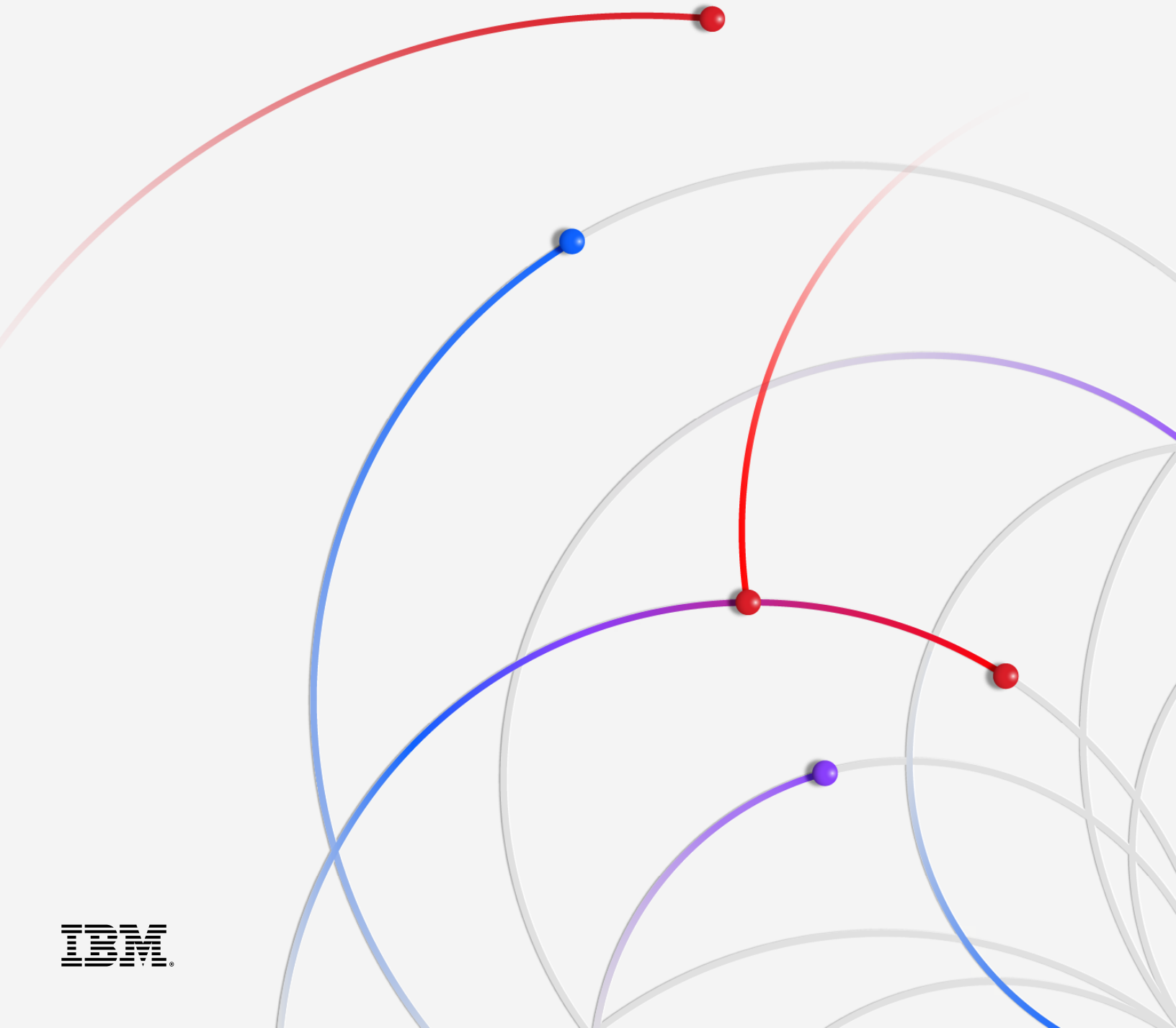
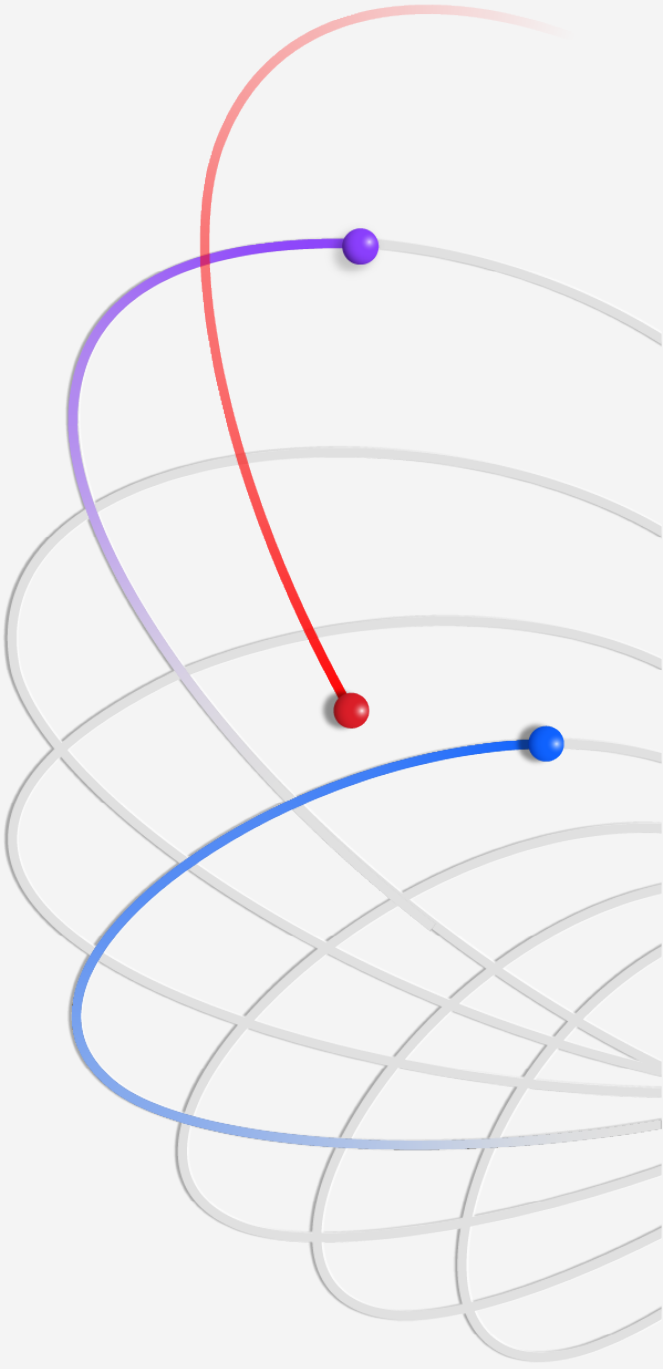
Cost of a Data Breach Report 2024



