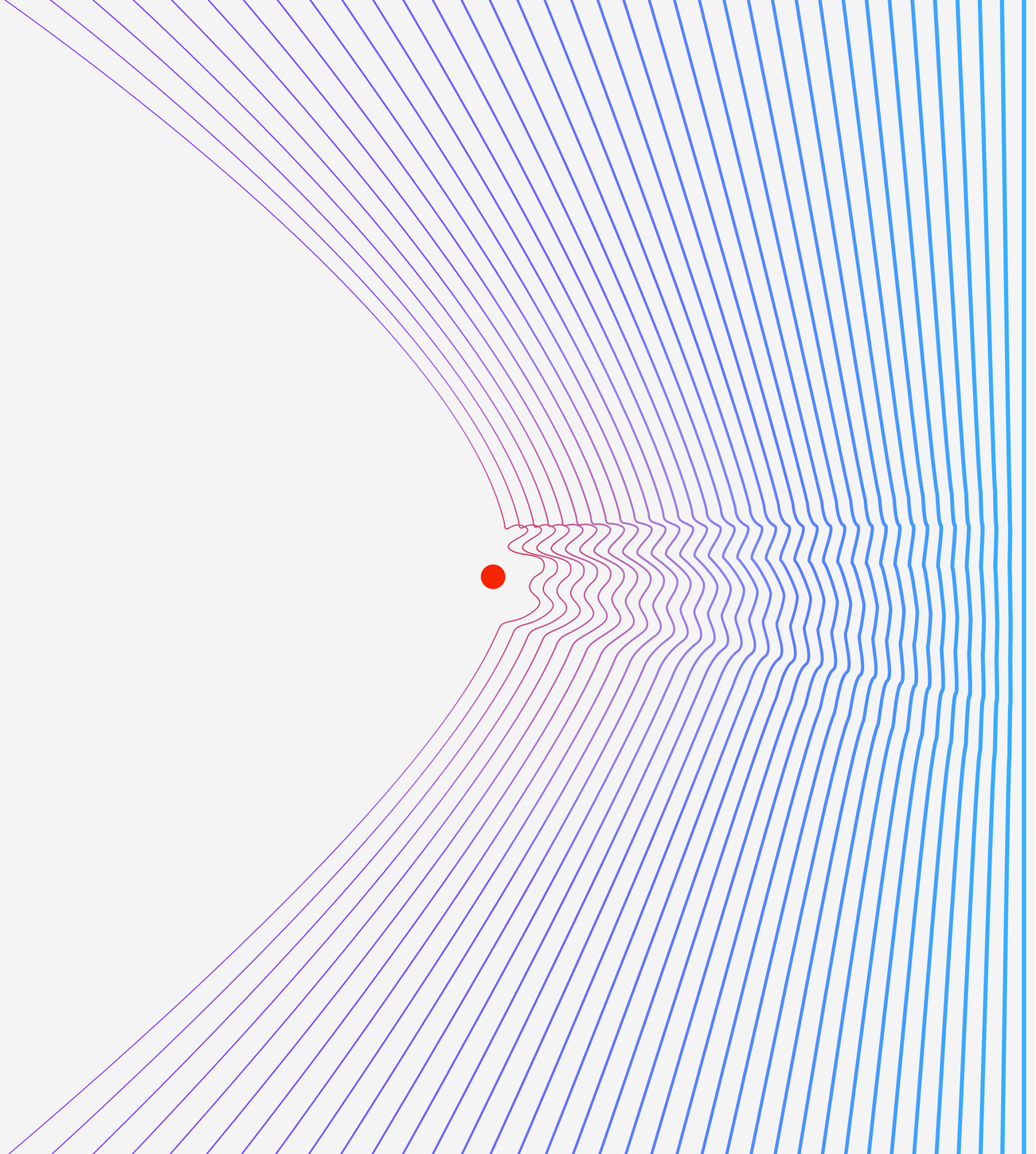
IBM **Security**

Cost of a Data Breach Report 2023



IBM

Table of contents

01

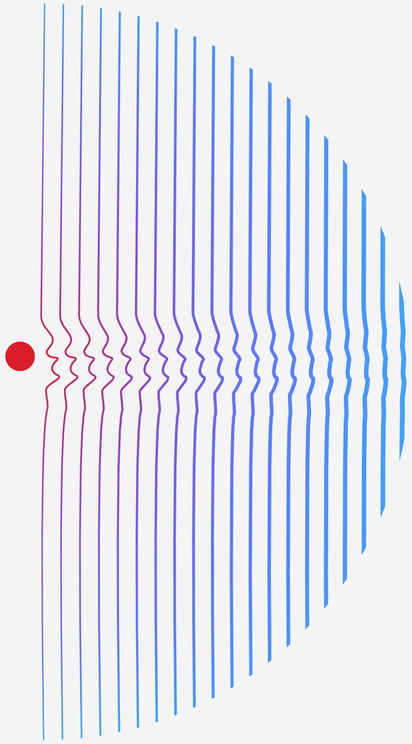
Executive summary

The Cost of a Data Breach Report equips IT, risk management and security leaders with quantifiable evidence to help them better manage their security investments, risk profile and strategic decision-making processes. The 2023 edition represents this report's 18th consecutive year.

This year's research—conducted independently by Ponemon Institute and sponsored, analyzed and published by IBM Security®—studied 553 organizations impacted by data breaches that occurred between March 2022 and March 2023.

The years mentioned in this report refer to the year the report was published, not necessarily the year of the breach. The breaches studied took place across 16 countries and regions and in 17 different industries.

Throughout this report, we'll examine the root causes and both short-term and long-term consequences of data breaches. We'll also explore the factors and technologies that enabled companies to limit losses—as well as those that led to increased costs.



What’s new in the 2023 report

Each year, we continue to evolve the Cost of a Data Breach Report to match new technologies, emerging tactics and recent events. For the first time, this year’s research explores:

- How breaches are identified: whether by an organization’s own security teams, another third party or the attacker
- The impact of involving law enforcement in a ransomware attack
- The effect of ransomware playbooks and workflows
- Specific costs associated with regulatory fines
- If and how companies plan to increase security investment as a result of a breach
- The impact of the following mitigation strategies:
  - Threat intelligence
  - Vulnerability and risk management
  - Attack surface management (ASM)
  - Managed security service providers (MSSPs)

As the cost of a breach continues to increase, this report delivers essential insights to help security and IT teams better manage risk and limit potential losses. The report is divided into five major sections:

- The executive summary with key findings and what’s new in the 2023 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

Key findings

The key findings described here are based on IBM Security analysis of research data compiled by Ponemon Institute. Cost amounts in this report are measured in US dollars (USD).

USD 4.45M

Average total cost of a breach
The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million. Taking a long-term view, the average cost has increased 15.3% from USD 3.86 million in the 2020 report.

51%

Percentage of organizations planning to increase security investments as a result of a breach
While data breach costs continued to rise, report participants were almost equally split on whether they plan to increase security investments because of a data breach. The top areas identified for additional investments included incident response (IR) planning and testing, employee training, and threat detection and response technologies.

USD 1.76M

The effect of extensive security AI and automation on the financial impact of a breach
Security AI and automation were shown to be important investments for reducing costs and minimizing time to identify and contain breaches. Organizations that used these capabilities extensively within their approach experienced, on average, a 108-day shorter time to identify and contain the breach. They also reported USD 1.76 million lower data breach costs compared to organizations that didn’t use security AI and automation capabilities.

1 in 3

Number of breaches identified by an organization's own security teams or tools
Only one-third of companies discovered the data breach through their own security teams, highlighting a need for better threat detection. 67% of breaches were reported by a benign third party or by the attackers themselves. When attackers disclosed a breach, it cost organizations nearly USD 1 million more compared to internal detection.

USD 470,000

Additional cost experienced by organizations that didn't involve law enforcement in a ransomware attack
This year's research shows that excluding law enforcement from ransomware incidents led to higher costs. While 63% of respondents said they involved law enforcement, the 37% that didn't also paid 9.6% more and experienced a 33-day longer breach lifecycle.

53.3%

Since 2020, healthcare data breach costs have increased 53.3%
The highly regulated healthcare industry has seen a considerable rise in data breach costs since 2020. For the 13th year in a row, the healthcare industry reported the most expensive data breaches, at an average cost of USD 10.93 million.

82%

The percentage of breaches that involved data stored in the cloud—public, private or multiple environments
Cloud environments were frequent targets for cyberattackers in 2023. Attackers often gained access to multiple environments, with 39% of breaches spanning multiple environments and incurring a higher-than-average cost of USD 4.75 million.

USD 1.68M

Cost savings from high levels of DevSecOps adoption
Integrated security testing in the software development process (DevSecOps) showed sizable ROI in 2023. Organizations with high DevSecOps adoption saved USD 1.68 million compared to those with low or no adoption. Compared to other cost-mitigating factors, DevSecOps demonstrated the largest cost savings.

USD 1.49M

Cost savings achieved by organizations with high levels of IR planning and testing
In addition to being a priority investment for organizations, IR planning and testing emerged as a highly effective tactic for containing the cost of a data breach. Organizations with high levels of IR planning and testing saved USD 1.49 million compared to those with low levels.

USD 1.44M

Increase in data breach costs for organizations that had high levels of security system complexity
Organizations that reported low or no security system complexity experienced an average data breach cost of USD 3.84 million in 2023. Those with high levels of security system complexity reported an average cost of USD 5.28 million, representing an increase of 31.6%.

USD 1.02M

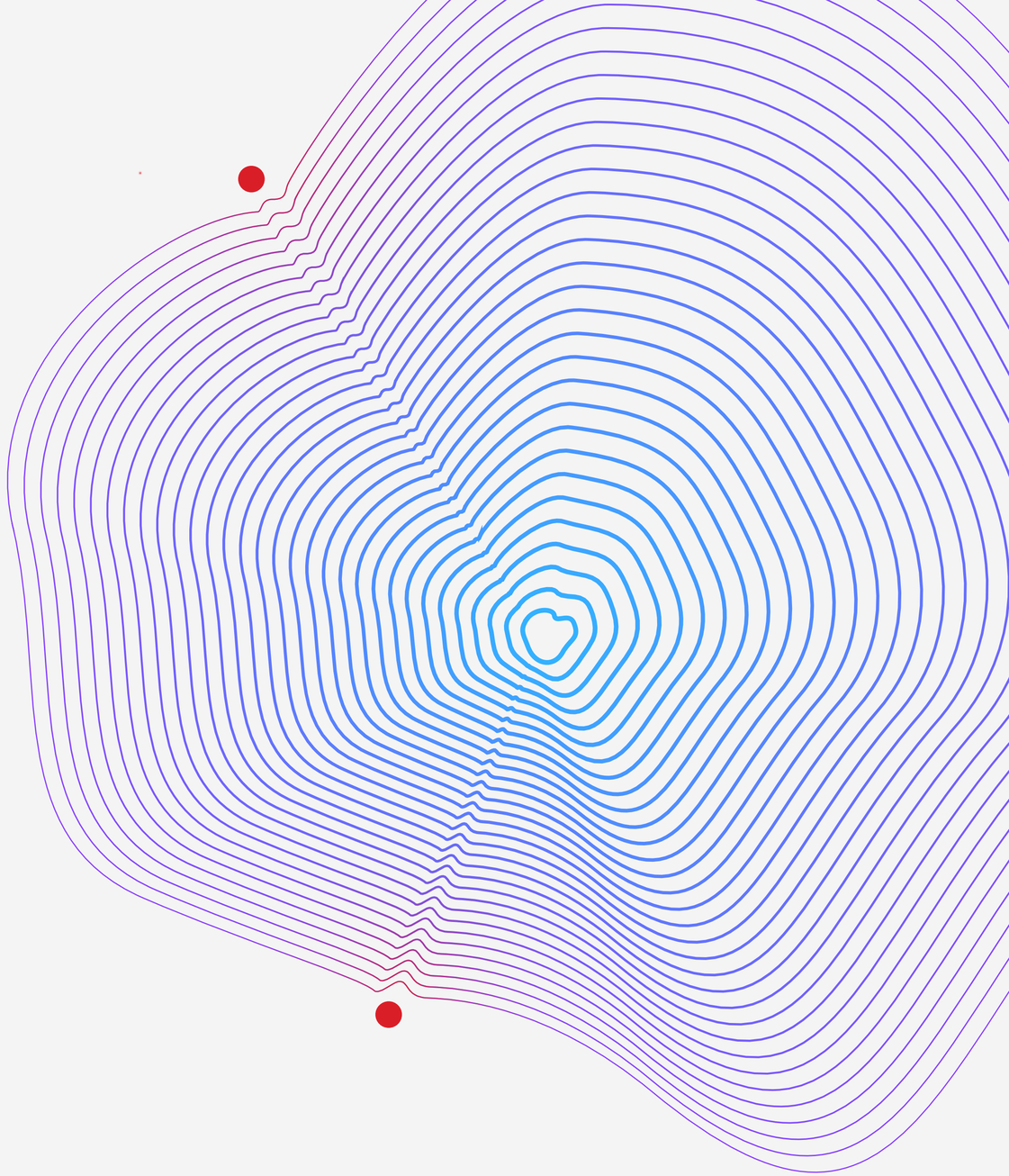
Average cost difference between breaches that took more than 200 days to find and resolve, and those that took less than 200 days
Time to identify and contain breaches—known as the breach lifecycle—continues to be integral to the overall financial impact. Breaches with identification and containment times under 200 days cost organizations USD 3.93 million. Those over 200 days cost USD 4.95 million—a difference of 23%.

02

Complete findings

In this section, we provide the detailed findings of this report across 18 themes. Topics are presented in the following order:

- Global highlights
- Initial attack vectors
- Identifying attacks
- Data breach lifecycle
- Key cost factors
- Ransomware and destructive attacks
- Business partner supply chain attacks
- Software supply chain attacks
- Regulatory environments
- Cloud breaches
- Mega breaches
- Security investments
- Security AI and automation
- Incident response
- Threat intelligence
- Vulnerability and risk management
- Attack surface management
- Managed security service providers



Global highlights

The Cost of a Data Breach Report provides a global picture of the cost of data breaches, built using data from over 553 breaches in 16 different countries and taking into account hundreds of cost factors. This section examines critical metrics at the level of global average. We also explore the average per-record comparative costs between countries and industries.

USD 4.45M

Global average total cost of a data breach

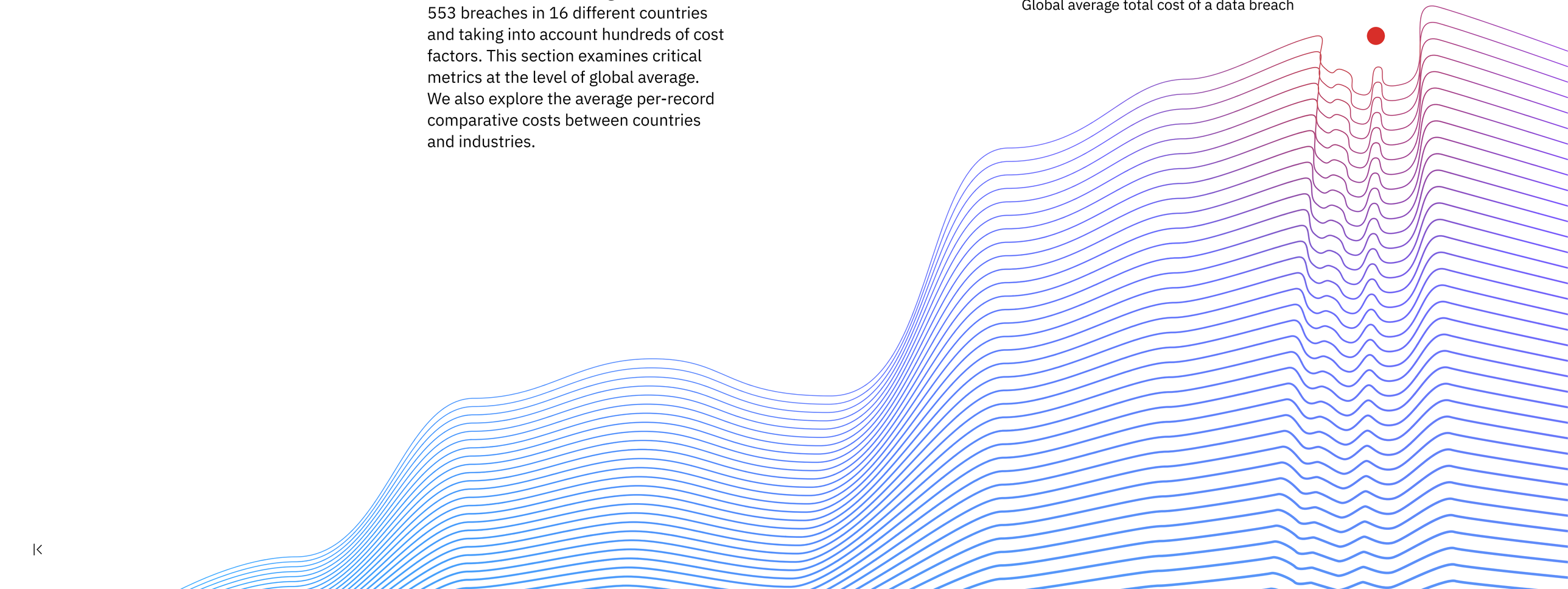


Figure 1. The cost of a data breach climbed to a new high.
Globally, the average cost of a data breach rose to USD 4.45 million, a USD 100,000 increase from 2022. This represents a 2.3% increase from the 2022 average cost of USD 4.35 million. Since 2020, when the average total cost of a data breach was USD 3.86 million, the average total cost has increased 15.3%.

Figure 2. Per-record cost of a data breach also reached a new high.
In 2023, the average cost per record involved in a data breach was USD 165, a small increase from the 2022 average of USD 164. This matches the relatively small growth from 2021 to 2022, where the cost rose by just USD 3. In the last seven years, the largest increase in average per-record costs was between 2020 and 2021, when the average rose from USD 146 to USD 161 or 10.3%. This study examined breaches sized between 2,200 and 102,000 records.[1]

Total cost of a data breach

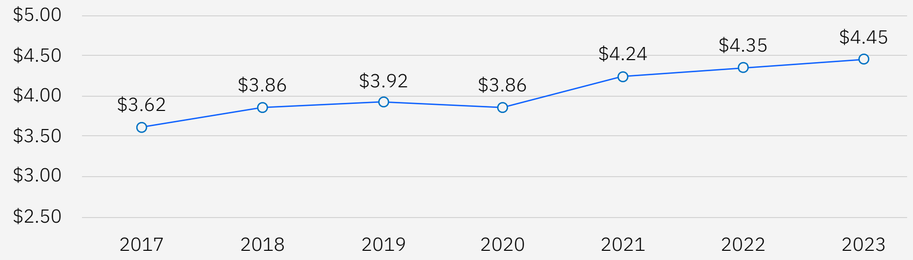


Figure 1. Measured in USD millions

Per-record cost of a data breach

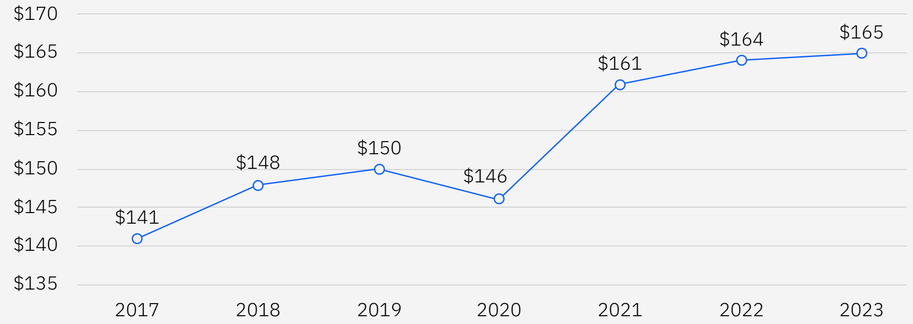


Figure 2. Measured in USD

Figure 3. For the 13th consecutive year, the United States held the title for the highest data breach costs.
The top five countries or regions with the highest average cost of a data breach saw considerable changes from 2022.

		2023	2022
1	↑	**United States** USD 9.48 million	**United States** USD 9.44 million
2	↑	**Middle East** USD 8.07 million	**Middle East** USD 7.46 million
3	↓	**Canada** USD 5.13 million	**Canada** USD 5.64 million
4	↓	**Germany** USD 4.67 million	**United Kingdom** USD 5.05 million
5	↓	**Japan** USD 4.52 million	**Germany** USD 4.85 million

Of this year's top five, Japan is the only country that didn't appear on the 2022 top five list, moving up from the number 6 most expensive spot last year. The top 5 list last year also included the United Kingdom (UK) at an average data breach cost of USD 5.05 million. This year, the UK saw a significant drop in average cost at USD 4.21 million—down 16.6% from last year—resulting in placement just outside of the top five.

The United States again had the highest average total cost of a data breach at USD 9.48 million, an increase of 0.4% from last year's USD 9.44 million. Like last year, the Middle East had the second-highest average total cost of a data breach at USD 8.07 million, up 8.2% from USD 7.46 million.

In Canada, the average total cost of a data breach decreased from USD 5.64 million to USD 5.13 million or 9%. The average cost also decreased in Germany, dropping from USD 4.85 million to USD 4.67 million or 3.7%. Japan saw the average drop slightly, from USD 4.57 million to USD 4.52 million or 1.1%.

Cost of a data breach by country or region

Figure 3. Measured in USD millions

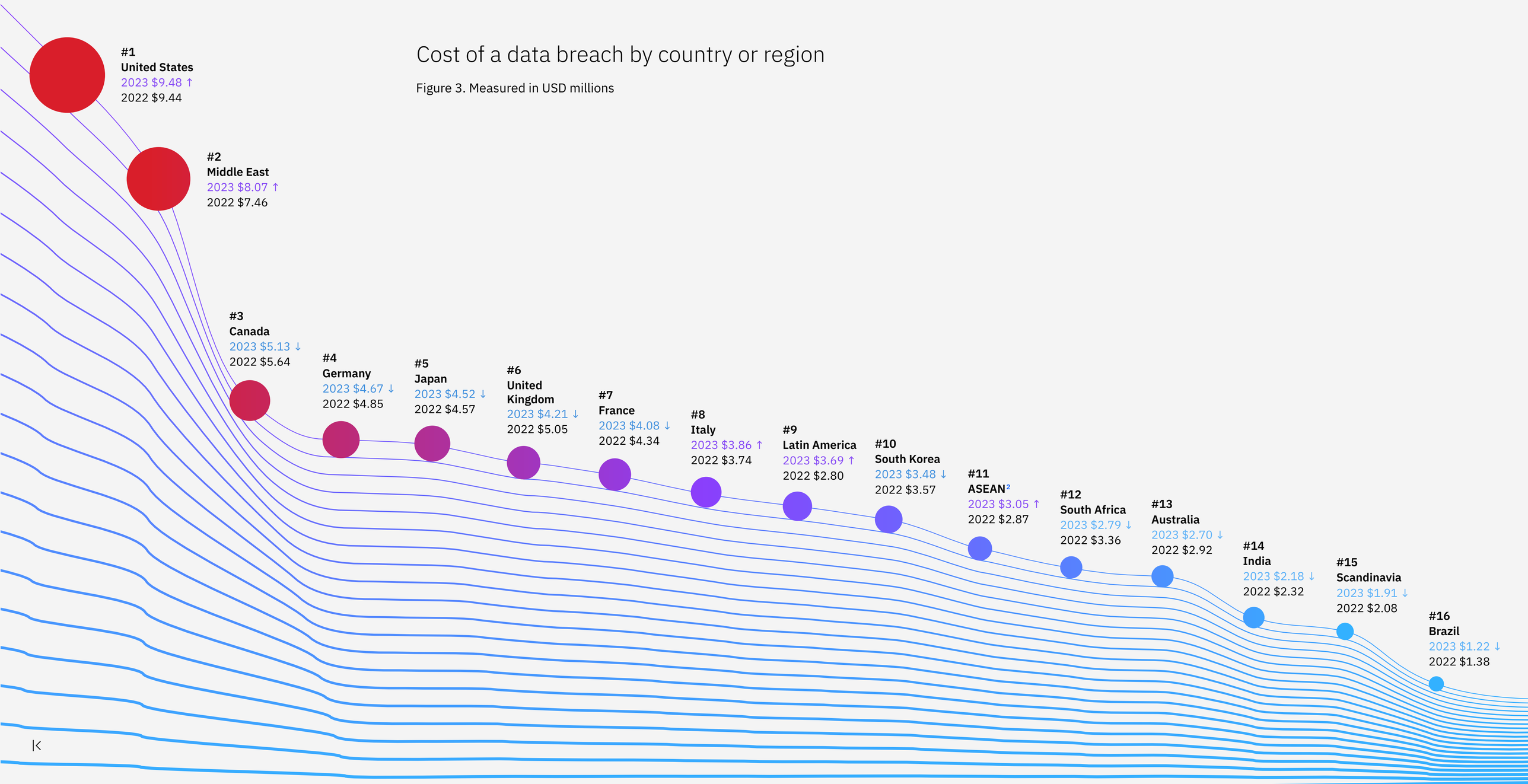


Figure 4. Across industries, healthcare reported the highest costs for the 13th year in a row.
Healthcare continues to experience the highest data breach costs of all industries, increasing from USD 10.10 million in 2022 to USD 10.93 million in 2023—an increase of 8.2%. Over the past three years, the average cost of a data breach in healthcare has grown 53.3%, increasing more than USD 3 million compared to the average cost of USD 7.13 million in 2020. Healthcare faces high levels of industry regulation and is considered critical infrastructure by the US government. Since the start of the COVID-19 pandemic, the industry has seen notably higher average data breach costs.

