach communicate with the company and redress activities to victims and regulators, including the following:
- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fines

Lost business
Activities that attempt to minimize the loss of customers, business disruption and revenue losses, including the following:
- Business disruption and revenue losses from system downtime
- Cost of losing customers and acquiring new customers
- Reputation losses and diminished goodwill

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, a financial record or both, or debit card are potentially put at risk. These records can be in electronic or paper format. Breaches included in the study ranged from 2,200 to 102,000 compromised records.

What is a compromised record?
A record is information that identifies the natural person or 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 over 3,600 separate interviews with individuals at 550 organizations that suffered a data breach between March 2021 and March 2022. Interviewees included IT, compliance and information security practitioners familiar with their organization's data breach and the costs associated with resolving the breach. For privacy purposes, we didn't collect organization-specific information.

How do you calculate the average cost of a data breach?
We collected both the direct and indirect expenses incurred by the organization. Direct expenses included engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs included in-house investigations and communication, and the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

This research represented only events directly relevant to the data breach experience. 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. However, such activities didn't directly affect the cost of a data breach for this research.

For consistency with prior years, we used 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 was the organization. In survey research, the unit of analysis is the individual. We recruited 550 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 doesn't apply to catastrophic or mega data breaches, such as Equifax, Capital One or Facebook. These events aren't typical of the breaches many organizations experience. To draw useful conclusions in understanding data breach cost behaviors, we targeted data breach incidents that didn't exceed 102,000 records.

It's 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 13 very large breaches of this size.

Why did you use simulation methods to estimate the cost of a mega data breach?
The sample size of 13 companies that experienced a mega breach was too small to perform a statistically significant analysis using activity-based cost methods. To remedy this issue, we deployed Monte Carlo simulation to estimate a range of possible, meaning random, outcomes through repeated trials.

In total, we performed more than 150,000 trials. The grand mean of all sample means provided a most likely outcome at each size of data breach, ranging from 1 million to 60 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 5,027 organizations.

The benchmark didn’t capture any company-identifying information.

Research limitations

Our study used a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, the inherent limitations with this benchmark research need to be carefully considered before drawing conclusions from findings.

Non-statistical results
Our study drew upon a representative, non-statistical sample of global entities. Statistical inferences, margins of error and confidence intervals can’t be applied to these data, given that our sampling methods weren’t scientific.

Non-response
Non-response bias wasn’t tested, so it’s possible that companies that didn’t participate are substantially different in terms of underlying data breach cost.

Sampling-frame bias
Because our sampling frame was judgmental, the quality of results was influenced by the degree to which the frame was representative of the population of companies being studied. We believe that the current sampling frame was biased toward companies with more mature privacy or information security programs.

Company-specific information
The benchmark didn’t capture company-identifying information. Individuals could 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 can’t be determined.

Extrapolated cost results
While certain checks and balances can be incorporated into the benchmark process, it’s always possible that respondents didn’t provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

Currency conversions
The conversion from local currencies to the US dollar deflated average total cost estimates in other countries. For purposes of consistency with prior years, we decided to continue to use the same accounting method rather than adjust the cost.

About Ponemon Institute and IBM Security

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 doesn't collect any personally identifiable information from individuals or company identifiable information in business research. Furthermore, strict quality standards ensure that subjects aren't 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. 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

Take the next steps

Zero trust security solutions
Wrap security around every user, device and connection.
Learn more

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

Data security
Discover, classify and protect sensitive enterprise data.
Learn more

Security orchestration, automation and response
Accelerate incident response with orchestration and automation.
Learn more

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

Cloud security
Integrate security into your journey to hybrid multicloud.
Learn more

Endpoint security
Protect devices, users and organizations against sophisticated attacks.
Learn more

Cybersecurity services
Reduce risk with consulting, cloud and managed security services.
Learn more

Incident response and threat intelligence
Proactively manage and respond to security threats.
Learn more

Schedule a one-on-one consultation with an IBM Security X-Force expert
Schedule now

View the action guide →

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2022

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.