The top five most costly industries underwent some changes from last year's rankings. Technology dropped out of the top five while the industrial sector was added, showing a 5.8% increase as it moved from the seventh-highest to the fifth. According to IBM threat intelligence, manufacturing is the industry most commonly targeted by cybercriminals.

		2023	2022
1	↑	**Healthcare** USD 10.93 million	**Healthcare** USD 10.10 million
2	↓	**Financial** USD 5.90 million	**Financial** USD 5.97 million
3	↓	**Pharmaceuticals** USD 4.82 million	**Pharmaceuticals** USD 5.01 million
4	↑	**Energy** USD 4.78 million	**Technology** USD 4.97 million
5	↑	**Industrial** USD 4.73 million	**Energy** USD 4.72 million

Cost of a data breach by industry

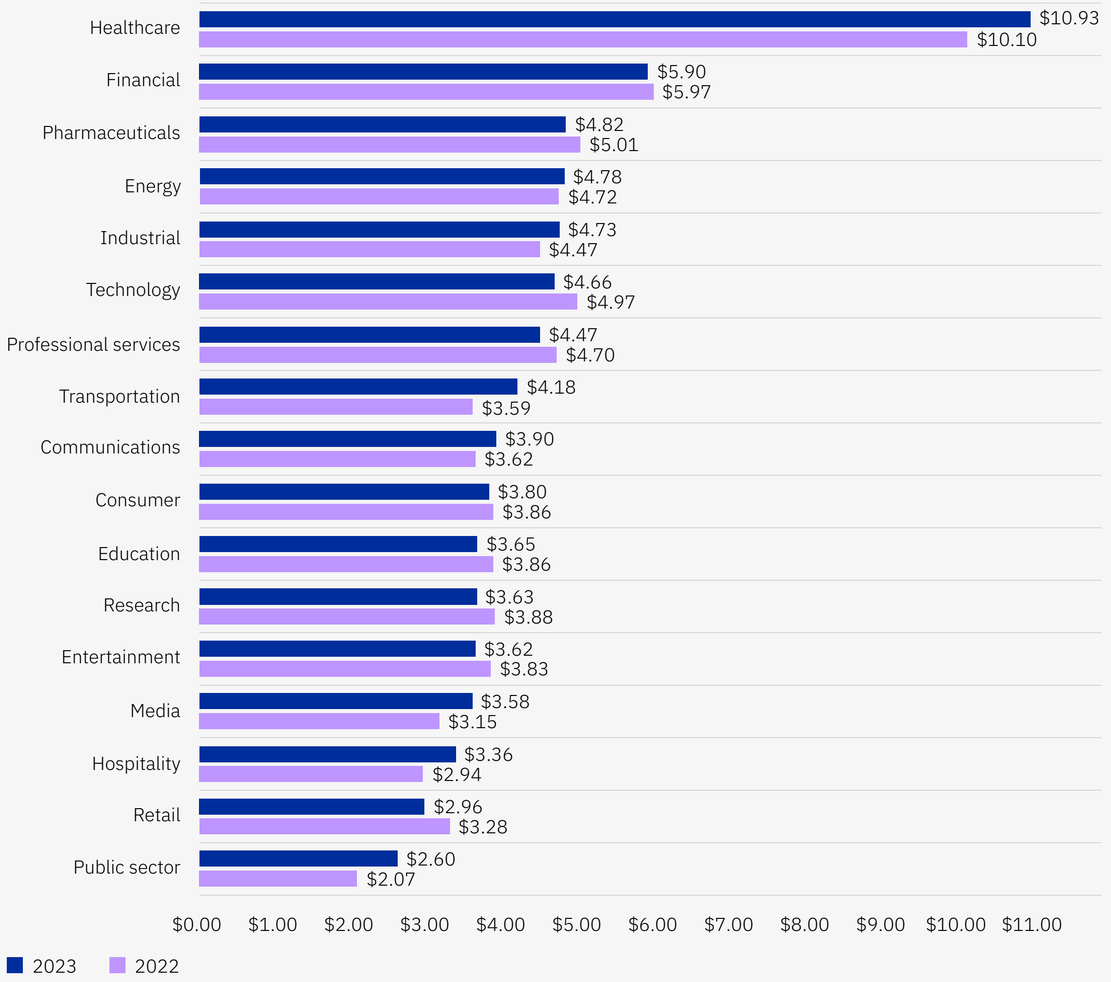


Figure 4. Measured in USD millions

Figure 5. Mean times to identify and contain breaches stayed roughly the same.
Compared to 2022, both the mean time to identify (MTTI) and the mean time to contain (MTTC) breaches saw only marginal changes. Mean time to identify refers to the time it takes an organization to uncover a security breach. Mean time to contain refers to the time required to resolve a security breach once it has been identified.

In 2022, it took organizations 207 days to identify a breach. In 2023, it took only 204 days. On the other hand, organizations required an average of 73 days to contain breaches in 2023, while they required just 70 days on average in 2022. The highest mean times to contain and identify breaches both occurred in 2021, at 212 and 75 days, respectively.

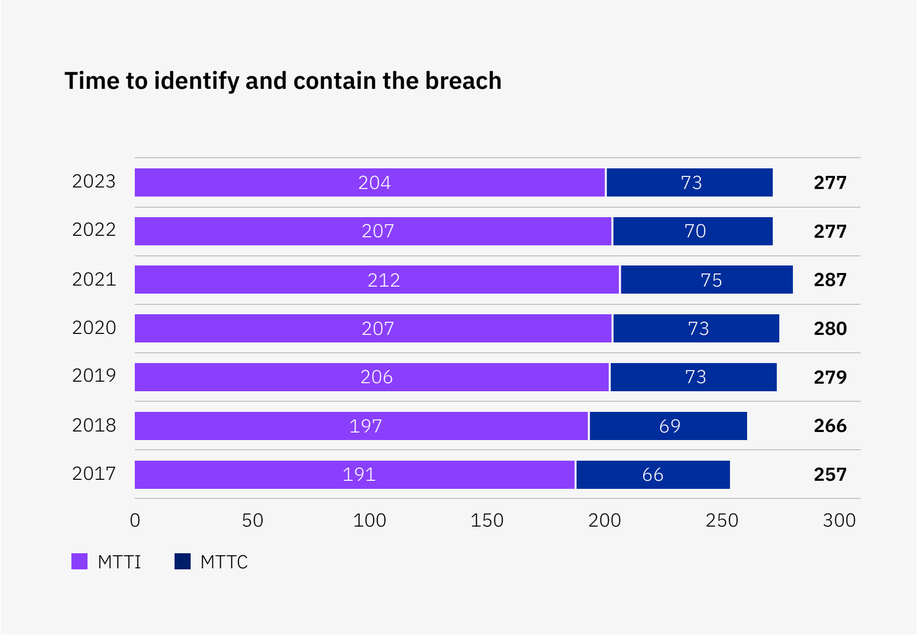


Figure 5. Measured in days

Figure 6. Lost business costs hit a five-year low.
Last year's report saw detection and escalation costs rise to become the costliest category of data breach expenses, indicating a shift toward longer and more-complex breach investigations. The trend continued this year as detection and escalation costs remained in the top spot and rose from USD 1.44 million to USD 1.58 million, demonstrating a change of USD 140,000 or 9.7%. Detection and escalation costs include activities that enable a company to reasonably detect a breach and can include forensic and investigative activities, assessment and audit services, crisis management, and communications to executives and boards.

The other key cost segments of a data breach—lost business cost, post-breach response and notification—also saw changes compared to 2022. Lost business costs dropped 8.5%, from USD 1.42 million in 2022 to USD 1.30 million in 2023. Lost business costs include activities such as business disruptions and revenue losses from system downtime, the cost of lost customers and acquiring new customers, and reputation losses and diminished goodwill.

Notably, the notification cost segment rose from USD 310,000 in 2022 to USD 370,000 in 2023, which represents a 19.4% increase. Post-breach response costs rose by just USD 20,000. Notification costs include activities that enable the company to notify data subjects, data protection regulators and other third parties.

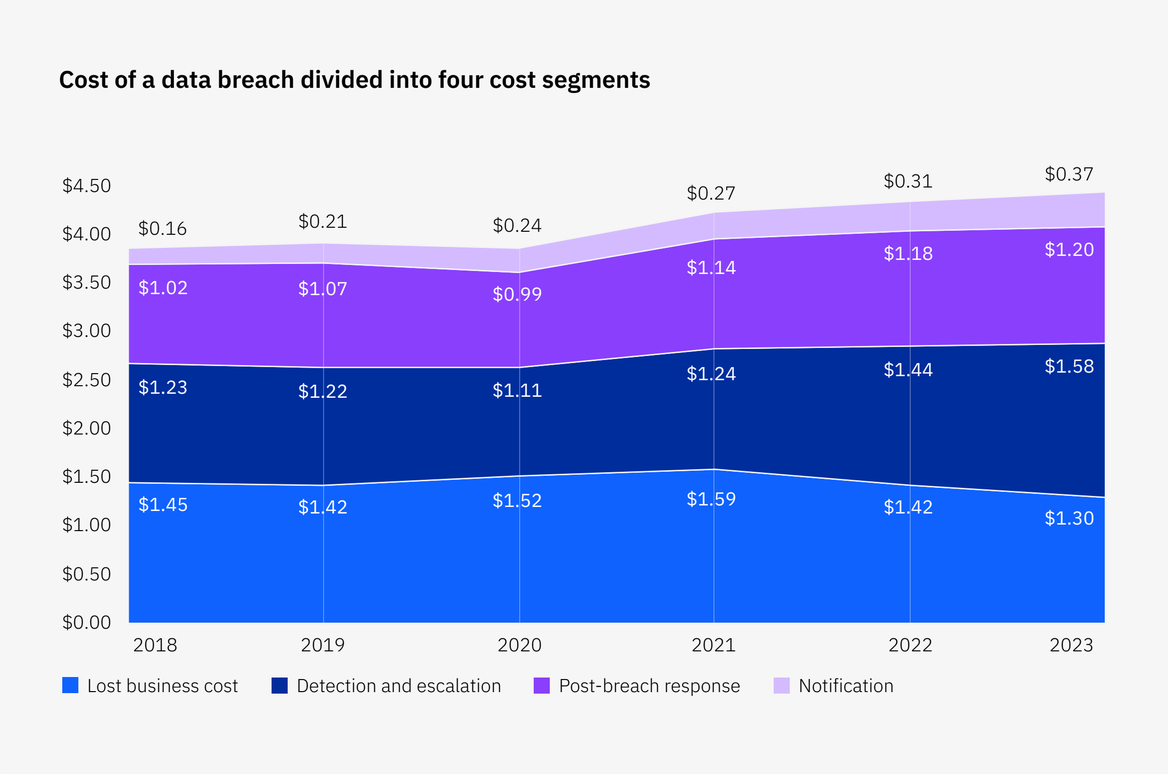


Figure 6. Measured in USD millions

Figure 7. Smaller organizations faced considerably higher data breach costs than last year.
In 2023, organizations with more than 5,000 employees saw the average cost of a data breach decrease compared to 2022. On the other hand, those with 5,000 or fewer employees saw considerable increases in the average cost of a data breach.

Organizations with fewer than 500 employees reported that the average impact of a data breach increased from USD 2.92 million to USD 3.31 million or 13.4%. Those with 500–1,000 employees saw an increase of 21.4%, from USD 2.71 million to USD 3.29 million. In the 1,001–5,000 employee range, the average cost of a data breach increased from USD 4.06 million to USD 4.87 million, rising nearly 20%.

In the 10,001–25,000 range, respondents reported an average cost of USD 5.46 million, a decrease of 1.8% from 2022's figure of USD 5.56 million. Organizations with more than 25,000 employees saw the average cost drop from USD 5.56 million in 2022 to USD 5.42 million in 2023, a decrease of USD 140,000 or 2.5%.

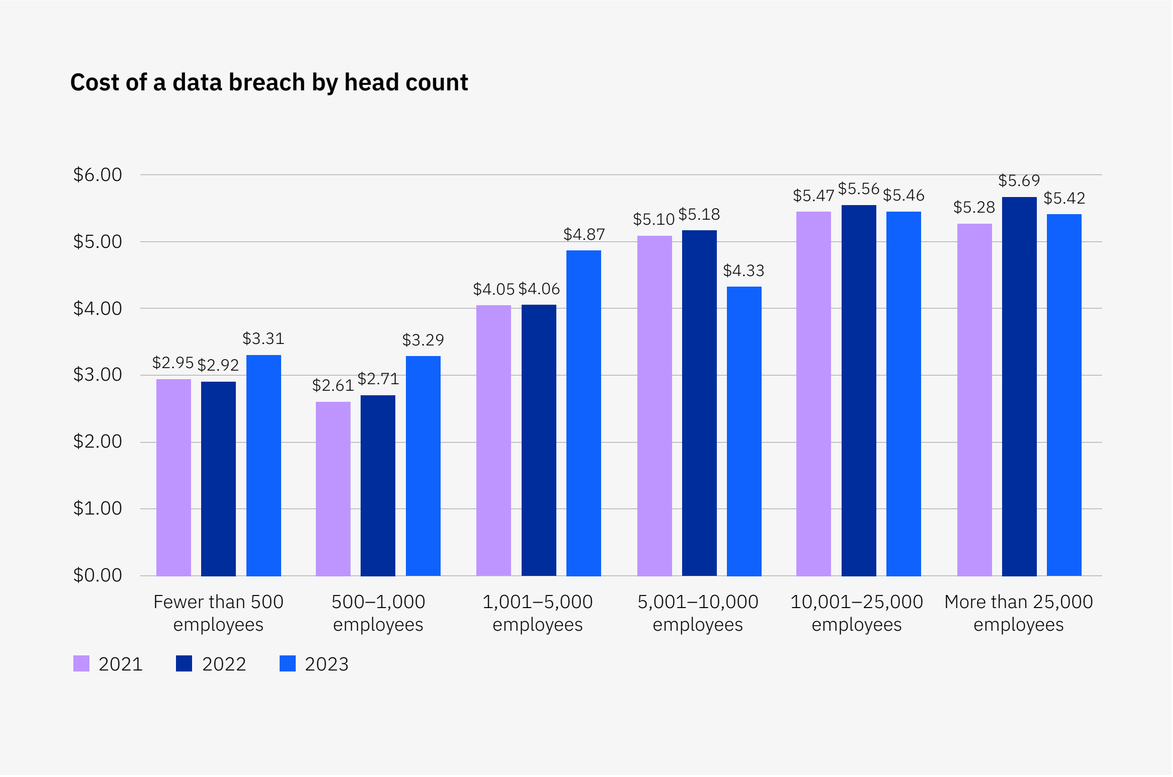


Figure 7. Measured in USD millions

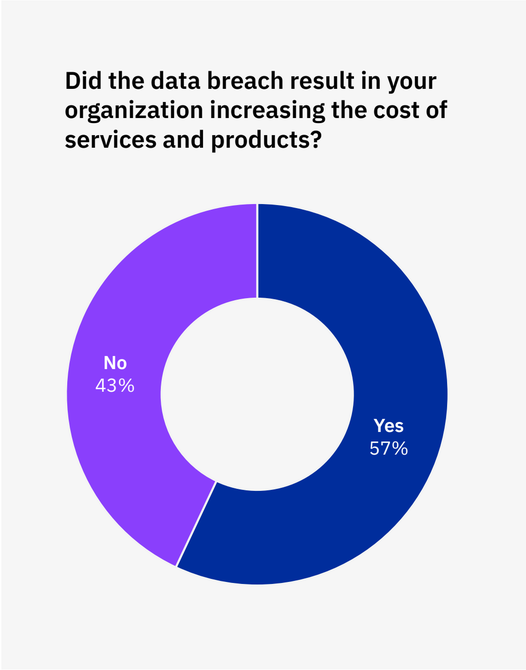


Figure 8. Share of total sample of breached organizations

Figure 8. Most organizations continue to increase the prices of services and products as a result of a data breach. The majority (57%) of respondents indicated that data breaches led to an increase in the pricing of their business offerings, passing on costs to consumers. This finding is similar to our 2022 report, where 60% of respondents said they increased prices.

Figures 9a and 9b. Customer PII was the costliest—and most common—record compromised.
Of all record types, customer and employee personal identifiable information (PII) was the costliest to have compromised. In 2023, customer PII such as names and Social Security numbers cost organizations USD 183 per record, with employee PII close behind at USD 181 per record. The least expensive record type to have compromised is anonymized customer data, which cost organizations USD 138 per record in 2023.

As was the case in 2022 and 2021, customer PII was the most commonly breached record type in 2023. 52% of all breaches involved some form of customer PII. This is an increase of five percentage points from 2022, when customer PII accounted for 47% of all data compromised. The second-most commonly compromised data type was employee PII at 40%. Compromised employee PII has seen sizable growth from 2021, when it only accounted for 26% of all records compromised.

Compromised intellectual property grew three percentage points since 2022, while anonymized (non-PII) data dropped seven percentage points from 2022—decreasing from 33% to 26%. Other corporate data, such as financial information and client lists, increased from 15% of data compromised in 2022 to 21% in 2023.

Type of data compromised

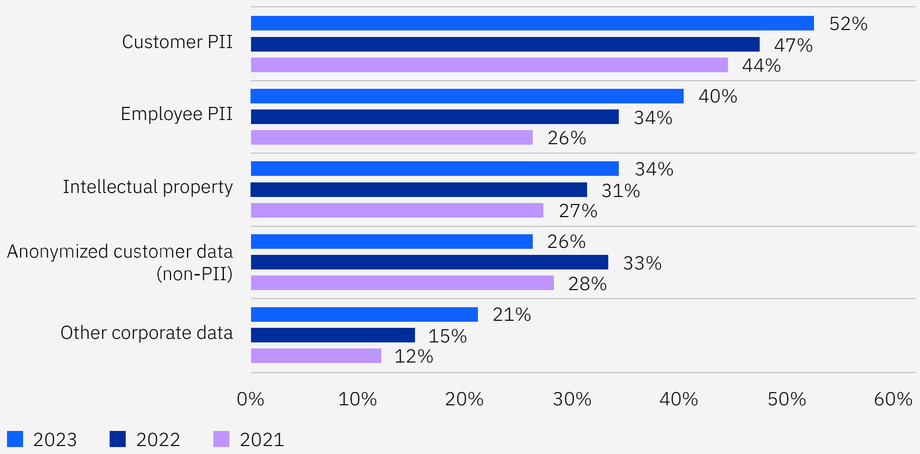


Figure 9a. More than one response permitted

Per-record cost of a data breach by type of record compromised

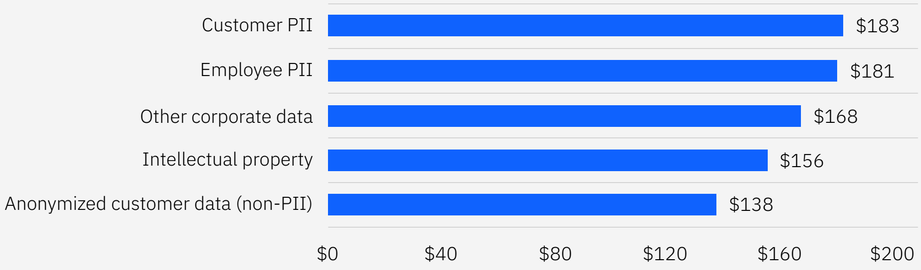
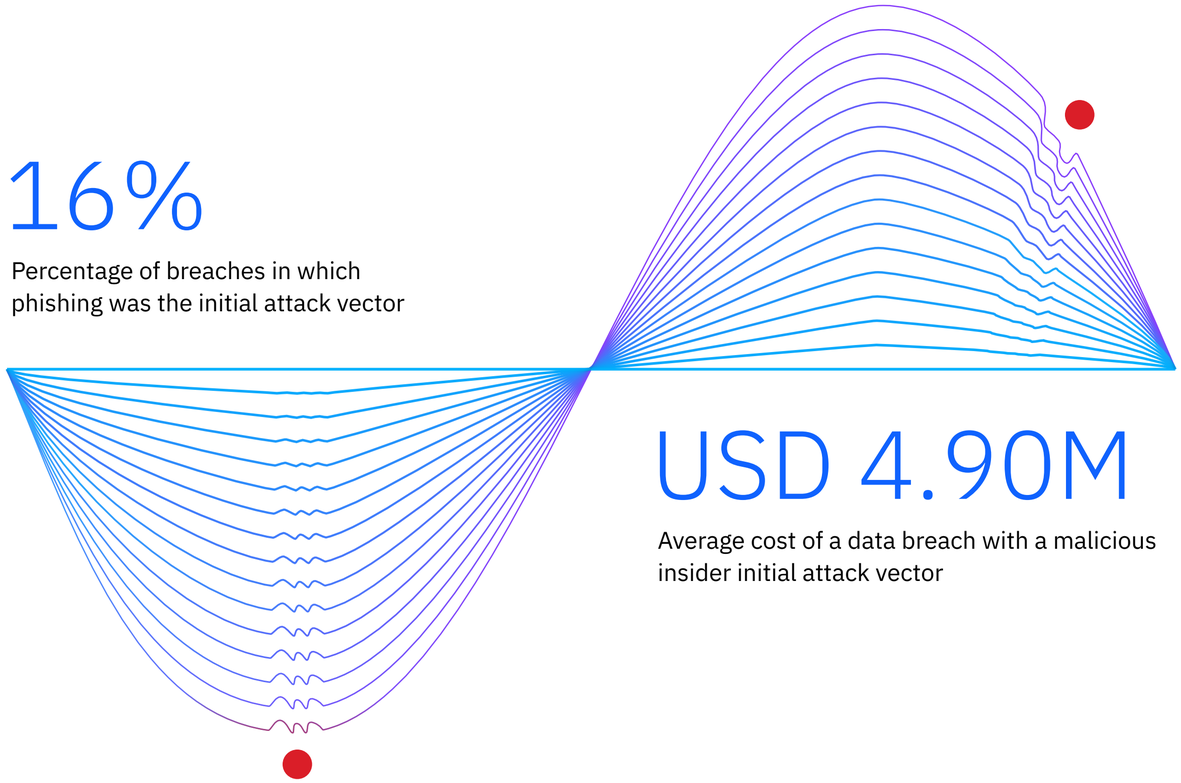


Figure 9b. Measured in USD

Initial attack vectors

This section examines the initial attack vector identified for data breaches in the study and its impact on the breach cost and timeline. It identifies the most common root causes for data breaches in the report and compares the average cost of breaches for each category as well as the average time to identify and contain those breaches. Phishing and stolen or compromised credentials were the two most prevalent attack vectors in this year's report, and both also ranked among the top four costliest incident types.



16%

Percentage of breaches in which phishing was the initial attack vector

USD 4.90M

Average cost of a data breach with a malicious insider initial attack vector

Figure 10. Phishing and stolen or compromised credentials were the two most common initial attack vectors. Phishing and stolen or compromised credentials were responsible for 16% and 15% of breaches, respectively, with phishing moving into the lead spot by a small margin over stolen credentials, which was the most common vector in the 2022 report. Cloud misconfiguration was identified as the initial vector for 11% of attacks, followed by business email compromise at 9%. This year, for the first time, the report examined both zero-day (unknown) vulnerabilities as well as known, unpatched vulnerabilities as the source of the data breach and found that more than 5% of the breaches studied originated from known vulnerabilities that had yet to be patched.

Although relatively rare at 6% of occurrences, attacks initiated by malicious insiders were the costliest, at an average of USD 4.90 million, which is 9.6% higher than the global average cost of USD 4.45 million per data breach. Phishing was the most prevalent attack vector and the second most expensive at USD 4.76 million. Breaches attributed to system error were the least costly, at an average of USD 3.96 million, and the least common, at 5% of occurrences.

Cost and frequency of a data breach by initial attack vector

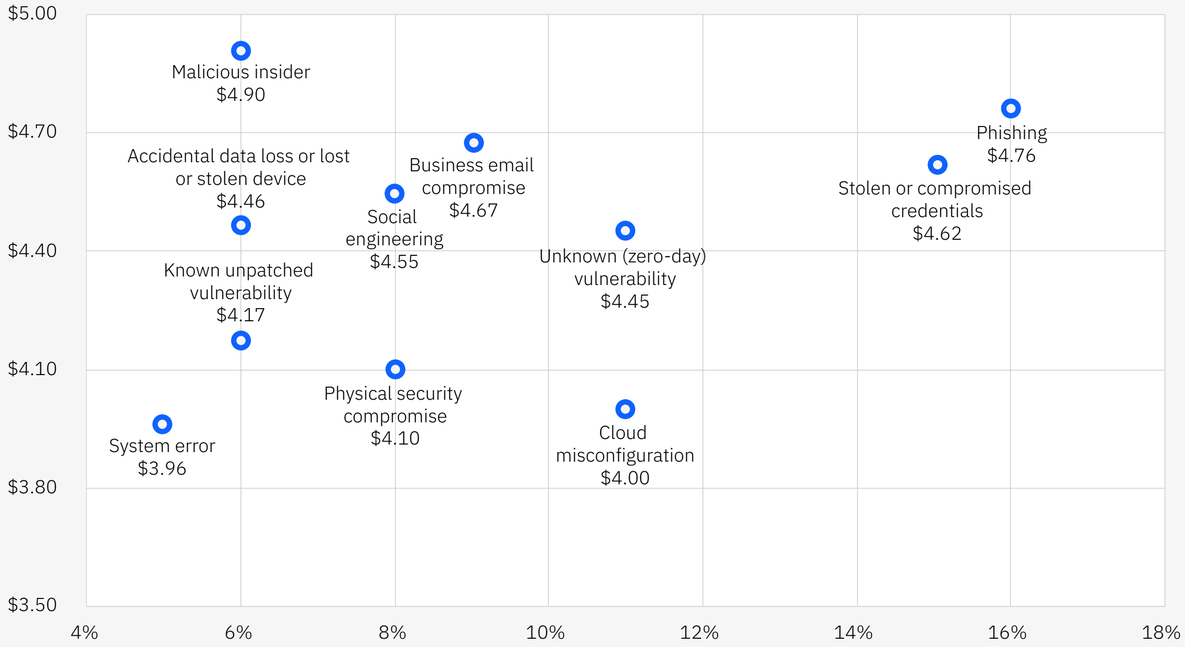


Figure 10. Measured in USD millions

Figure 11. Breaches that initiated with stolen or compromised credentials and malicious insiders took the longest to resolve.
This year, it took nearly 11 months (328 days) to identify and contain data breaches resulting from stolen or compromised credentials, on average, and about 10 months (308 days) to resolve breaches that were initiated by a malicious insider. Those two vectors, along with phishing and business email compromise, were also responsible for the costliest breaches.

As a point of comparison, the overall mean time to identify and contain a data breach was 277 days or just over nine months. That figure has remained relatively constant over the past few years of the report.

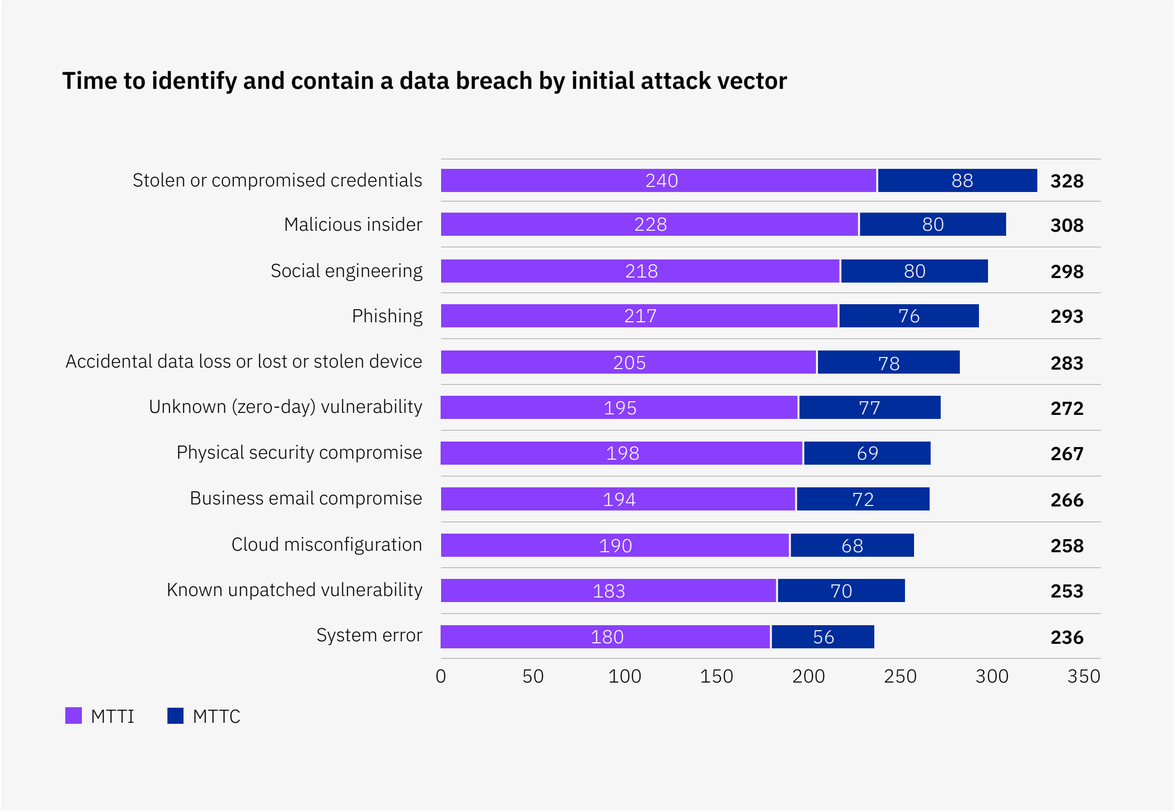
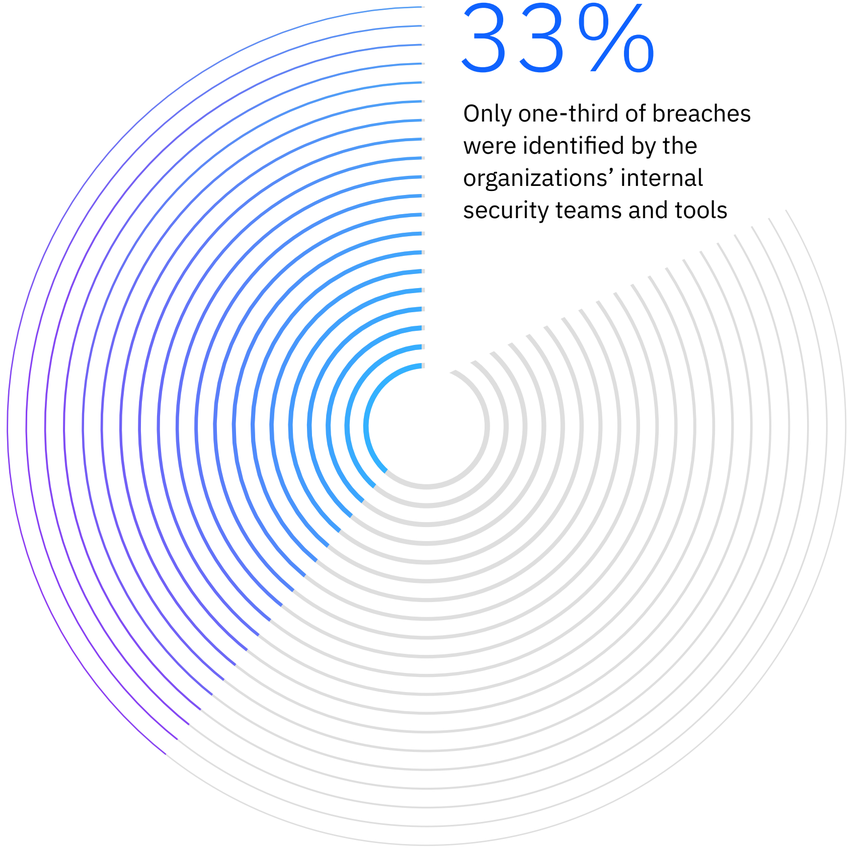


Figure 11. Measured in days

Identifying attacks

This section looks at how breaches were identified and the differences in cost and containment time based on the identification method, analyses that are reported for the first time this year. There are three categories that define how breaches are identified: by an organization's internal security teams and tools, including managed security service providers (MSSPs); by a benign third party, such as a security researcher or law enforcement; and by disclosure from the attacker, as in the case of ransomware.



33%

Only one-third of breaches were identified by the organizations' internal security teams and tools

Figure 12. Breaches were most commonly identified by a benign third party.
40% of breaches were identified by a benign third party or outsider, whereas 33% of breaches were identified by internal teams and tools. Over one-quarter or 27% of breaches were disclosed by the attacker as part of a ransomware attack.

Figure 13. Data breaches disclosed by the attacker, such as with ransomware, cost significantly more.
Attacks disclosed by attackers had an average cost of USD 5.23 million, which was a 19.5% or USD 930,000 difference over the average cost of breaches identified through internal security teams or tools of USD 4.30 million. Additionally, breaches disclosed by attackers cost 16.1% or USD 780,000 more than the USD 4.45 million average cost of a data breach for 2023. Breaches identified by an organization's own security teams and tools were significantly less expensive, costing nearly USD 1 million less than incidents disclosed by the attacker.

How was the breach identified?

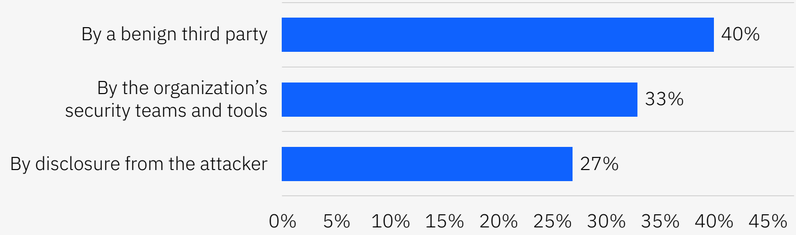


Figure 12. Only one response permitted

Cost of a data breach by how the breach was identified

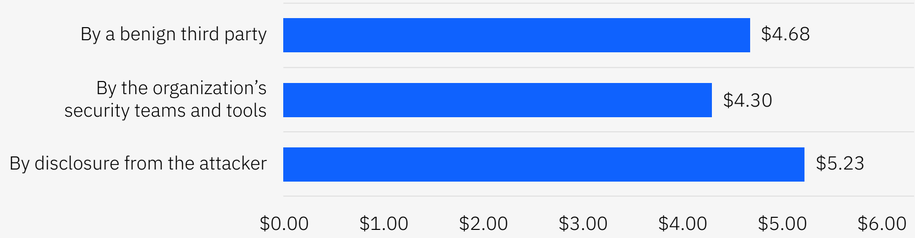


Figure 13. Measured in USD millions

Figure 14. Data breaches disclosed by the attacker also took the longest time to identify and contain.
Respondents required a mean time of 320 days to identify and contain breaches disclosed by the attacker. This time frame was 80 additional days or 28.2% longer compared to breaches identified internally, which took a mean time of 241 days to identify and contain. The mean time to identify and contain a breach disclosed by the attacker took 47 days or 15.9% longer compared to breaches identified by a benign third party.

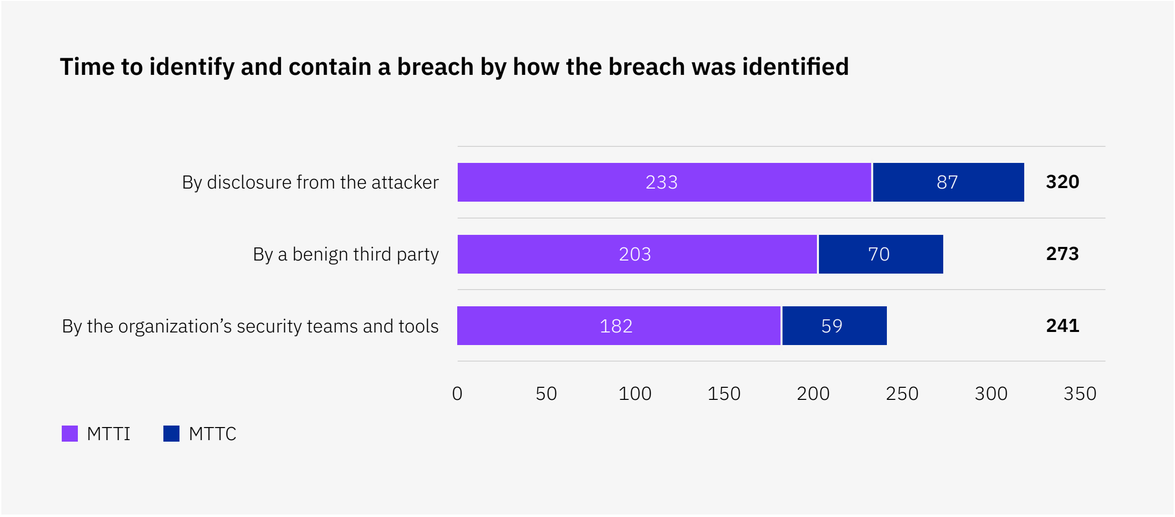


Figure 14. Measured in days

Data breach lifecycle

The data breach lifecycle is defined as the elapsed time between the initial detection of the breach and its containment. “Time to identify” describes the time, in days, it takes to discover an incident. “Time to contain” refers to the time, in days, it takes for an organization to resolve the situation and restore service after the breach has been detected. These two metrics help determine the effectiveness of an organization’s IR and containment processes.

277 days

Time to identify and contain a data breach

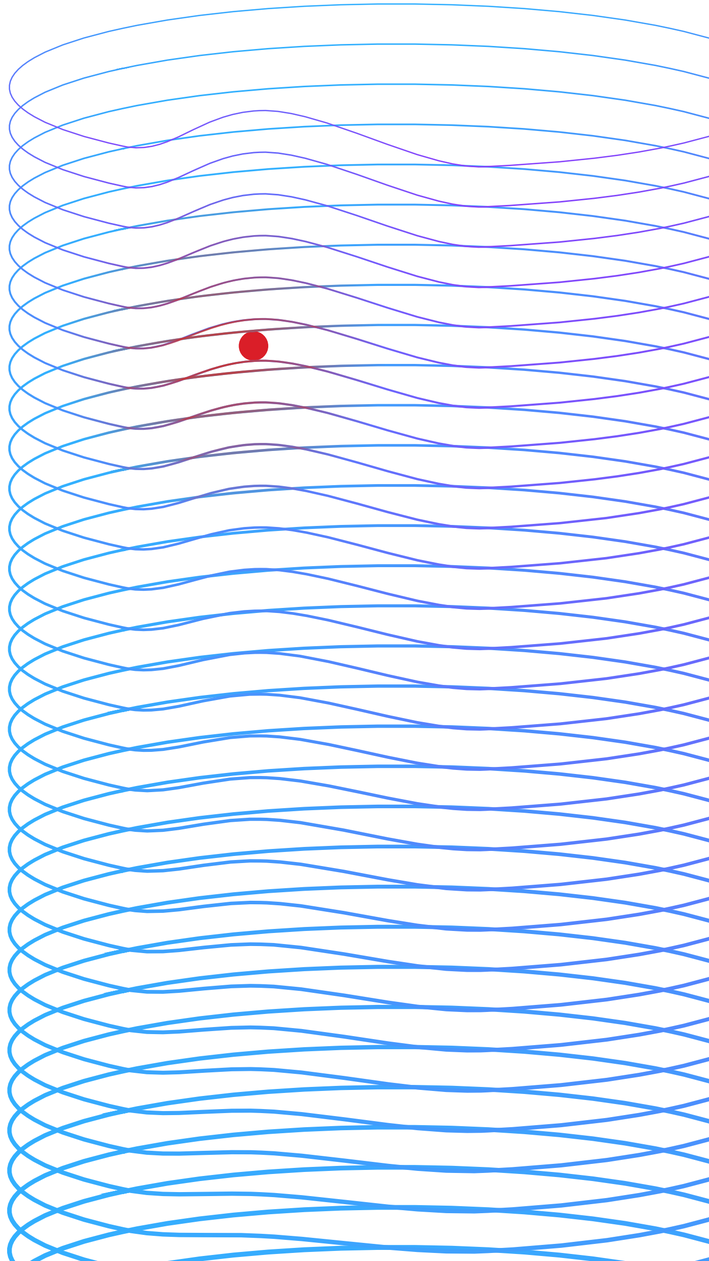


Figure 15. A shorter data breach lifecycle continues to be associated with lower data breach costs.
A shorter data breach lifecycle of fewer than 200 days was associated with an average cost of USD 3.93 million, while a longer lifecycle of more than 200 days was associated with an average cost of USD 4.95 million. This reflects a 23% difference and a cost savings of USD 1.02 million for the shorter lifecycle.

Looking back at previous years, the average cost of a data breach based on the 200-day lifecycle has been relatively consistent, although it changed incrementally.

For a data breach lifecycle of fewer than 200 days, the 2023 value of USD 3.93 million grew 5.1% from the previous year's average cost of USD 3.74 million. For a data breach lifecycle of more than 200 days, the 2023 value of USD 4.95 million grew 1.9% from the previous year's average cost of USD 4.86 million. The average cost savings of USD 1.02 million reported in 2023 reflects an 8.9% decrease from 2022's cost savings of USD 1.12 million.

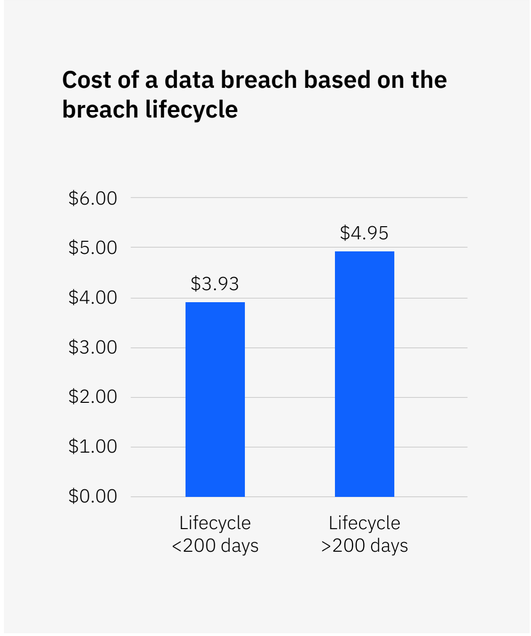


Figure 15. Measured in USD millions

Key cost factors

The types of security technologies and practices employed within an organization are among many factors that influence the mean cost of a data breach. This section quantifies 27 cost factors to help security and risk decision-makers understand the degree to which these factors amplify or mitigate costs. These factors aren't additive, so it's not consistent with the research methodology to add multiple cost factors together to calculate the potential cost of a breach.

This year, the Cost of a Data Breach Report considers several new factors, including supply chain breaches, ASM tools, data security and protection software, endpoint detection and response (EDR) tools, threat intelligence, proactive threat hunting, IR teams, and security orchestration, automation and response (SOAR) tools.

USD 5.36M

Average cost of a breach for organizations with high levels of security skills shortage

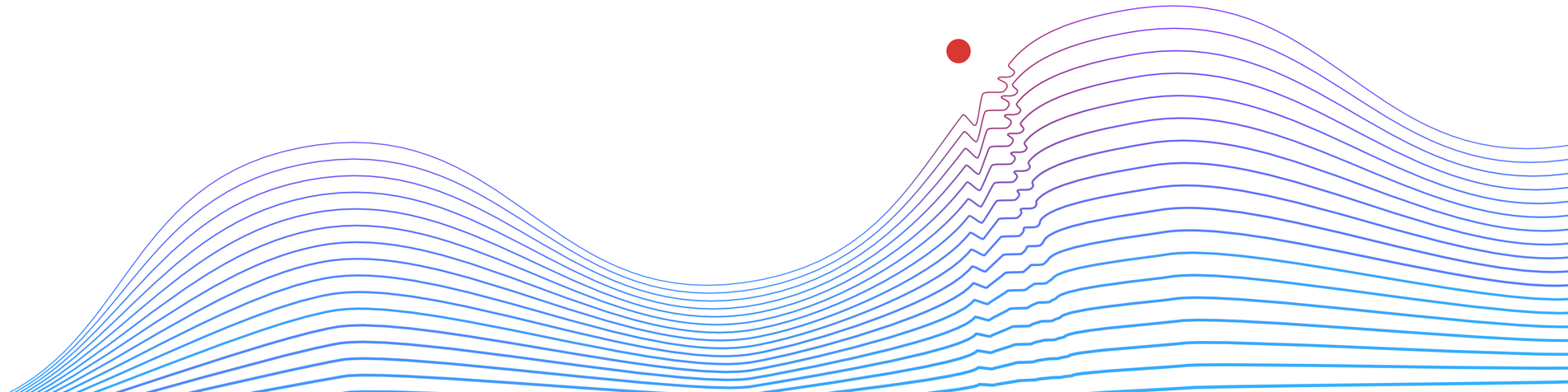


Figure 16. The impact of 27 factors on the mean cost of a data breach.
The chart demonstrates the average cost difference of breaches at organizations with these cost-influencing factors compared to the overall average data breach cost of USD 4.45 million. Cost mitigators describe those factors that are associated with a lower-than-average breach cost, while cost amplifiers are associated with a higher-than-average breach cost.

The three factors that rank most effective as cost mitigators—those associated with the biggest cost reduction—are the adoption of a DevSecOps approach, employee training, and IR planning and testing. For example, breaches at organizations with a DevSecOps approach in place had an average cost that was USD 249,000 less than the 2023 mean cost of a data breach of USD 4.45 million or approximately USD 4.20 million.

The biggest cost amplifiers were security system complexity, security skills shortage, and noncompliance with regulations. For example, breaches at organizations with security system complexity had an average cost of USD 241,000 more than the 2023 mean cost of a data breach of USD 4.45 million or approximately USD 4.69 million.

Impact of key factors on total cost of a data breach

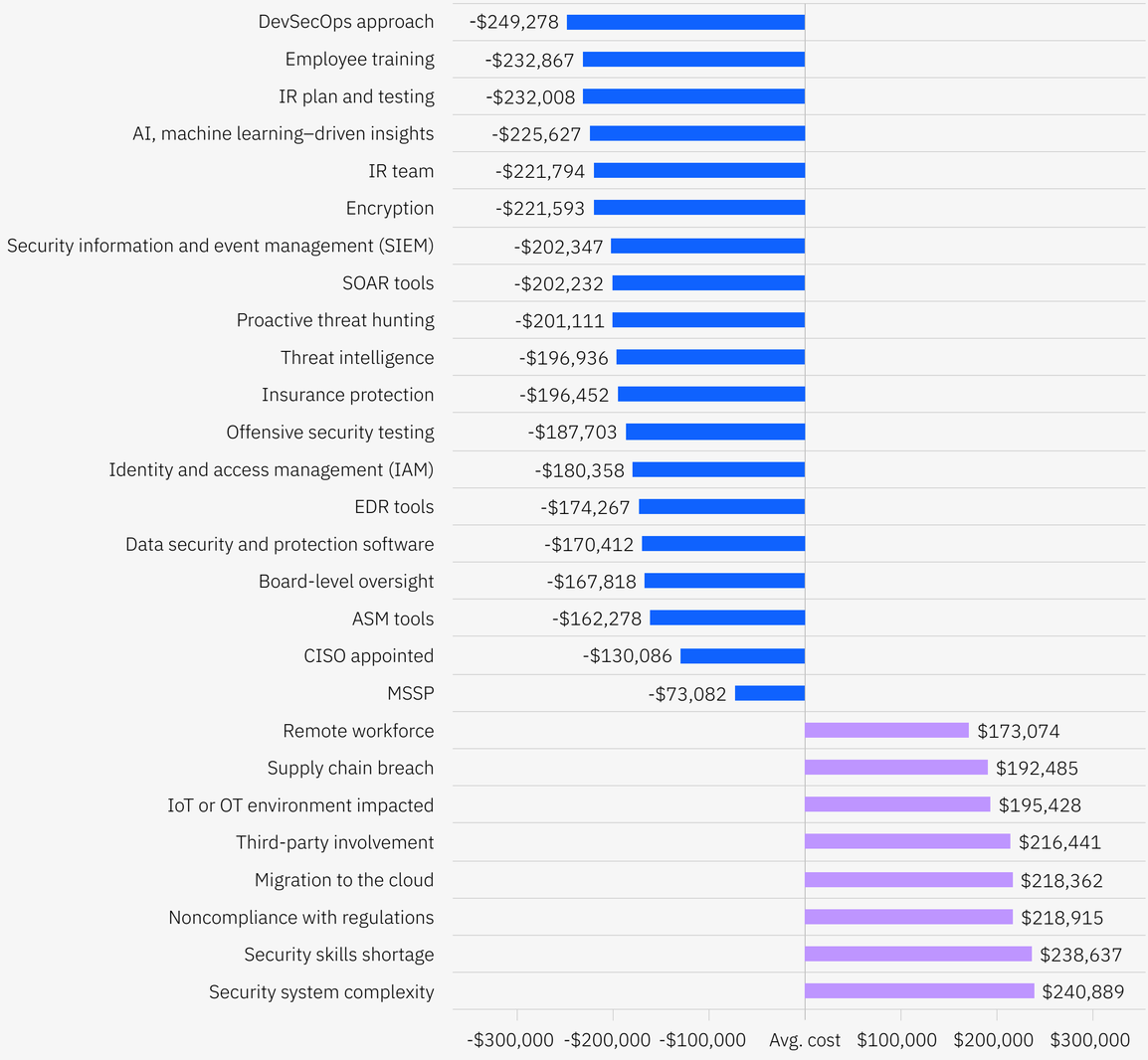


Figure 16. Measured in USD

Figure 17. The three most impactful cost amplifiers out of 27 factors.
This chart compares organizations with the highest levels of a top-ranking cost amplifier to those with the lowest level, which in some cases could mean no instance of that same factor. This comparison differs from the prior analysis (Figure 16) in which a high presence of these factors is compared to the mean. There was a difference of USD 1.58 million or 34.6% between high levels and low levels of secrity skills shortage. A difference of USD 1.44 million or 31.6% occurred between high levels and low levels of security system complexity. And there was a difference of USD 1.04 million or 23% between high levels and low levels of noncompliance with regulations.

Organizations with a high level of security skills shortage had a USD 5.36 million average cost, which was USD 910,000 higher than the average cost of a data breach, a difference of 18.6%. Those with a high level of security system complexity had a USD 5.28 million average cost, for a difference of USD 830,000 or 17.1% compared to the average cost of a data breach. Organizations with a high level of noncompliance with regulations showed an average cost of USD 5.05 million, which exceeded the average cost of a data breach by USD 560,000, a difference of 12.6%.

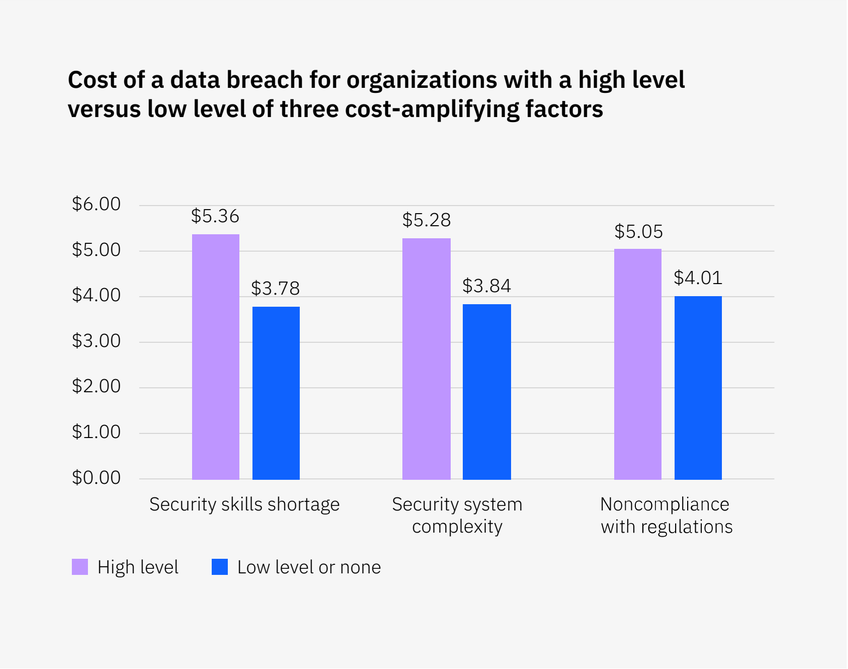


Figure 17. Measured in USD millions

Figure 18. The three most impactful cost mitigators out of 27 factors.
The chart compares organizations with the highest levels of a top-ranking cost mitigator to those with the lowest level, which in some cases could mean no instance of that same factor. The average cost of a breach showed a difference of USD 1.68 million or 38.4% between organizations with high levels and low levels of a DevSecOps approach. There was a difference of USD 1.49 million or 34.1% between high levels and little to no IR planning and testing. And last, there was a difference of USD 1.5 million or 33.9% between high levels and low levels of employee training.

Organizations with high levels of these cost mitigators present had a significantly lower than average cost of a data breach. High-level DevSecOps adopters had an average cost of USD 3.54 million—a difference of USD 910,000 or 22.8% compared to the overall average cost of a data breach. Organizations with a low usage of a DevSecOps approach had an average cost of USD 5.22 million, which was significantly higher by a difference of USD 770,000 or 15.9% compared to the average cost of a data breach.

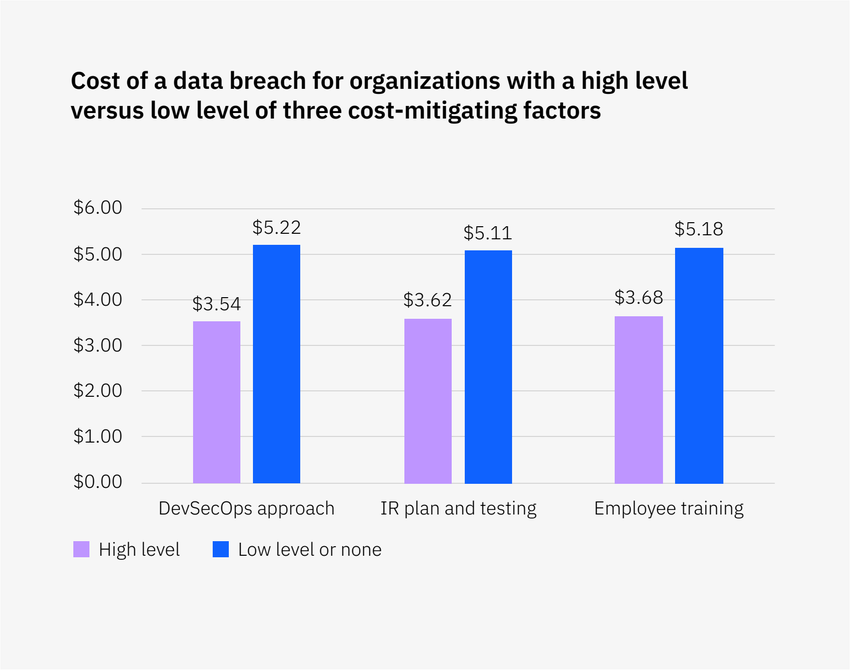


Figure 18. Measured in USD millions

Ransomware and destructive attacks

This year, ransomware and destructive attacks[3] accounted for 24% and 25% of malicious attacks, respectively.

As in the 2022 report, we looked at the lifecycle of these types of breaches and the impact of paying a ransom compared to not paying a ransom. This study doesn't include the cost of the ransom in calculating the total cost of the breach. In the 2023 report, for the first time, we examined the influence of involving law enforcement in the effort to contain a ransomware attack.

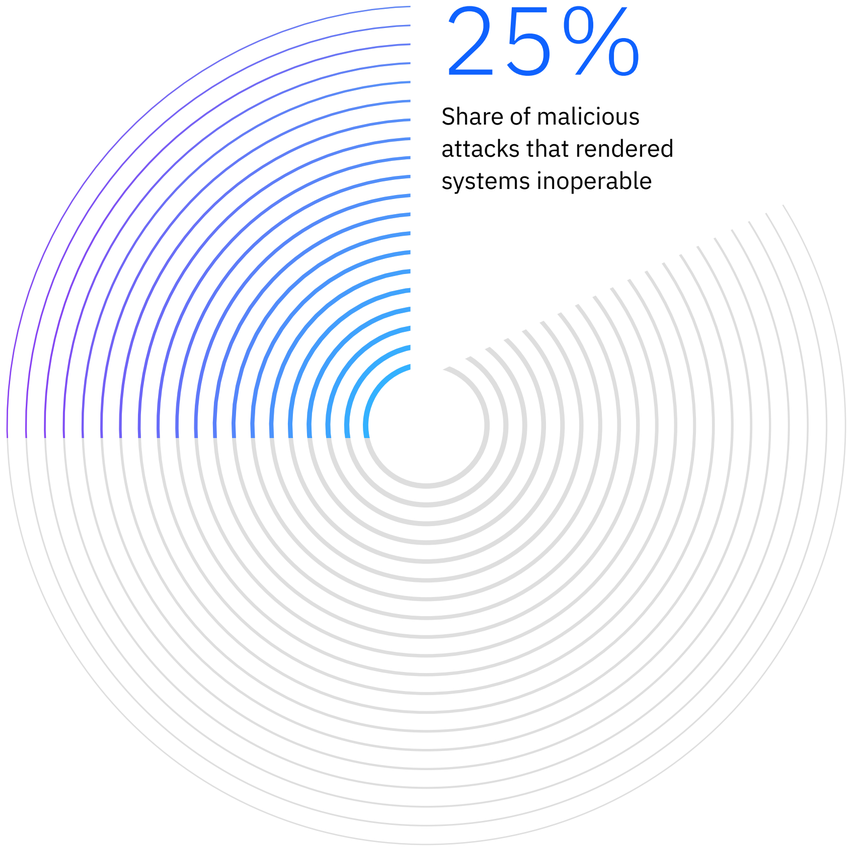


Figure 19. Nearly one-quarter of attacks involved ransomware.
Destructive attacks that left systems inoperable accounted for one out of every four attacks, and another 24% involved ransomware. Business partner and software supply chain attacks accounted for 15% and 12% of attacks, respectively.

Figure 20. Ransomware attack costs increased significantly.
At USD 5.13 million, the average cost of a ransomware attack in the 2023 report increased 13% from the average cost of USD 4.54 million in the 2022 report. At USD 5.24 million, the average cost of a destructive attack in the 2023 report also increased 2.3% from the average cost of USD 5.12 million in the 2022 report.

Share of total breaches by type of malicious attack

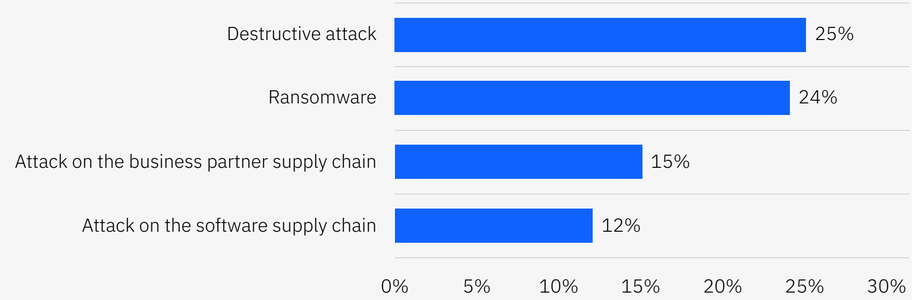


Figure 19. Percentages for each attack type shown are out of total breaches; bars will not sum to 100%

Cost of a ransomware or destructive attack

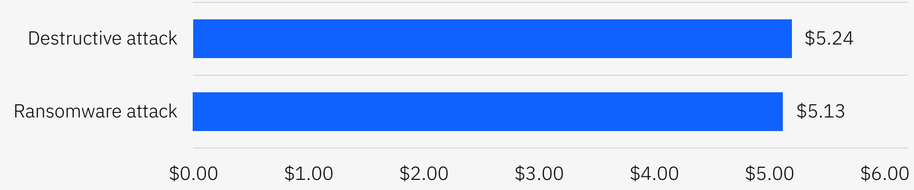


Figure 20. Measured in USD millions

Figures 21 and 22. Organizations that involved law enforcement saw significant time and cost savings.
37% of ransomware victims opted not to involve law enforcement to help contain a ransomware breach, but those that did experienced a less costly ransomware breach overall. The average cost of a ransomware breach was USD 5.11 million when law enforcement wasn't involved and USD 4.64 million when law enforcement was involved, for a difference of 9.6% or USD 470,000.

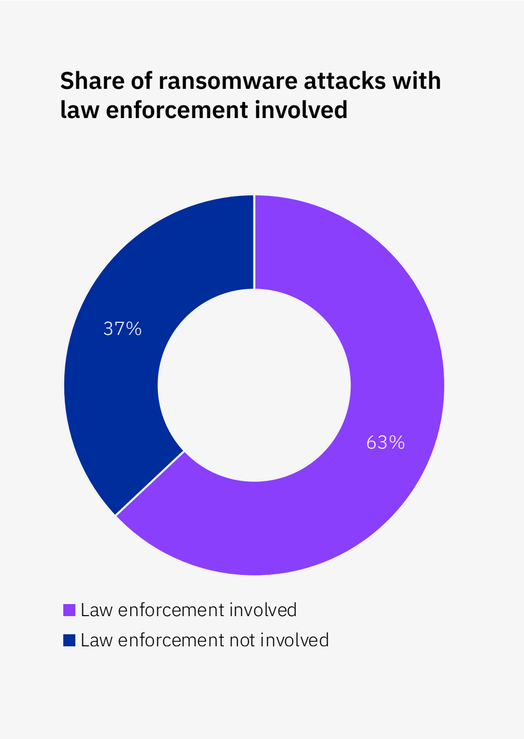


Figure 21. Share of all ransomware attacks

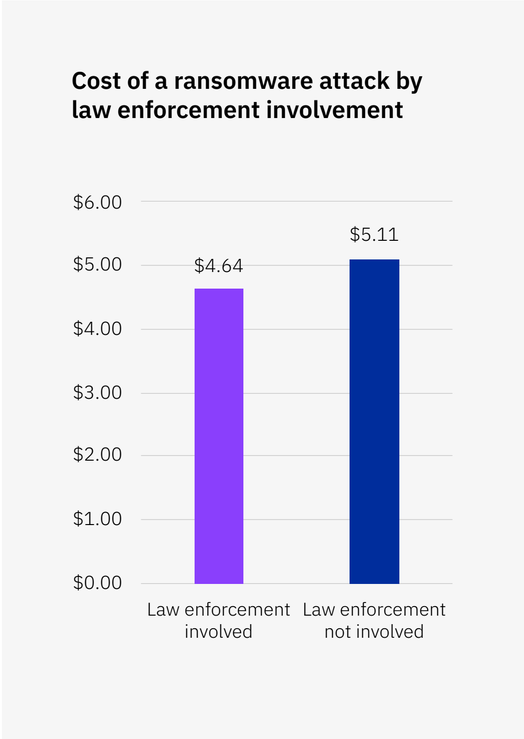


Figure 22. Measured in USD millions

Figure 23. Law enforcement helped shorten time to identify and contain ransomware breaches.
Total time to identify and contain a ransomware breach was 11.4% or 33 days shorter with law enforcement involvement, at 273 days in total compared to 306 days. The mean time to contain a ransomware breach was 63 days or 23.8% shorter with law enforcement involvement compared to 80 days without. It's clear that involving law enforcement can help reduce the cost and duration of a ransomware breach.

Time to identify and contain a ransomware attack with law enforcement involvement

Figure 23. Measured in days

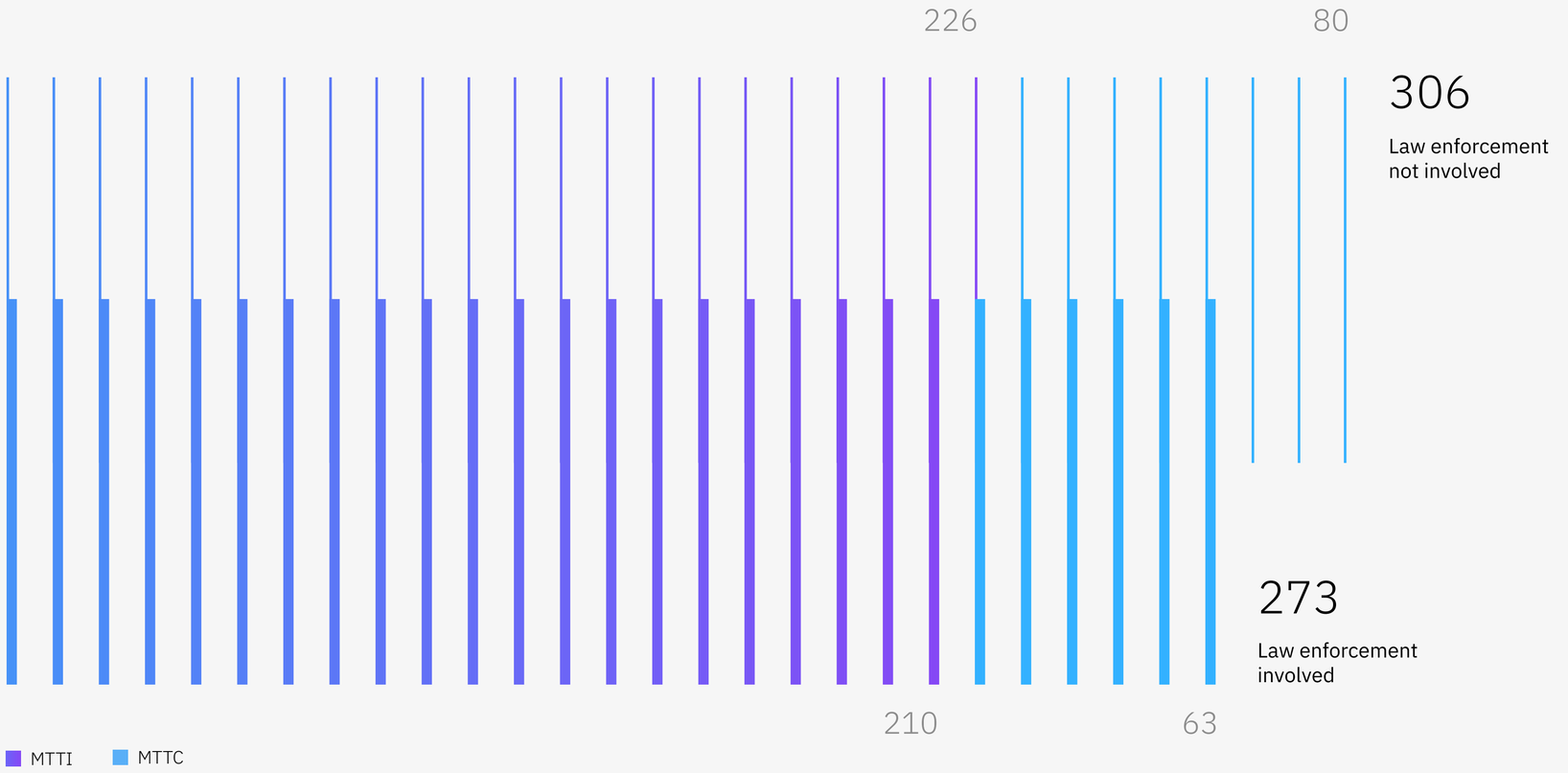


Figure 24. Automated response playbooks or workflows cut down the time to contain a ransomware breach.
Among organizations that experienced a ransomware attack, those that had automated response playbooks or workflows designed specifically for ransomware attacks were able to contain them in 68 days or 16% fewer days compared to the average of 80 days for organizations without automated response playbooks or workflows.

Figure 25. Paying the ransom led to minimal cost savings.
Organizations that paid the ransom during a ransomware attack achieved only a small difference in total cost, at USD 5.06 million compared to USD 5.17 million, a cost difference of USD 110,000 or 2.2%. However, this calculation doesn't include the cost of the ransom itself. Given the high cost of most ransomware demands, organizations that paid the ransom likely ended up spending more overall than those that didn't pay the ransom. In the 2022 report, the total cost savings were USD 630,000, with a total cost difference of 13.1%, again not including the cost of the ransom itself. The data shows that paying a ransom has become increasingly less advantageous overall, with an 82.5% decrease in savings from the 2022 to 2023 reports.

Impact of automated response playbooks or workflows for ransomware on time to contain a ransomware breach

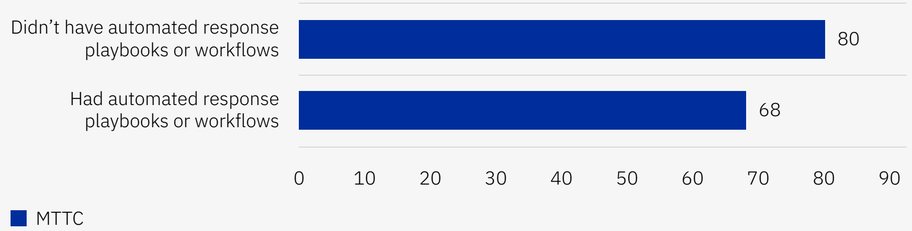


Figure 24. Measured in days

Cost of a ransomware attack based on whether the ransom was paid

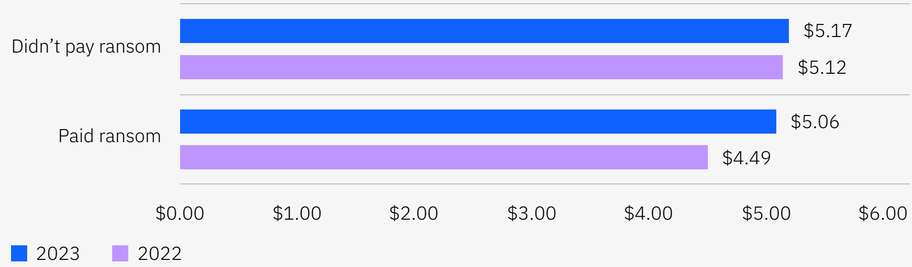


Figure 25. Measured in USD millions (cost of ransom not included)

Business partner supply chain attacks

A business partner supply chain compromise is a data breach that originates with an attack on a business partner. In this year's study, 15% of organizations identified a supply chain compromise as the source of a data breach.

Figures 26 and 27. A business partner supply chain compromise cost 11.8% more and took 12.8% longer to identify and contain than other breach types.
The cost of a data breach due to a business partner supply chain compromise averaged USD 4.76 million, which was USD 530,000 or 11.8% higher than the USD 4.23 million average cost of a data breach that was due to another cause.

Organizations took an average of 233 days to identify and 74 days to contain a business partner supply chain compromise, for a total lifecycle of 307 days. That average lifecycle was 37 days or 12.8% longer than the average lifecycle of 270 days for data breaches attributed to another cause.

Cost of a data breach due to a business partner supply chain compromise

Figure 26. Measured in USD millions

Time to identify and contain a data breach based on occurrence of a business partner supply chain compromise

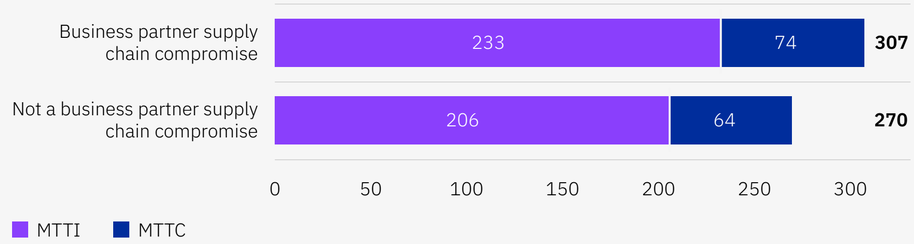
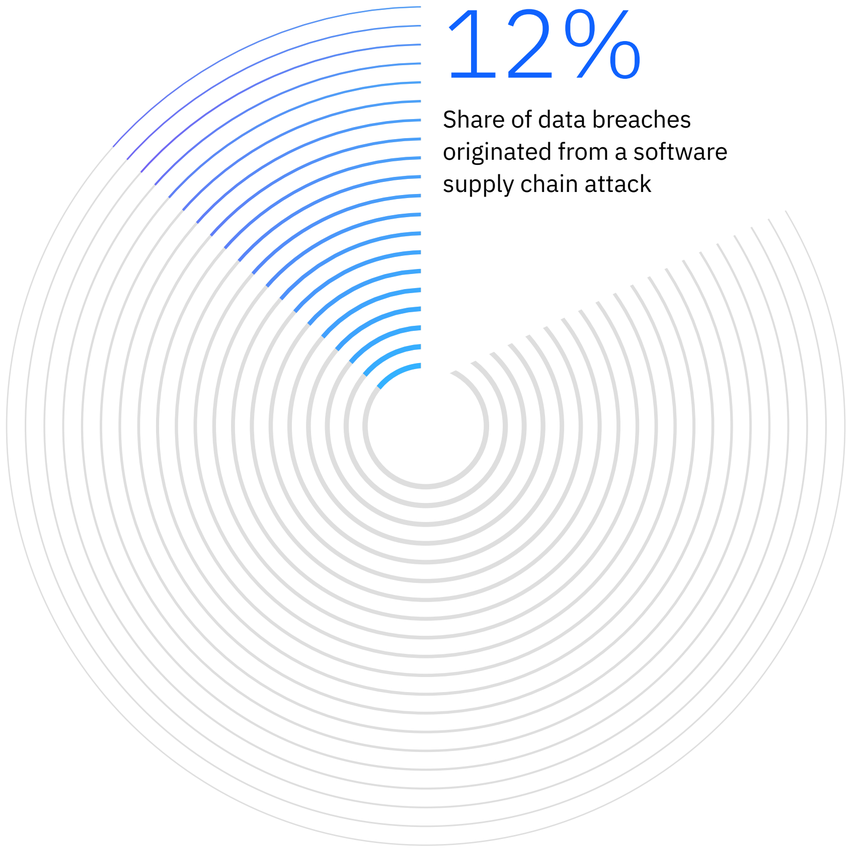


Figure 27. Measured in days

Software supply chain attacks

For the first time this year, the study also examined attacks that originated from a software supply chain attack in which an attacker infiltrates a software vendor's network and deploys malicious code to compromise the software before the vendor sends it to its customers. The compromised software then attacks the customer's data or system. In this year's study, 12% of organizations identified a software supply chain attack as the source of a data breach.



Figures 28 and 29. Software supply chain compromises cost 8.3% more and took 8.9% longer to identify and contain than other breach types.
The cost of a data breach due to a software supply chain compromise averaged USD 4.63 million, which was USD 370,000 or 8.3% higher than the USD 4.26 million average cost of a data breach that was due to another cause. A breach due to a software supply chain compromise had an 8.9% longer lifecycle, at 294 days compared to 269, than data breaches due to other causes.

Although a supply chain compromise originating from within the software supply chain is less costly than one originating from a business partner, both still cost more and take longer than the average data breach.

Cost of a data breach based on occurrence of a software supply chain compromise

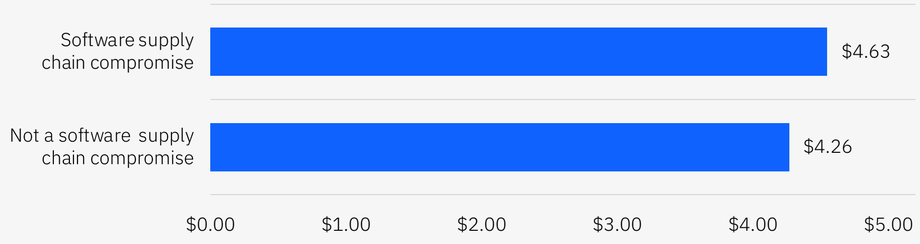


Figure 28. Measured in USD millions

Time to identify and contain a data breach based on occurrence of a software supply chain compromise

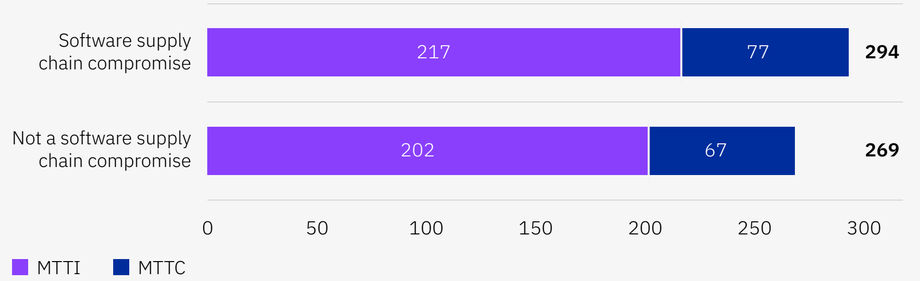


Figure 29. Measured in days

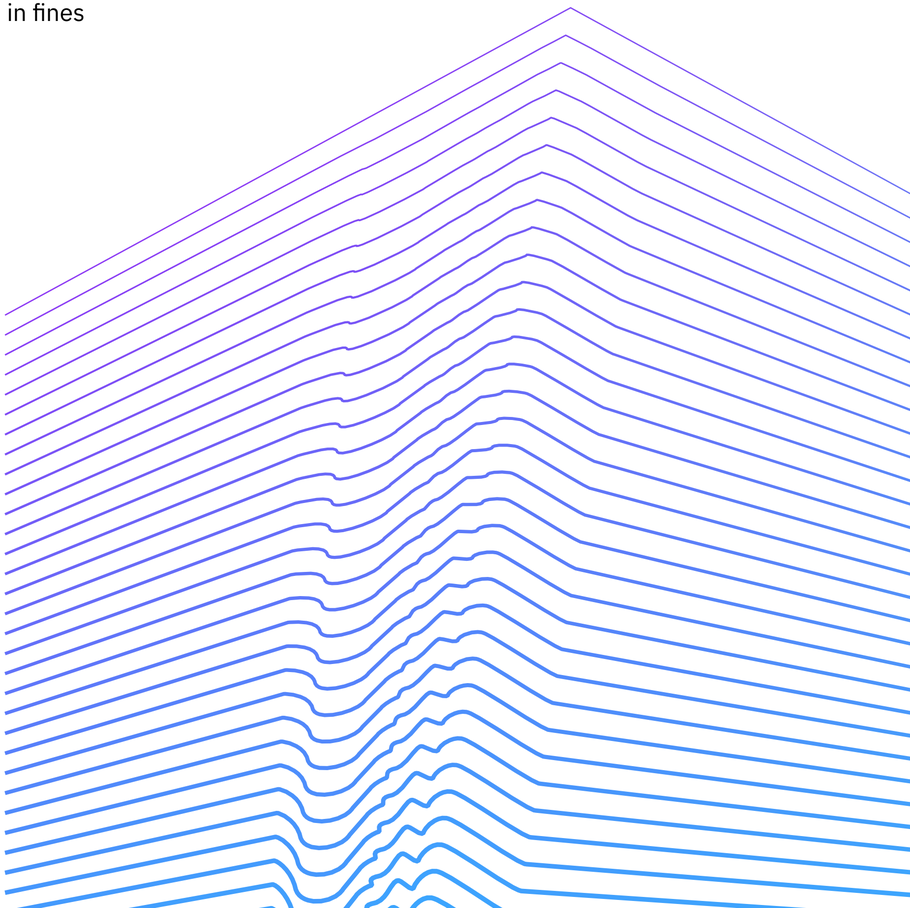
Regulatory environments

The research examined how the degree of data regulation affected the cost of a data breach. In environments with high levels of data regulation, 58% of costs continued to accrue after the first year. In low-regulation environments, 64% of the costs associated with a breach were more likely to be resolved within the first year.

The cost of a data breach tends to change in the time elapsed since the breach. There may be different costs associated with each stage of the breach as it's identified and contained and as the compromised data is recovered or repaired.

USD 250,000

20% of organizations that experienced a data breach paid this much or more in fines



Figures 30a and 30b. Peak costs were incurred more than two years after a data breach was identified in high-data regulation environments.
Organizations in low-regulation environments took on nearly two-thirds of their data breach costs in the first year, whereas organizations in high-regulation environments took on less than half of their data breach costs in the first year. Data breach costs in low-regulation environments peaked at 21% of total costs accrued in the time frame of 6–9 months. Data breach costs in high-regulation environments peaked at 21% of total costs accrued after the two-year mark. The bulk of data breach costs in a low-regulation environment spiked early on and tapered with time. In a high-regulation environment, costs oscillated and continued to rise two years after the breach was identified.

Distribution over time of data breach costs in low-data versus high-data regulation environments

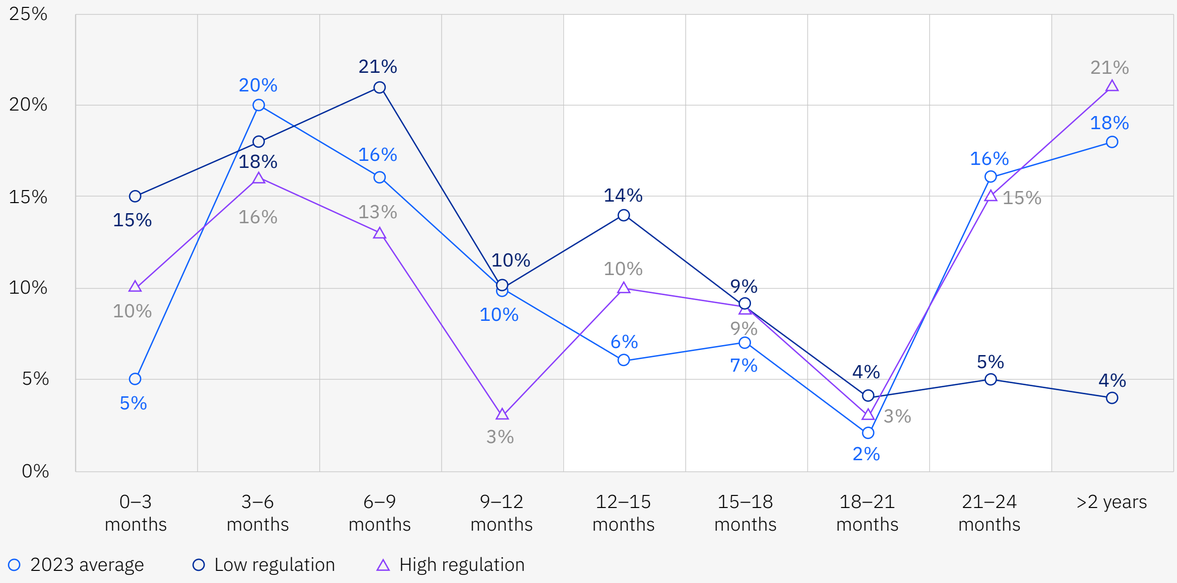


Figure 30a. Percentage of total costs accrued in three-month intervals

Distribution of data breach costs by year in low-data versus high-data regulation environments

Time elapsed since breach	Percentage of total cost		
	2023 average	Low regulation	High regulation
First year	51%	64%	42%
Second year	31%	32%	37%
Two-plus years	18%	4%	21%

Figure 30b. Percentage of total costs over the years

Figure 31. Data breach costs for critical infrastructure industries exceed USD 5 million.
Critical infrastructure organizations included those in the financial services, industrial, technology, energy, transportation, communication, healthcare, education and public sector industries. These organizations incurred data breach costs that were USD 1.26 million higher than the average cost of USD 3.78 million for organizations in other industries, a difference of 28.6%. This USD 5.04 million value also reflects a 4.6% increase of USD 4.82 million over the 2022 reported average cost of a data breach for critical infrastructure industries.

Cost of a data breach for critical infrastructure industries versus other industries

Figure 31. Measured in USD millions

Figures 32 and 33. Fewer than one-third of organizations incurred fines due to data breaches, and 80% of fines amounted to USD 250,000 or less.
Of the organizations studied, 31% incurred fines as a result of a data breach, and only 20% of those fines exceeded USD 250,000. A fine of USD 250,000 represented 5.6% of the average total cost of a data breach in the 2023 report.

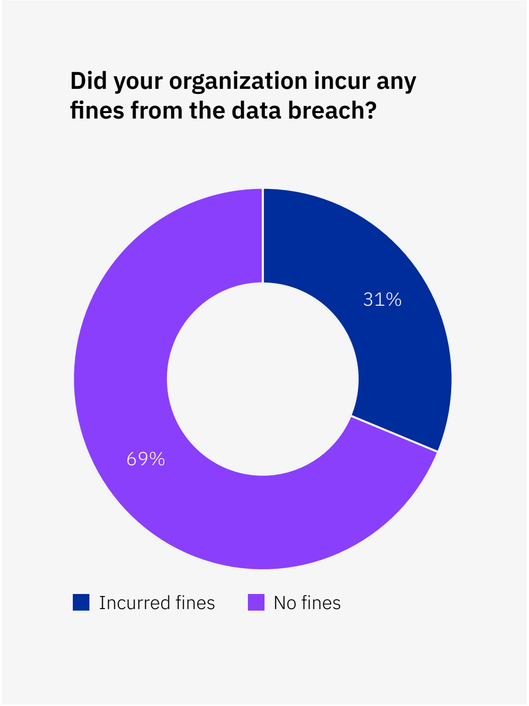


Figure 32. Share of all organizations

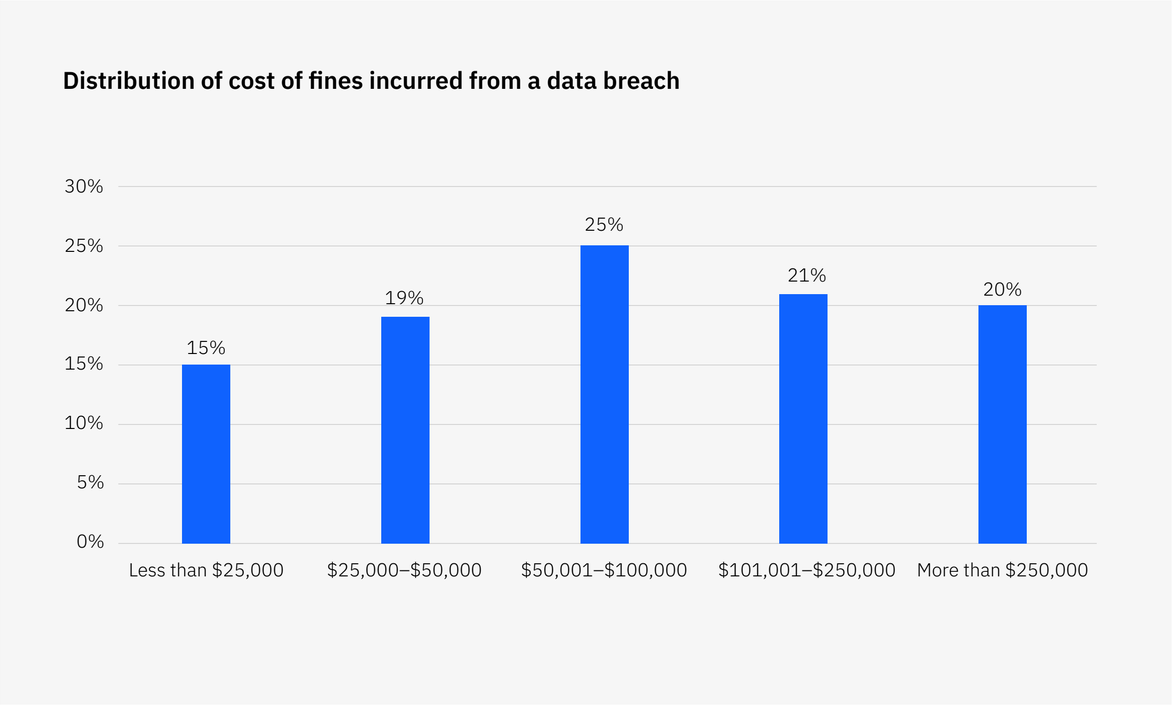
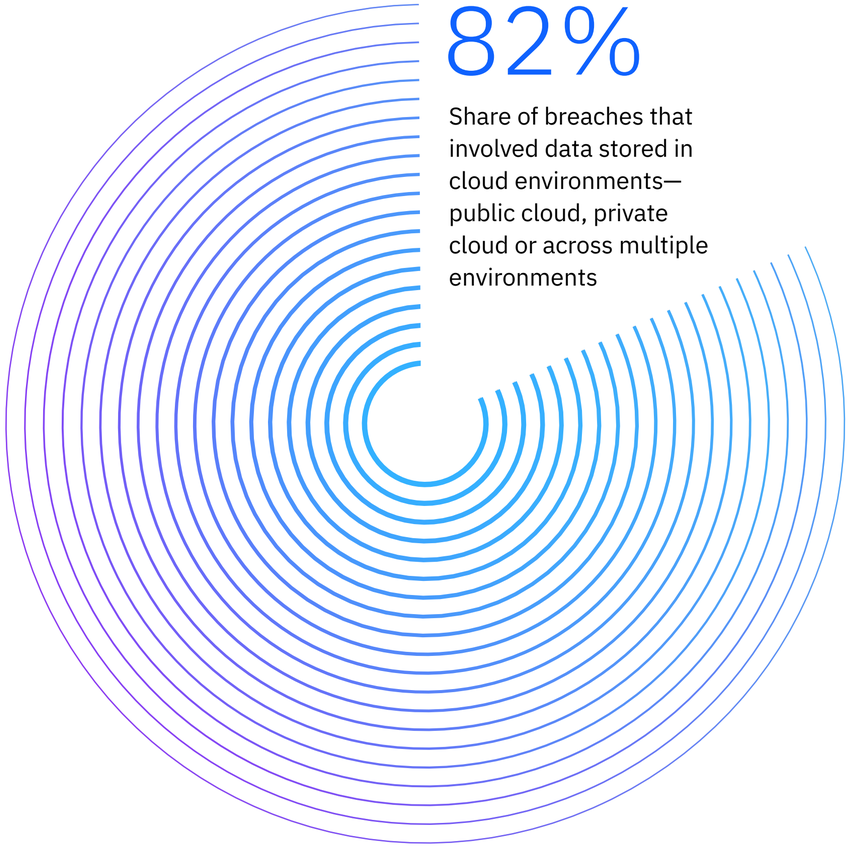


Figure 33. Among those that experienced fines, as measured in USD

Cloud breaches

The cost and duration of a breach varied depending on where the data was stored. Most commonly, the breaches studied included data that spanned multiple environments—including cloud and on premises—and breaches of this type also contributed to higher costs and longer time to identify and contain a data breach.



82%

Share of breaches that involved data stored in cloud environments—public cloud, private cloud or across multiple environments

Figure 34. Breaches most commonly impacted data stored across multiple environments.
The largest percentage of breaches, 39%, involved data stored across multiple environments, followed by 27% of breaches that involved data stored in the public cloud. The number of breaches occurring across multiple environments surpassed the combined 34% of breaches occurring only in private cloud or on-premises environments.

Figure 35. Data breaches in public clouds and multiple environments had higher costs.
In the 2023 report, the cost of data breaches across multiple environments reached USD 4.75 million, the highest cost of the environments analyzed, and 17.6% higher than the USD 3.98 million cost of data breaches in a private cloud environment, which was the lowest cost of the environments analyzed. The cost of data breaches across multiple environments also exceeded the average cost of a data breach of USD 4.45 million by a margin of 6.5%.

Where was the breached data stored?

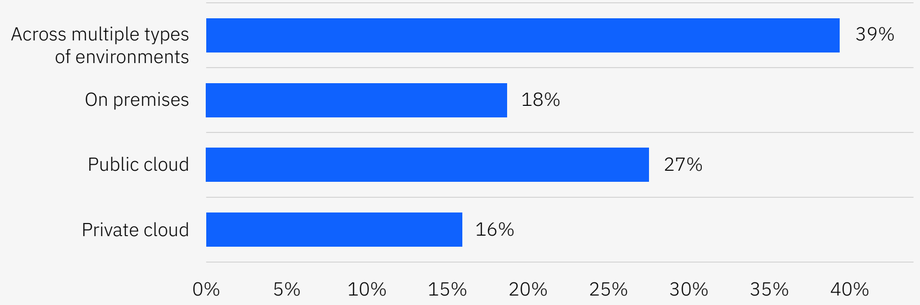


Figure 34. Share of all breaches

Cost of a data breach by storage location of breached data

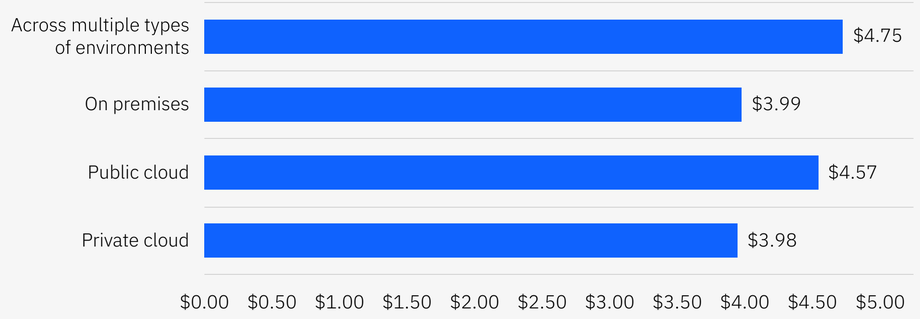


Figure 35. Measured in USD millions

Figure 36. The use of public clouds and multiple environments also contributes to longer data breach lifecycles.
The longest time to identify and contain a breach involved data stored across multiple environments, taking 291 days. This interval exceeded the shortest time to identify and contain a breach—which was 235 days in a private cloud environment—by 56 days or 21.3%. It's also worth noting that the use of multiple environments is the only model that exceeds the 2023 reported average time to identify and contain a data breach of 277 days by a margin of 14 days or 4.9%.

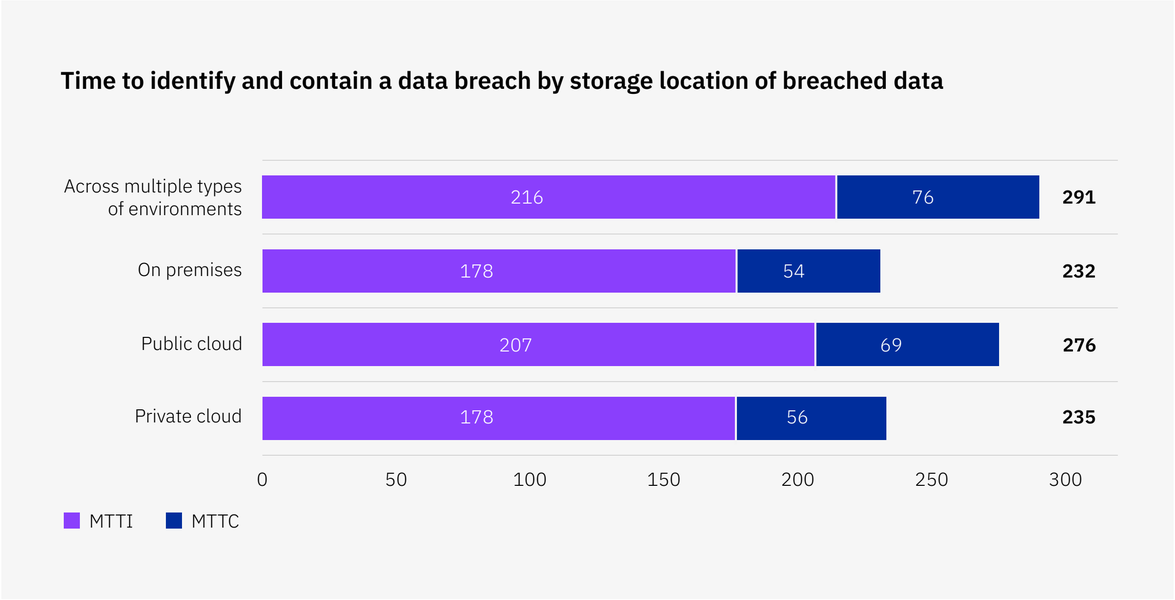
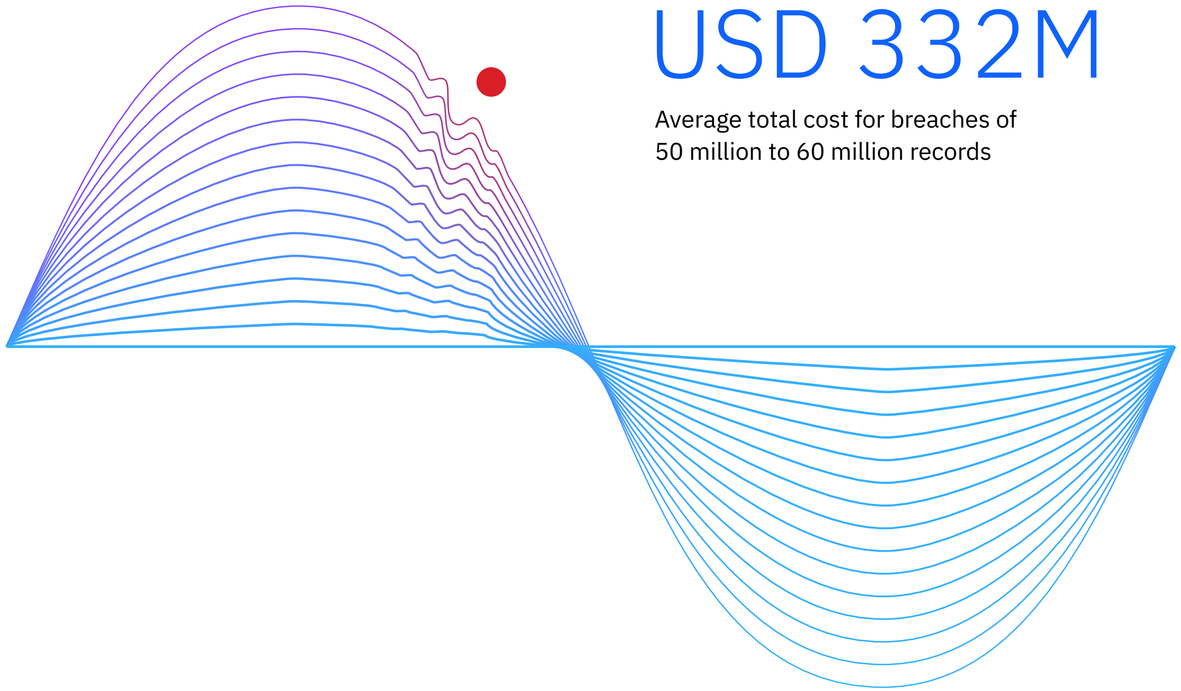


Figure 36. Measured in days

Mega breaches

Mega breaches, characterized by more than one million compromised records, are relatively rare. But they exert a powerful impact due to their outsized scope.

This year's study included 20 organizations that endured the loss or theft of between 1 million and 60 million records due to data breaches. The study deployed a distinct methodology to examine those mega breaches. They were considered separately from the study's other 553 breaches, each including no more than 101,200 lost or compromised records. For a full explanation of the research methodology, see the data breach FAQs at the end of this report.



USD 332M

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

Figure 37. The cost of mega breaches fell in the 2023 report.
Across all breach size cohorts, the average cost of a mega breach fell to varying degrees. The highest percentage decrease occurred in the 1 million to 10 million cohort, with a 26.5% decrease from USD 49 million in the 2022 report to USD 36 million in the 2023 report. The smallest percentage decrease occurred in the 30 million to 40 million cohort, with a 3.8% decrease from USD 316 million in the 2022 report to USD 304 million in the 2023 report. In the 50 million to 60 million cohort, the 2022 reported cost of USD 387 million decreased by USD 55 million or 14.2% to equal USD 332 million in the 2023 report.

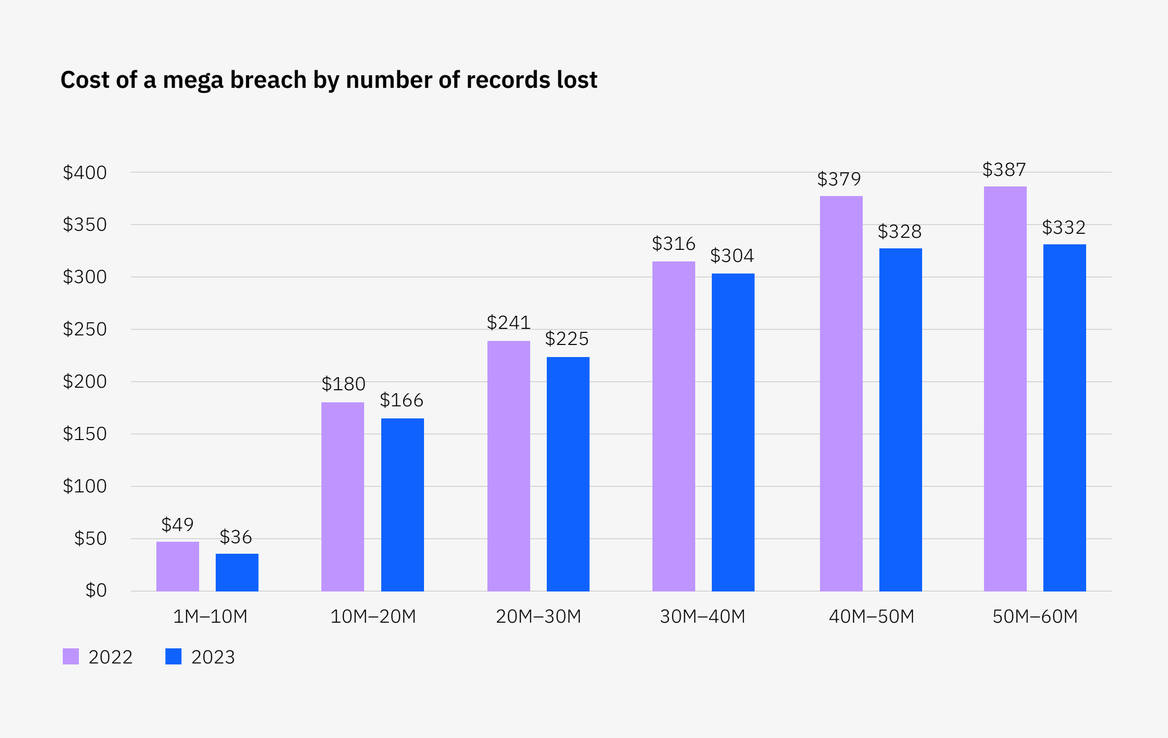


Figure 37. Measured in USD millions

Security investments

This section examines the security investment strategies that organizations adopted after experiencing a data breach. We'll explore how often organizations increased spending after a breach as well as how they chose to allocate funds.

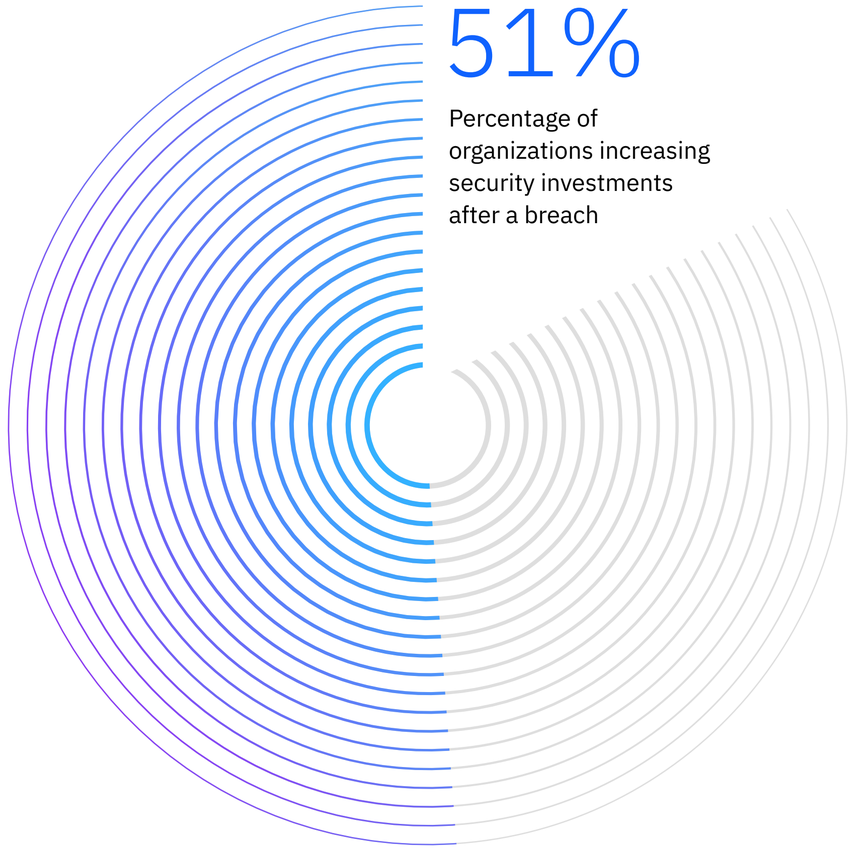


Figure 38. Respondents were split on increasing security investment after a breach.
Even as the global cost of a data breach increased, research participants reported divided perspectives on increasing security investments after an incident. 51% of respondents indicated they planned for additional security spending after the breach.

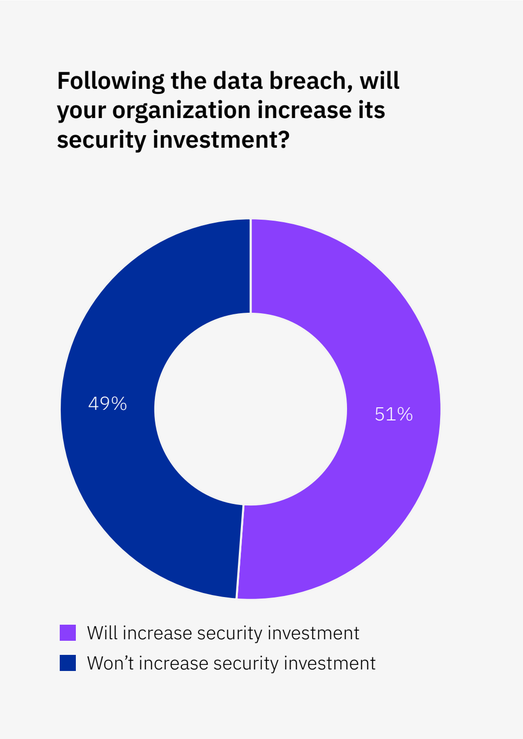


Figure 38. Percentage of all organizations

Figure 39. IR planning and testing and employee training saw significant post-breach investment.
Of the 51% that increased spending after a breach, organizations' most common investment was in IR planning and testing at 50%, followed closely by employee training at 46%. Threat detection and response technologies placed third at 38%, making them the top-ranked technology or tool investment considered in this section. Notably, these three investments map closely to top factors associated with lower data breach costs that are explored in this year's key cost factors section. At only 18% of respondents, insurance protection was the least common investment after a breach.

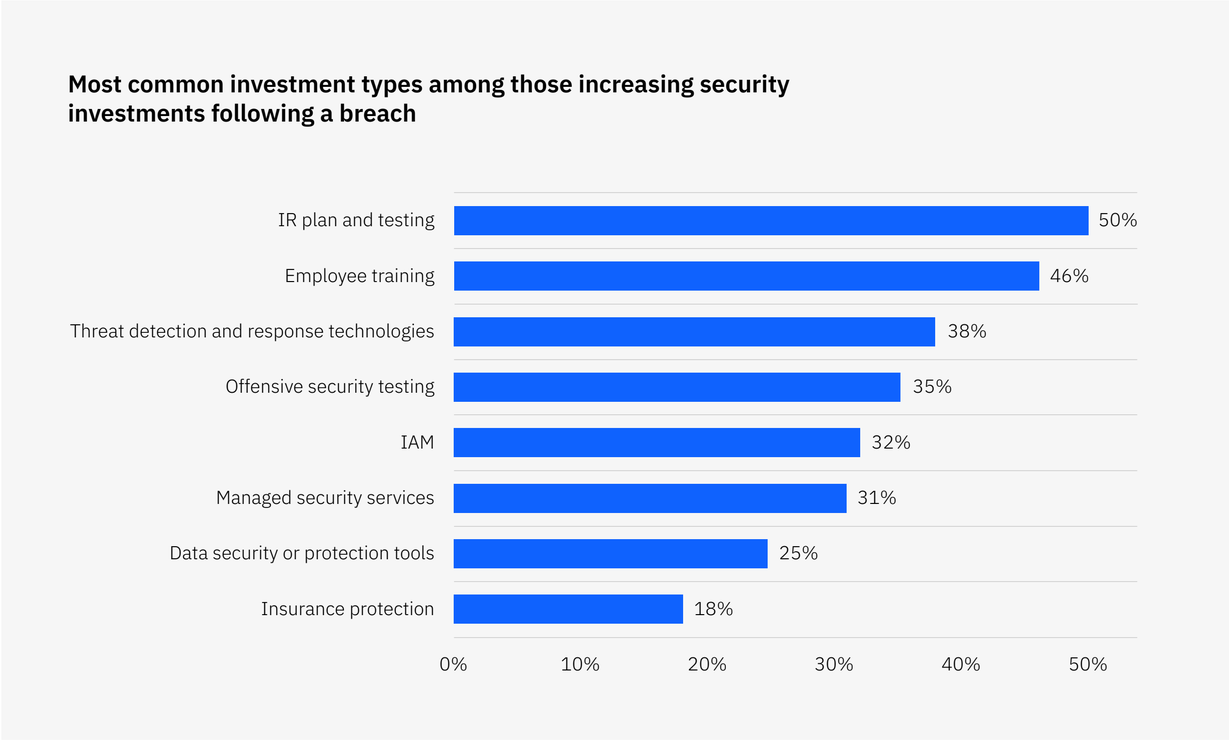


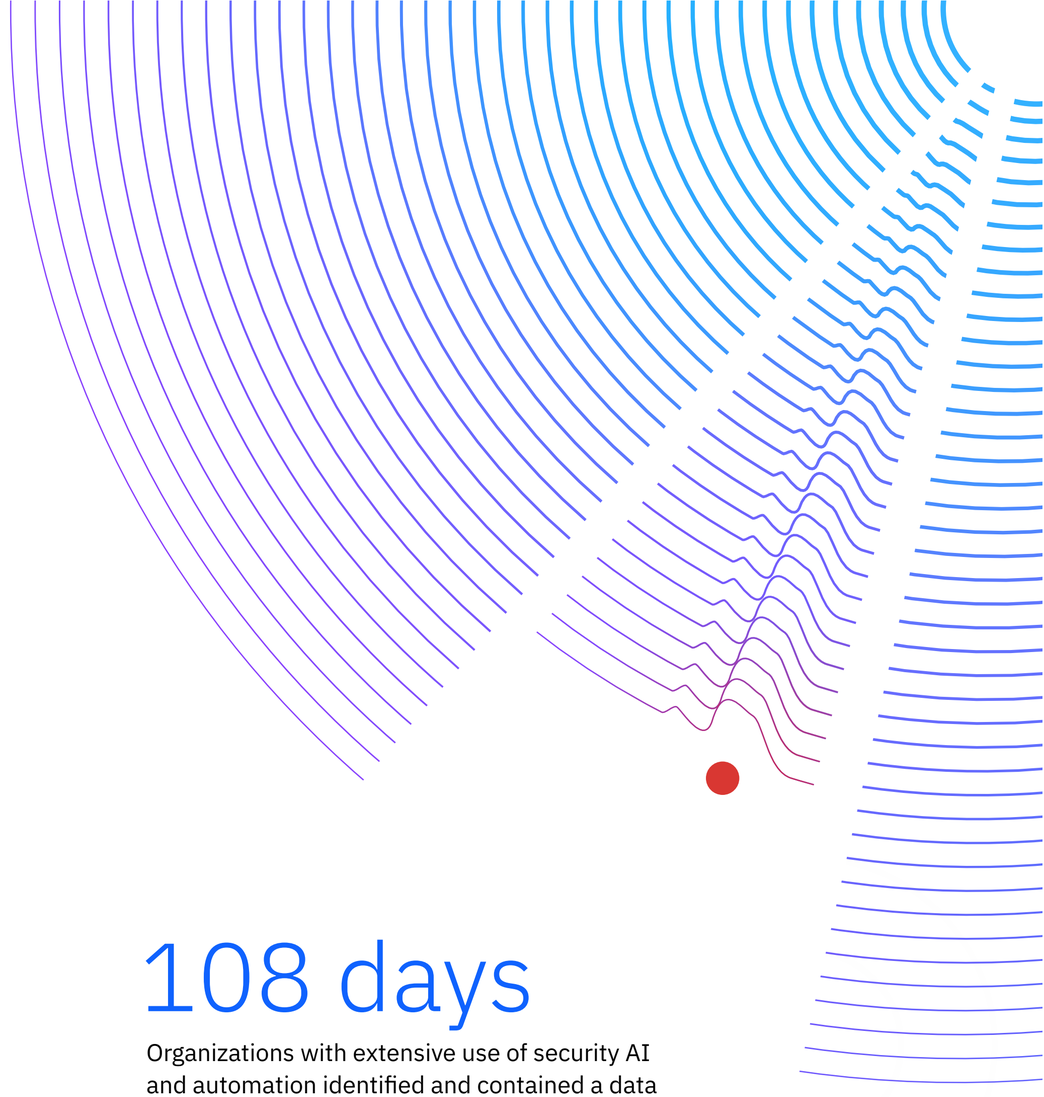
Figure 39. Share among organizations that are increasing investment; more than one response permitted

Security AI and automation

With security AI and automation use cases for the security industry advancing, this report examines the impact of these technologies on data breach costs and timelines. Examples include the use of AI, machine learning, automation and orchestration to augment or replace human intervention in detection and investigation of threats as well as the response and containment process. 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.

Though this is the sixth year of investigating the impact of AI and automation on cybersecurity, this year we're introducing new criteria that considered AI's permeation throughout an organization's security processes as opposed to its level of deployment—ranging from not deployed to partially or fully deployed—in prior years' data.

- "Extensive use" refers to the integration of security AI and automation throughout operations, including several different tool sets and capabilities.
- "Limited use" refers to applying AI to just one or two use cases within security operations.
- "No use" refers to security processes that are driven solely by manual inputs.



108 days

Organizations with extensive use of security AI and automation identified and contained a data breach 108 days faster than organizations with no use.

Figure 40. A 61% majority of organizations employ some level of security AI and automation.
Only 28% of organizations extensively used security AI and automation tools in their cybersecurity processes, while 33% had limited use. That leaves nearly 4 in 10 relying solely on manual inputs in their security operations.

Figure 41. Extensive security AI and automation use delivered cost savings of nearly USD 1.8 million.
Organizations with extensive use of security AI and automation demonstrated the highest cost savings comparatively, with an average cost of a data breach at USD 3.60 million, which was USD 1.76 million less and a 39.3% difference compared to no use. Even organizations with limited use of security AI and automation measured an average cost of a data breach of USD 4.04 million, which was USD 1.32 million less or a 28.1% difference compared to no use. However, organizations with no use of security AI and automation experienced an average cost of a data breach of USD 5.36 million. This is 18.6% more than the 2023 average cost of a data breach of USD 4.45 million.

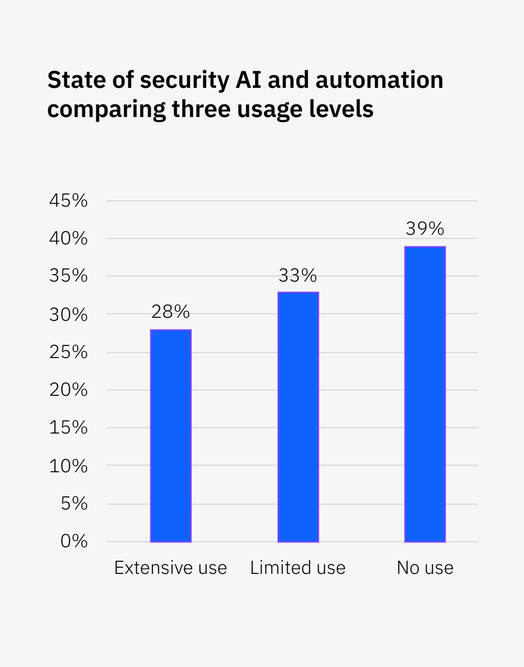


Figure 40. Percentage of organizations per usage level

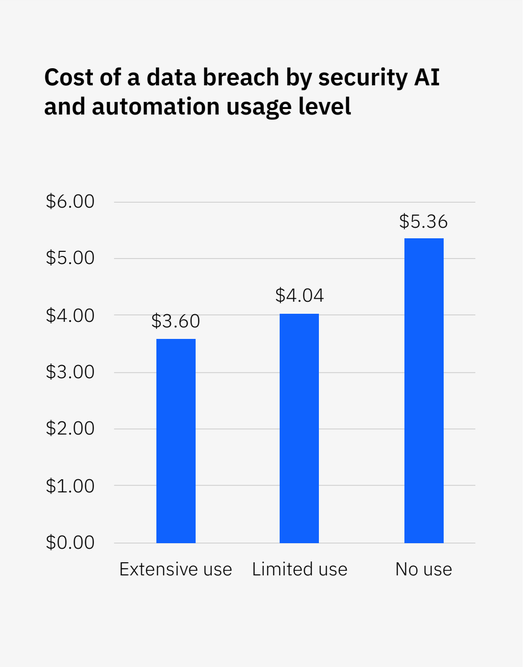


Figure 41. Measured in USD millions

Figure 42. Extensive security AI and automation reduced the time to identify and contain a breach by more than 100 days.
Respondents from organizations that extensively used security AI and automation were able to identify and contain a breach in 214 days, which was 108 days shorter than those with no use. This means identifying and containing a breach with extensive use of security AI and automation took just 66% of the time it took organizations with no use. Limited use also made a significant impact, with an average time to identify and contain a breach in 234 days, which was 88 days shorter than organizations with no use. It's clear that even a limited effort to integrate security AI and automation into security workflows can offer a significant acceleration in the time to identify and contain a breach as well as a sizable reduction in costs.

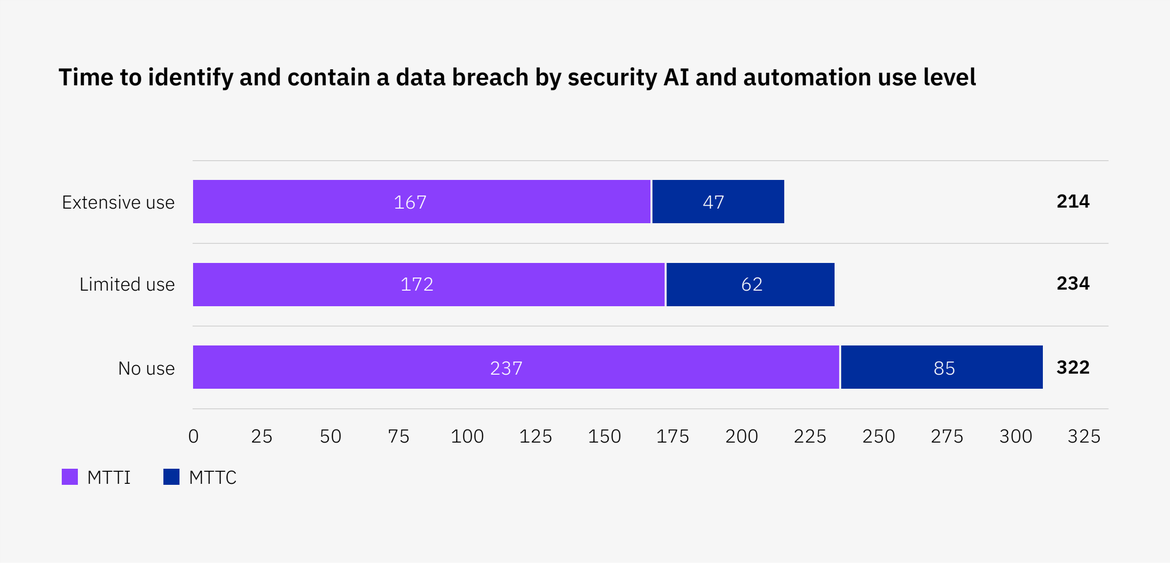
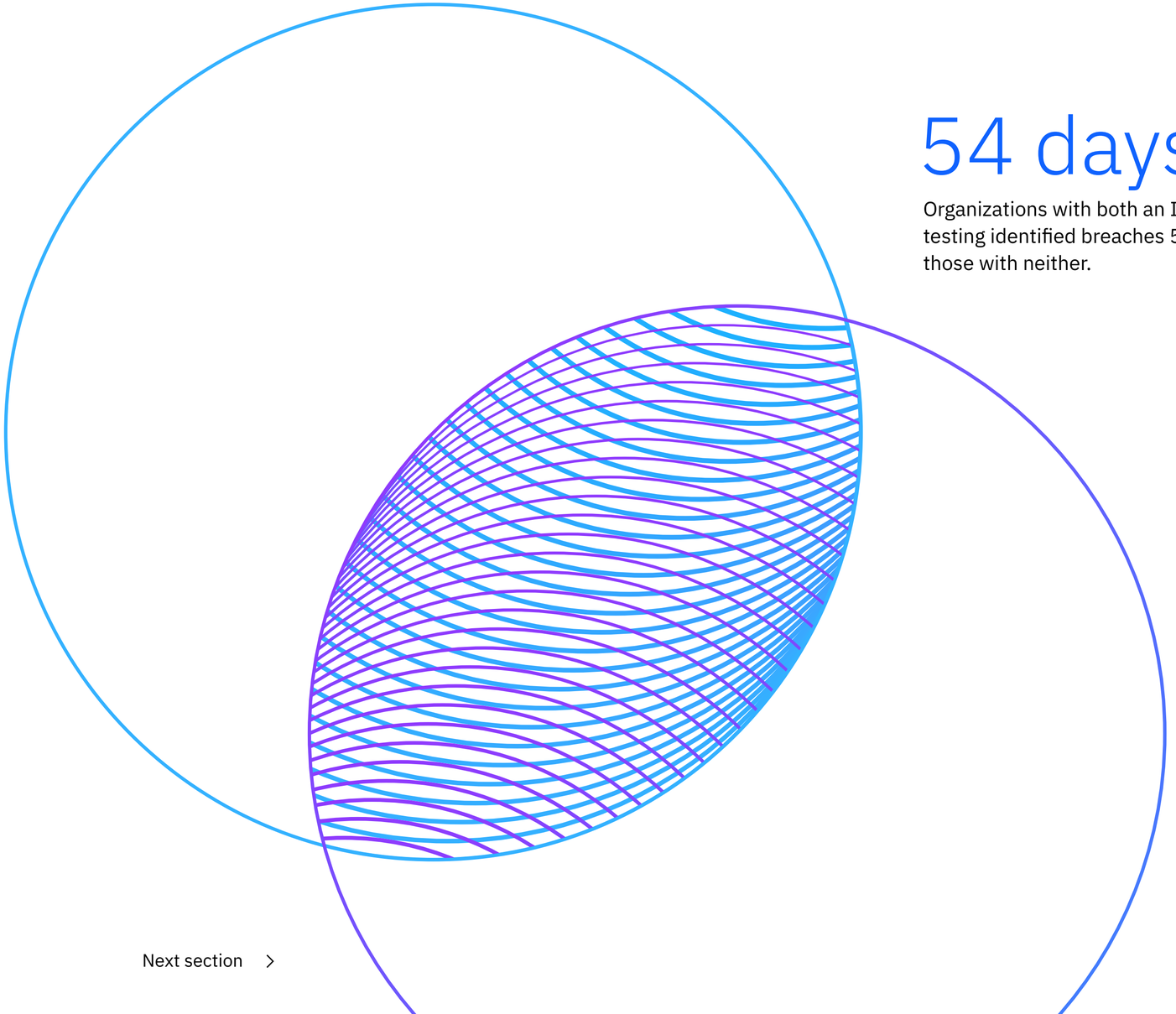


Figure 42. Measured in days

Incident response

IR strategies and tactics have been instrumental in reducing the impact of data breaches. The most effective IR strategy for reducing the duration of a data breach was to combine formation of an IR team with testing of the IR plan. However, some organizations pursued only one of those two strategies. As a standalone effort, IR plan testing was more effective than only forming an IR team in reducing the total time to identify and contain the breach.



54 days

Organizations with both an IR team and IR plan testing identified breaches 54 days faster than those with neither.

Figure 43. The combined IR strategy saved 54 days in identifying and containing a breach.
The dual strategy of forming an IR team and testing an IR plan demonstrated a shorter time, 252 days, to identify and contain a data breach compared to 306 days of employing neither approach, a difference of 54 days or 19.4%. Testing the IR plan without forming a team was nearly as effective, resulting in a difference of 48 days or 17%.

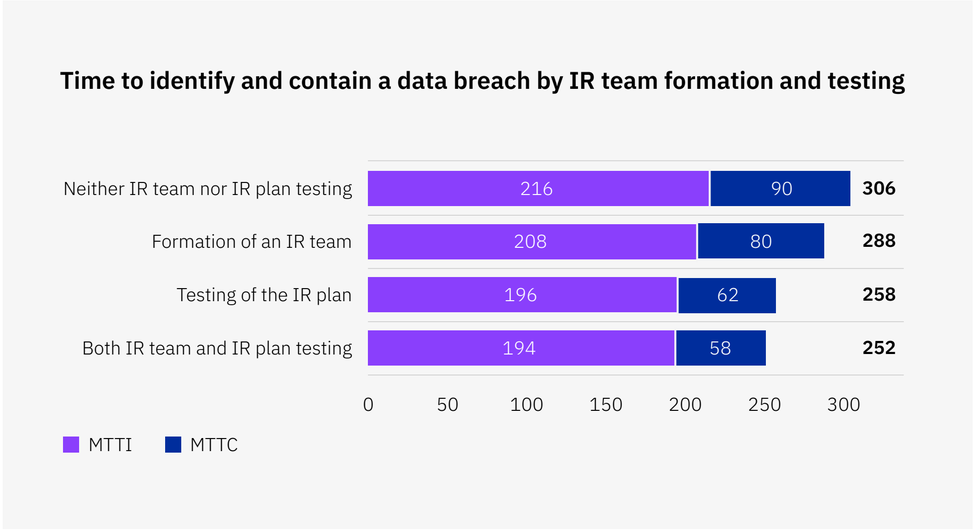
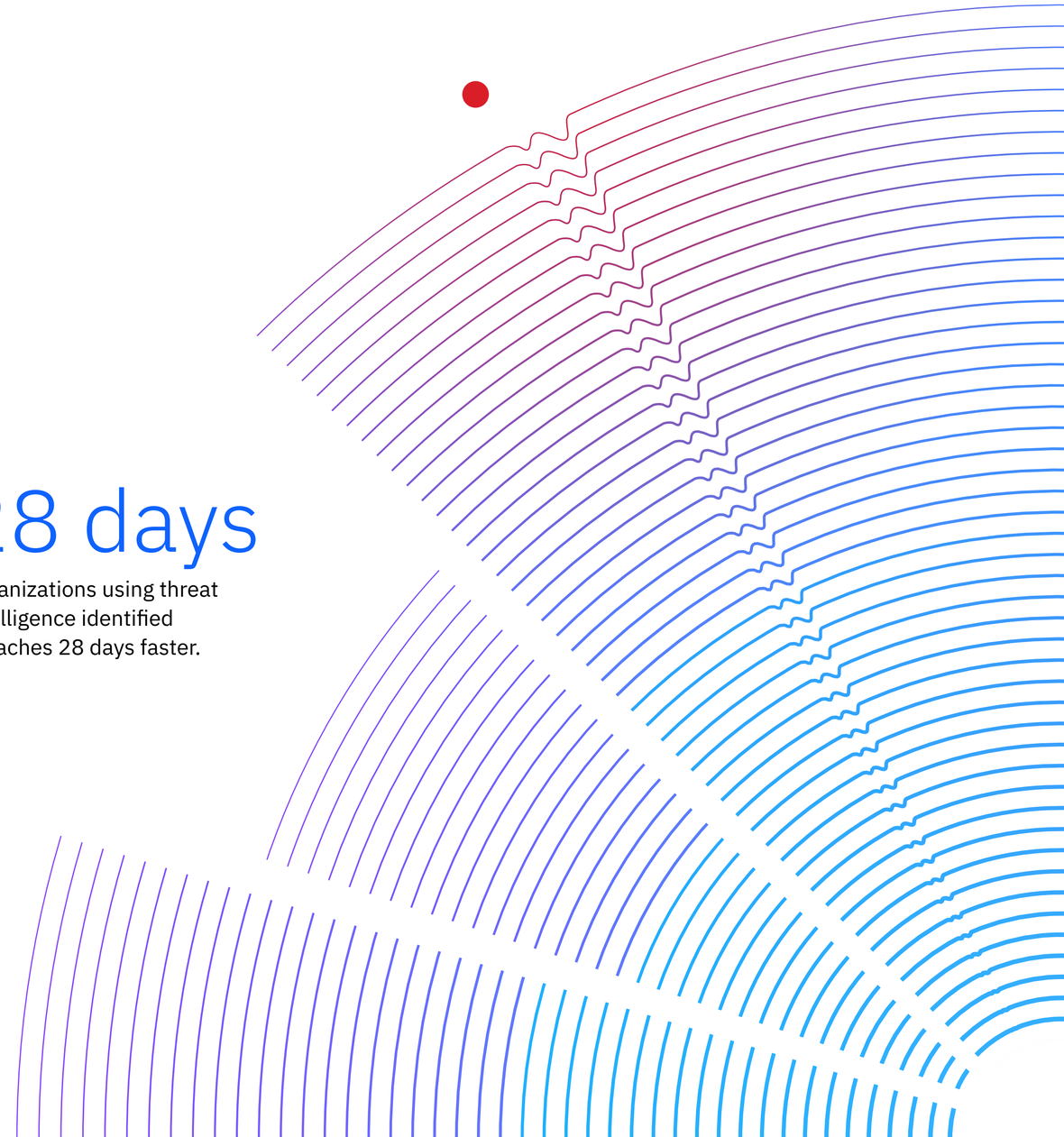


Figure 43. Measured in days

Threat intelligence

New to the report this year is the impact of threat intelligence services on the mean time to identify a breach. Threat intelligence services provide security leaders with information and insights about cyberthreats and vulnerabilities to help them improve their organization's security posture.



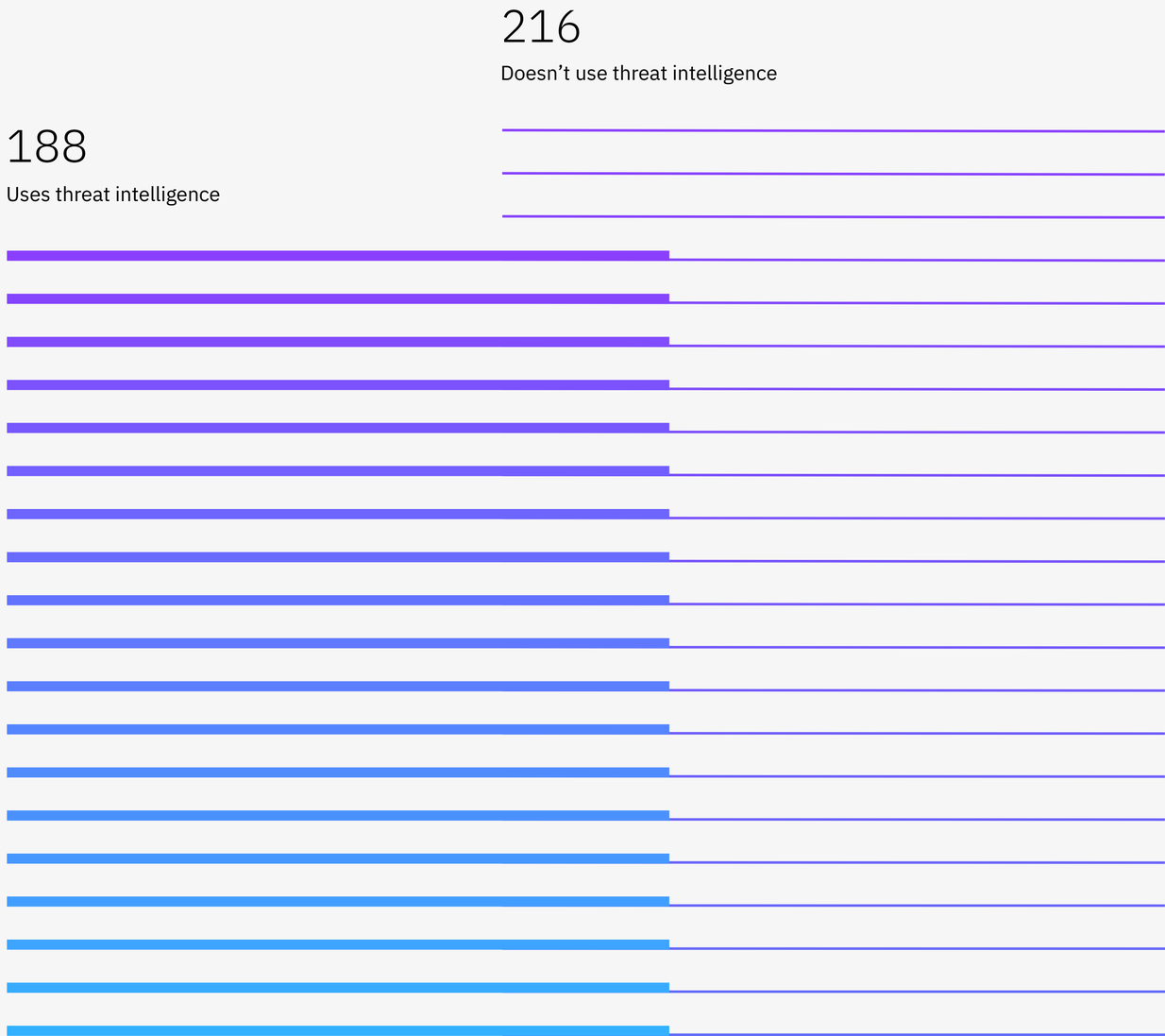
28 days

Organizations using threat intelligence identified breaches 28 days faster.

Figure 44. Threat intelligence reduced breach identification time.
This year's research showed that threat intelligence users uncovered breaches in 13.9% less time than those without a threat intelligence investment, a difference of 28 days. Compared to this year's global MTTI of 204 days, organizations employing threat intelligence services were able to identify breaches in 8.2% or 16 days less time. Respondents that did not use threat intelligence took 5.7% or 12 days longer than the global average to identify breaches.

Time to identify a data breach using threat intelligence

Figure 44. MTTI measured in days

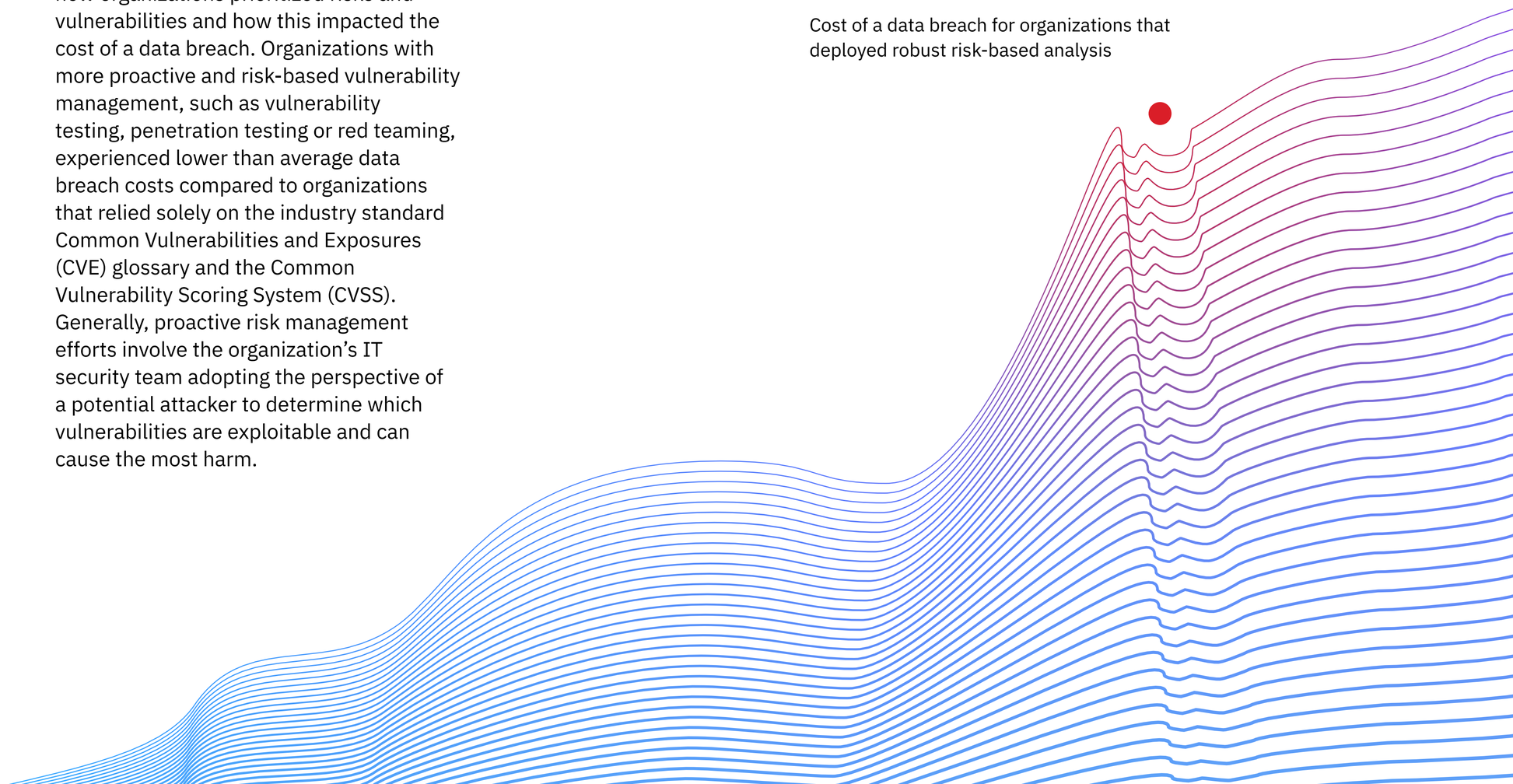


Vulnerability and risk management

New this year, the research examined how organizations prioritized risks and vulnerabilities and how this impacted the cost of a data breach. Organizations with more proactive and risk-based vulnerability management, such as vulnerability testing, penetration testing or red teaming, experienced lower than average data breach costs compared to organizations that relied solely on the industry standard Common Vulnerabilities and Exposures (CVE) glossary and the Common Vulnerability Scoring System (CVSS). Generally, proactive risk management efforts involve the organization's IT security team adopting the perspective of a potential attacker to determine which vulnerabilities are exploitable and can cause the most harm.

USD 3.98M

Cost of a data breach for organizations that deployed robust risk-based analysis



Figures 45 and 46. Organizations that prioritize activities beyond CVE score experienced less costly breaches. More than one-third of organizations or 36% relied solely on CVE scoring to prioritize vulnerabilities, while the majority of organizations or 64% used more involved risk-based analysis. The 2023 research showed a significant difference in the cost of data breaches between these two groups. Organizations that deployed more intensive, risk-based analysis experienced an average cost of a data breach of USD 3.98 million, a difference of 18.3%, compared to USD 4.78 million for organizations that relied on CVE scores only.

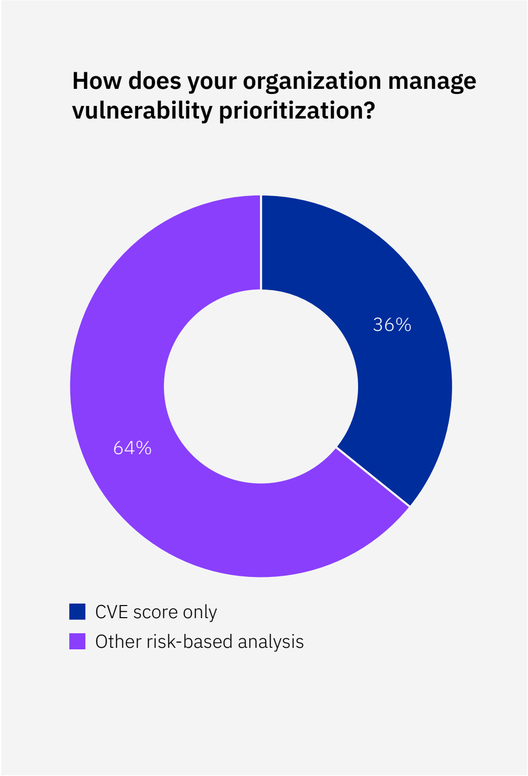


Figure 45. Percentage of all organizations

Figure 46. Measured in USD millions

Attack surface management

ASM is a set of processes that aids in the discovery, analysis, remediation and monitoring of an organization's potential attack surfaces or vulnerabilities. Organizations that deployed an ASM solution were able to identify and contain data breaches in 75% of the time of those without an ASM solution.

Figure 47. ASM helped accelerate total time to identify and contain a data breach by nearly 12 weeks.
Without an ASM solution, organizations took 260 days to identify a data breach and another 77 days to contain it, for a total of 337 days or about 11 months. Organizations with an ASM solution identified the breach in 193 days and contained it in 61 days. The 254-day total time to identify and contain a breach represented an acceleration of 83 days or about 12 weeks so the data breaches were identified and contained in 75% of the time taken by data breaches at organizations without ASM solutions.

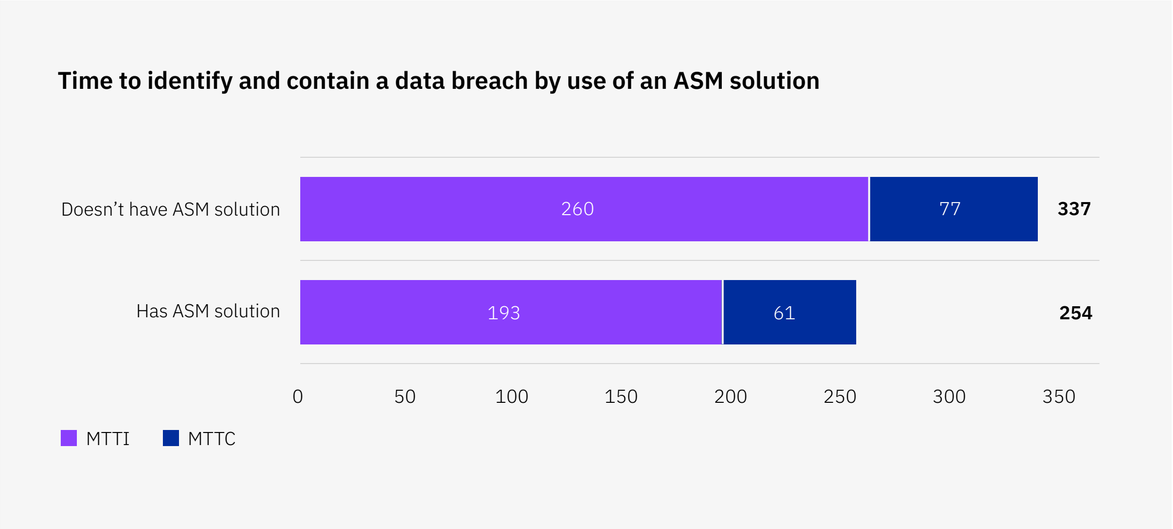


Figure 47. Measured in days

Managed security service providers

For the first time, our research explored the impact that partnering with an MSSP had on the time to identify and contain a breach. MSSPs offer organizations the ability to outsource security monitoring and management, often using high-availability security operations centers to provide around-the-clock services. MSSPs can help organizations enhance their security posture without increasing head count or investing in training for internal resources.

Figure 48. Organizations with MSSPs experienced a 21% shorter breach lifecycle.
In the 2023 report, organizations that had an MSSP were able to identify and contain breaches in 80% of the time of those without. Organizations that worked with an MSSP identified breaches 16 days faster or an 8.2% shorter identification time than the 2023 reported global average of 204 days. Those that didn't took 28 days longer or 12.8% longer. Containment times with no MSSP were five days longer or 6.6% longer than the 2023 reported global average of 73 days. Containment times with MSSP assistance were 10 days faster or 14.7% faster.

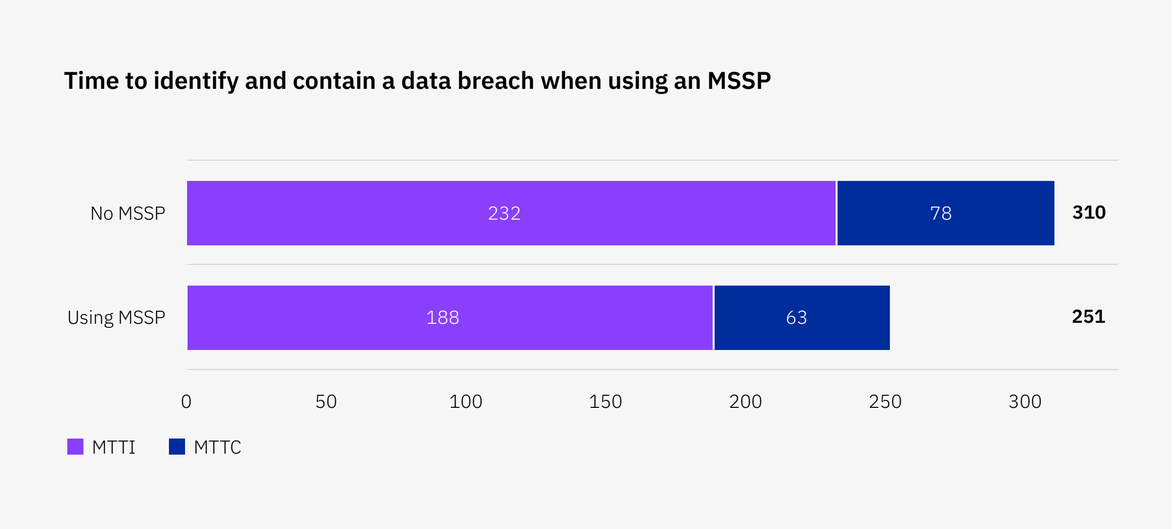


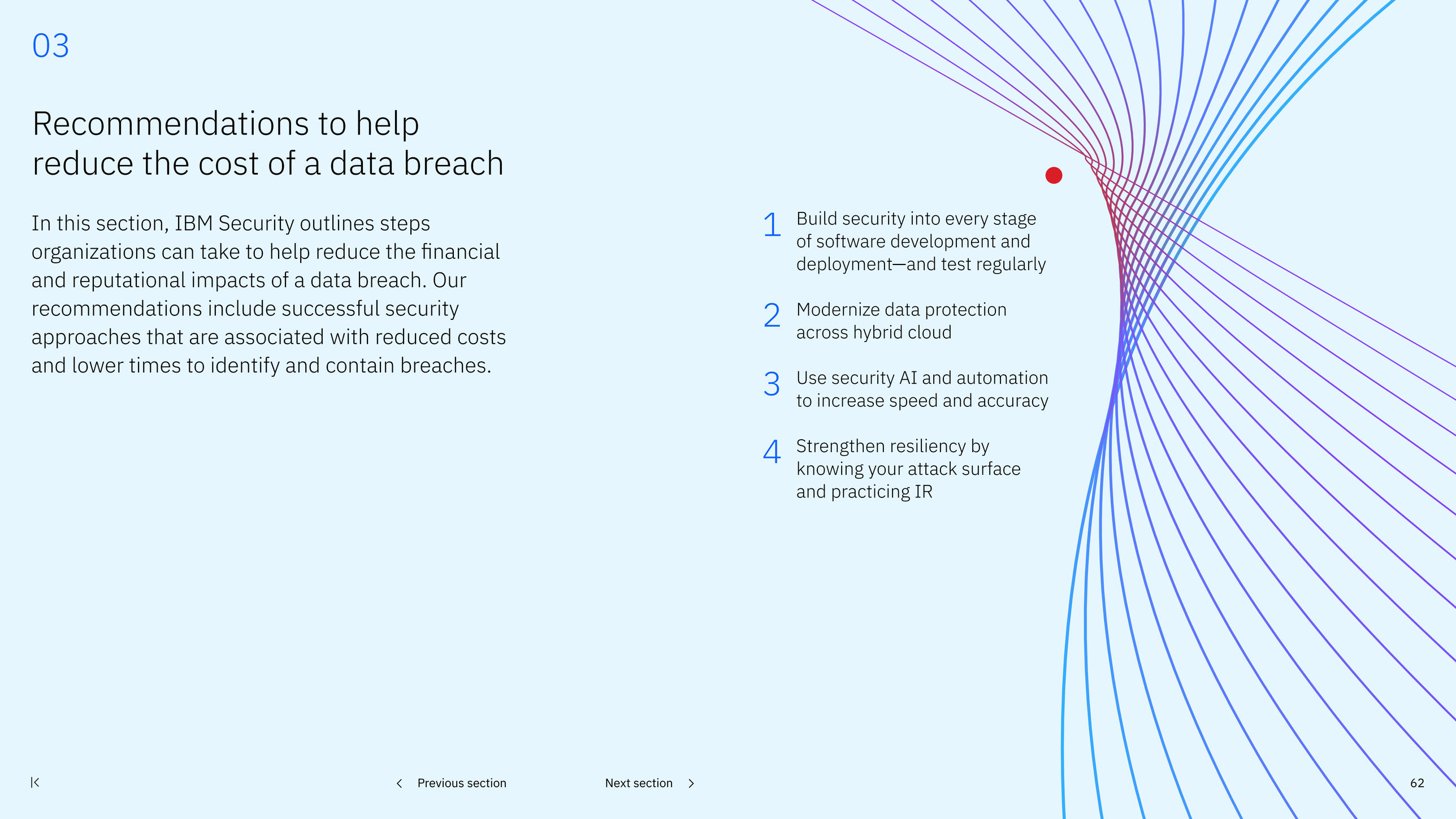
Figure 48. Measured in days

03

Recommendations to help reduce the cost of a data breach

In this section, IBM Security outlines steps organizations can take to help reduce the financial and reputational impacts of a data breach. Our recommendations include successful security approaches that are associated with reduced costs and lower times to identify and contain breaches.

1. Build security into every stage of software development and deployment—and test regularly
2. Modernize data protection across hybrid cloud
3. Use security AI and automation to increase speed and accuracy
4. Strengthen resiliency by knowing your attack surface and practicing IR



1

Build security into every stage of software development and deployment—and test regularly

Regulatory requirements continue to become more intricate, especially as technology becomes more intertwined with everyday activities and software becomes more feature rich and complex. A DevSecOps approach—the top cost mitigator in a special analysis of 27 factors in the 2023 report—will be essential to building security into any tools or platforms an organization depends on to engage its workforce or its customers.

Organizations of all types should look to ensure that security is at the forefront of the software they're developing as well as commercial off-the-shelf software that they're deploying. Application developers must continue to accelerate the adoption of the principles of secure by design and secure by default to ensure that security is a core requirement that's considered during the initial design phase of digital transformation projects and not simply addressed after the fact. The same principles are being applied to cloud environments to support cloud-native app development that makes a serious effort to protect user privacy and minimize attack surfaces.

Application testing or penetration testing from the perspective of an attacker can also give organizations the opportunity to identify and patch vulnerabilities before they turn into breaches. No technology or application will ever be fully secure, and adding more features introduces new risks. Ongoing application testing can help organizations identify new vulnerabilities.

2

Modernize data protection across hybrid cloud

Data is being created, shared and accessed at unprecedented scale across multicloud environments. Fast-paced adoption of new cloud applications and services is compounding the risk of "shadow data"—sensitive data not being tracked or managed—increasing security and compliance risks. The majority (82%) of data breaches in this report involved data stored in cloud environments, and 39% of breaches included data that spanned multiple types of environments. The cost and risk of these data breaches are compounded by an ever-evolving matrix of regulations and stiff penalties for noncompliance.

In the wake of these challenges, gaining visibility and control of data spread across hybrid cloud should be a top priority for organizations of all types and should include a focus on strong encryption, data security and data access policies. Companies should seek data security and compliance technologies that work on all platforms, allowing them to protect data as it moves across databases, applications and services deployed across hybrid cloud environments. Data activity–monitoring solutions can help ensure proper controls are in place while actively enforcing these policies—such as early detection of suspicious activity and blocking real-time threats to critical data stores.

Additionally, newer technologies such as data security posture management can help find unknown and sensitive data across the cloud, including structured and unstructured assets within cloud service providers, software as a service (SaaS) properties and data lakes. This can help identify and mitigate vulnerabilities in underlying data store configurations, entitlements and data flows.

As organizations continue to move further into hybrid multicloud operations, it's essential to deploy strong identity and access management (IAM) strategies that include technologies such as multifactor authentication (MFA), with particular focus on managing privileged user accounts that have an elevated access level.

3

Use security AI and automation to increase speed and accuracy
In the 2023 report, only 28% of organizations used security AI and automation extensively in their operations, which means many organizations have a significant opportunity to improve their speed, accuracy and efficiency. Extensive use of security AI and automation delivered nearly USD 1.8 million in data breach cost savings and accelerated the time to identify and contain a breach by more than 100 days compared to organizations with no use.

Security teams can benefit from having security AI and automation embedded throughout their tool sets. For example, using security AI and automation across threat detection and response tools can help analysts detect new threats more accurately and contextualize and triage security alerts more effectively. These technologies can also automate portions of the threat investigation process or recommend actions to speed response. Additionally, AI-driven data security and identity solutions can help drive a proactive security posture by identifying high-risk transactions, protecting them with minimal user friction and stitching together suspicious behaviors more effectively.

When applying AI within your security operations, look for technologies that offer trusted and mature use cases with demonstrated accuracy, effectiveness and transparency to eliminate potential bias, blind spots or drift. Organizations should plan an operational model for AI adoption that supports continuous learning as threats and technology capabilities evolve.

Organizations can also benefit from an approach that tightly integrates core security technologies for smoother workflows and the ability to share insights across common data pools. Chief information security officers (CISOs) and security operations (SecOps) leaders can also use threat intelligence reports to help with pattern recognition and threat visibility for emerging threats.

4

Strengthen resiliency by knowing your attack surface and practicing IR
Understand your exposure to the attacks most relevant to your industry and organization, and prioritize your security strategy accordingly. Tools such as ASM or techniques such as adversary simulation can help organizations gain an attacker-informed perspective into their unique risk profile and vulnerabilities, including which vulnerabilities are readily exploitable.

Additionally, having a team in place that's already versed in the right protocols and tools to respond to an incident has been shown to significantly reduce costs and the time to identify and contain the breach.

Not only was IR planning and testing a top 3 cost mitigator in the 2023 report, but the data also showed that organizations with high levels of these countermeasures in place incurred USD 1.49 million lower data breach costs compared to organizations with low levels or none, and they resolved incidents 54 days faster. Form a dedicated IR team, draft IR playbooks and regularly test IR plans in tabletop exercises or simulated environments such as a cyber range. Having an IR vendor on retainer can also help speed the time to respond to a breach.

Lastly, organizations should look to implement network segmentation practices to limit the spread of attacks and the extent of damage they can cause, strengthening overall resiliency and reducing recovery efforts.

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

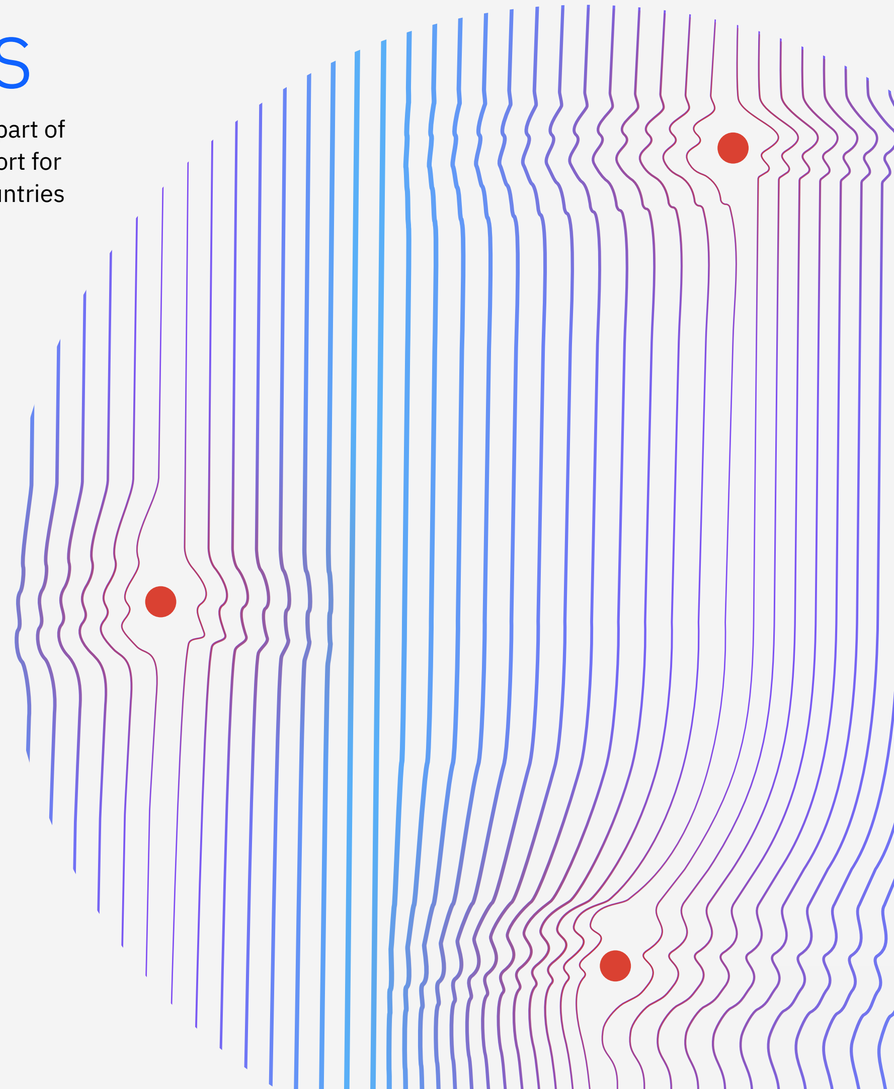
04

Organization demographics

This year’s study examined 553 organizations of various sizes across 16 countries and geographic regions and 17 industries. This section explores the breakdown of organizations in the study by geography and industry and defines the industry classifications.

18 years

The United States has been a part of the Cost of a Data Breach Report for 18 years, the longest of all countries or regions involved.



Geographic demographics

The 2023 study was conducted across 16 different countries and regions.

Global study at a glance

Countries	2023 sample	Percentage	Currency	2023 USD conversion rate[7]	Years studied
ASEAN	23	4%	SGD	1.3294	7
Australia	24	4%	AUD	1.4916	14
Brazil	43	8%	BRL	5.0702	11
Canada	26	5%	CAD	1.3525	9
France	34	6%	EUR	0.9198	14
Germany	45	8%	EUR	0.9198	15
India	51	9%	INR	82.19	12
Italy	24	4%	EUR	0.9198	12
Japan	42	8%	JPY	132.75	12
Latin America[4]	23	4%	MXN	18.025	4
Middle East[5]	36	7%	SAR	3.7037	10
Scandinavia[6]	22	4%	NOK	10.4445	5
South Africa	21	4%	ZAR	17.73	8
South Korea	23	4%	ZRW	1303.8	6
United Kingdom	49	9%	GBP	0.8085	16
United States	67	12%	USD	1.00	18
Total	**553**	**100%**			

Figure 49. Table of all countries studied

Industry demographics

The selection of 17 industries has been included in the study for multiple years.

Five industries together accounted for 55% of organizations sampled in this year's study.

14% Financial

12% Services

11% Technology

10% Industrial

8% Energy

Distribution of the sample by industry

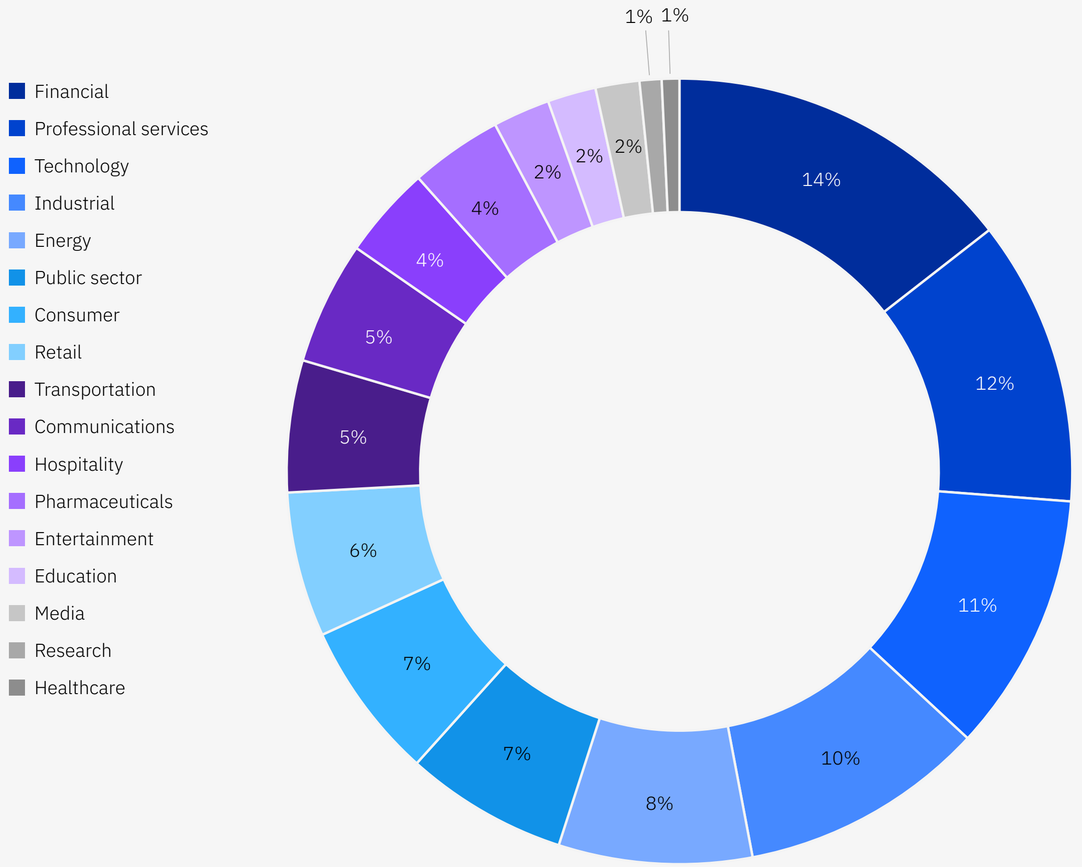


Figure 50. Percentage of industries

Industry definitions

Healthcare
Hospitals and clinics

Financial
Banking, insurance and investment companies

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

Pharmaceuticals
Pharmaceuticals including biomedical life sciences

Industrial
Chemical processing and engineering and manufacturing companies

Technology
Software and hardware companies

Education
Public and private universities and colleges and training and development companies

Services
Professional services such as legal, accounting and consulting firms

Entertainment
Movie production, sports, gaming and casinos

Transportation
Airlines, railroads and trucking and delivery companies

Communications
Newspapers, book publishers and public relations and advertising agencies

Consumer
Manufacturers and distributors of consumer products

Media
Television, satellite, social media and internet

Hospitality
Hotels, restaurant chains and cruise lines

Retail
Brick and mortar and e-commerce

Research
Market research, think tanks and research and development (R&D)

Public
Federal, state and local government agencies and nongovernmental organizations (NGOs)

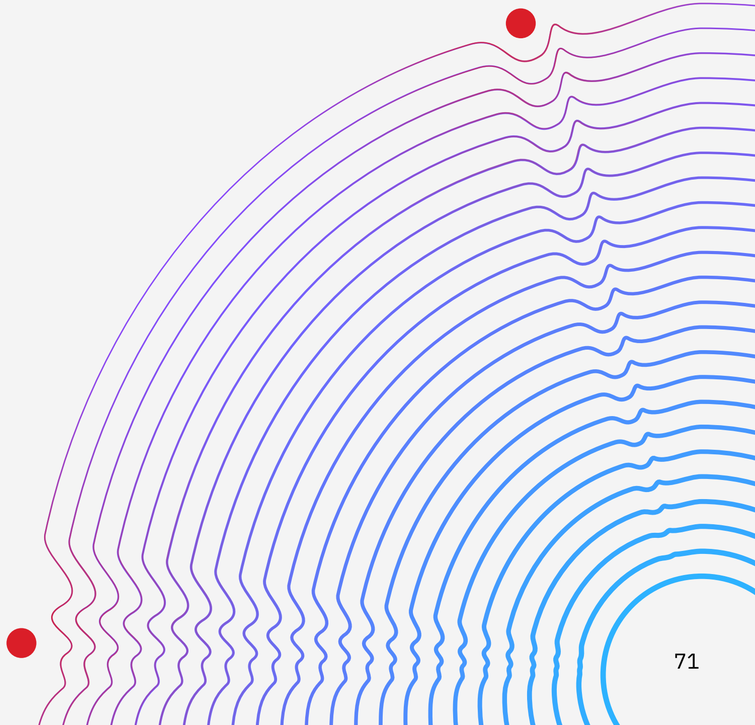
Research methodology

To preserve confidentiality, the benchmark instrument didn’t capture any company-specific information. Data collection methods excluded actual accounting information and instead relied on 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 separate estimate for indirect and opportunity costs.

In the interest of maintaining a manageable data set for benchmarking, we included only those cost activity centers with a crucial impact on data breach costs. Based on discussions with experts, we chose a fixed set of cost activities. After collecting benchmark information, we carefully reexamined each instrument for consistency and completeness.

We limited the scope of data breach cost factors to known categories that apply to a broad set of business operations involving personal information. We chose to focus on business processes instead of data protection or privacy compliance activities because we believed the process study would yield better-quality results.



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 2023 report ranged in size between 2,160 and 101,200 compromised records. We used a separate analysis to examine the costs of mega breaches; that methodology is explained further in the "Data breach FAQs" section of this 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 detect the breach, including:

- 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:

- Emails, letters, outbound calls or general notices 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 conduct redress activities to victims and regulators, including:

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing of 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:

- Business disruption and revenue losses due to system downtime
- Cost of losing customers and acquiring new customers
- Reputational damage and diminished goodwill

Data breach FAQs

What's a data breach?
A breach is defined as an event in which records containing personally identifiable information (PII); financial or medical account details; or other secret, confidential or proprietary data 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's a compromised record?
A record is information that reveals confidential or proprietary corporate, governmental or financial data, or identifies an 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 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 3,475 separate interviews with individuals at 553 organizations that suffered a data breach between March 2022 and March 2023. 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 communications along with 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.

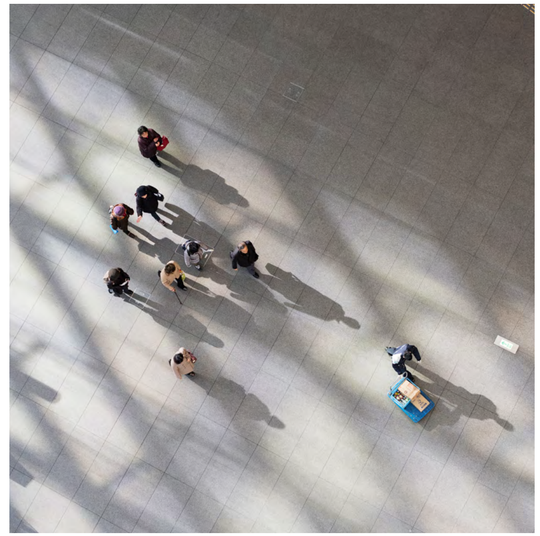
For consistency with prior years, we used the same currency translation method rather than adjusting accounting costs.

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 553 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?
It's not consistent with this research to use the overall cost per record as a basis for calculating the cost of single or multiple breaches totaling millions of records. The per-record cost is derived from our study of hundreds of data breach events in which each event featured 101,200 or fewer compromised records. To measure the impact of mega breaches that involve one million or more records, the study instead uses a simulation framework based on a sample of 20 events of that size.

Why did you use simulation methods to estimate the cost of a mega data breach?
The sample size of 20 companies that experienced a mega breach was not large enough to support a statistically significant analysis using the study's activity-based cost methods. To remedy this issue, we deployed Monte Carlo simulations to estimate a range of possible, meaning random, outcomes through repeated trials. In total, we performed more than 250,000 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, head count, geographic footprint and size of data breach. Since starting this research in 2005, we have studied the data breach experiences of 5,580 organizations.



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.

Nonstatistical results
Our study drew upon a representative, nonstatistical sample of global entities. Statistical inferences, margins of error and confidence intervals can't be applied to this data, given that our sampling methods weren't scientific.

Nonresponse
Nonresponse 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
Although 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. It's important to note that this issue may affect only the global analysis because all country-level results are shown in local currencies. The current real exchange rates used in this research report were published by the Federal Reserve on 31 March 2023.

06

About Ponemon Institute and IBM Security

Ponemon Institute
Founded in 2002, 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 PII 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 helps secure the world's largest enterprises and governments with an integrated portfolio of security products and services infused with dynamic security AI and automation capabilities. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to predict threats, protect data as it moves, and respond with speed and precision without holding back business innovation. IBM is trusted by thousands of organizations as their partner to assess, strategize, implement and manage security transformations.

IBM operates one of the world's broadest security research, development and delivery organizations; monitors more than 150 billion security events each day in more than 130 countries; and has been granted more than 10,000 security patents worldwide.

If you have questions or comments about this research report, including requests 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

Learn more about advancing your security posture

Visit ibm.com/security.

Join the conversation in the IBM Security Community.

Take the next steps

AI cybersecurity solutions
Speed up security response times and boost productivity.
Learn more

Threat detection and response solutions
Empower security teams to outsmart threats with speed, accuracy and efficiency.
Learn more

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

Ransomware solutions
Manage cybersecurity risks and vulnerabilities to minimize ransomware's impact.
Learn more

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

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

Data security and protection solutions
Protect data and simplify compliance across hybrid clouds.
Learn more

Attack surface management
Manage the expansion of your digital footprint and improve your organization's cyber resilience quickly.
Learn more

Unified endpoint management solutions
Scale your mobile workforce by securing and managing any device.
Learn more

Governance, risk and compliance services
Increase cybersecurity maturity with an integrated governance, risk and compliance approach.
Learn more

Schedule a one-on-one consultation
Meet with an IBM Security X-Force expert to discuss your needs.
Learn more

Request an IBM security and framing discovery workshop
Get assistance in modernizing your security program.
Learn more

1. 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.

2. ASEAN is a cluster sample of companies located in Singapore, Indonesia, the Philippines, Malaysia, Thailand and Vietnam.

3. Destructive attacks are defined as attacks that render systems inoperable and challenge reconstitution. They may or may not also involve a ransom.

4. Latin America is a cluster sample of companies located in Mexico, Argentina, Chile and Colombia.

5. Middle East is a cluster sample of companies located in Saudi Arabia and the United Arab Emirates.

6. Scandinavia is a cluster sample of companies located in Denmark, Sweden, Norway and Finland.

7. Foreign Exchange Rates - H.10, 31 March 2023.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2023

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.

All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Generally expected results cannot be provided as each client's results will depend entirely on the client’s systems and services ordered. 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.