IBM

Table of contents

Executive summary



IBM's annual Cost of a Data Breach Report provides IT, risk management and security leaders with timely, quantifiable evidence to guide them in their strategic decision-making. It also helps them better manage their risk profiles and security investments. This year's report—the 19th of the series—reflects changes caused by technological shifts, such as the rise of shadow data, which is data residing in unmanaged data sources, and the extent and costs of business disruption brought about by data breaches.

The report's research—conducted independently by Ponemon Institute and sponsored, analyzed and published by IBM—studied 604 organizations impacted by data breaches between March 2023 and February 2024. Researchers looked at organizations across 17 industries, in 16 countries and regions, and breaches that ranged from 2,100 to 113,000 compromised records. To gain on-the-ground insights, Ponemon Institute researchers interviewed 3,556 security and C-suite business leaders with firsthand knowledge of the data breach incidents at their organizations.

The result is a benchmark report that business and security leaders can use to strengthen their security defenses and drive innovation, particularly around the adoption of AI in security and security for their generative AI (gen AI) initiatives.

We lead this year's report with 2 major developments. First, the global average cost of a data breach increased 10% over the previous year, reaching USD 4.88 million, the biggest jump since the pandemic. Business disruption and post-breach customer support and remediation drove this cost spike. When asked how they're dealing with these costs, more than half of organizations said they are passing them on to customers. Having customers absorb these costs can be problematic in a competitive market already facing pricing pressures from inflation.

Second, on the defender side of the equation, researchers also found applying security AI and automation is paying off, lowering breach costs in some instances by an average of USD 2.2 million. AI and automation solutions are reducing the lifespan needed to identify and contain a breach and its resulting damage. Put another way, defenders without AI and automation to assist them can expect to take longer to detect and contain a breach, and see costs rise compared to those who use these solutions.

As we've seen across the industry, cybersecurity teams are consistently understaffed. This year's study found more than half of breached organizations faced severe security staffing shortages, a skills gap that increased by double digits from the previous year. This lack of trained security staff is growing as the threat landscape widens. The continuing race to adopt gen AI across nearly every function in the organization is expected to bring with it unprecedented risks and put even more pressure on these cybersecurity teams.

This report provides insights and recommendations from the research to help reduce the potential financial and reputational damages from a data breach.

What's new in the 2024 report

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

- Whether organizations experienced long-term operational disruption, for example, the inability to process sales orders, a complete shutdown of production facilities, ineffective customer services
- Whether the breach included data stored in unmanaged data sources, otherwise known as shadow data
- To what extent organizations are using AI and automation in each of 4 areas of security operations: prevention, detection, investigation and response
- The nature of extortion attacks, for example, extortion and ransomware attacks or extortion and data exfiltration only
- The time it takes to restore data, systems or services to their pre-breach state
- How long it took organizations to report the breach if they were mandated to do so
- Whether organizations that involved law enforcement following a ransomware attack paid the ransom

Key findings

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

USD 4.88M

Average total cost of a breach
The average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a 10% spike and the highest increase since the pandemic. A rise in the cost of lost business, including operational downtime and lost customers, and the cost of post-breach responses, such as staffing customer service help desks and paying higher regulatory fines, drove this increase. Taken together, these costs totaled USD 2.8 million, the highest combined amount for lost business and post-breach activities over the past 6 years.

USD 2.2M

Cost savings from extensive use of AI in prevention
2 out of 3 organizations studied stated they're deploying security AI and automation across their security operations center, a 10% jump from the prior year. When deployed extensively across prevention workflows—attack surface management (ASM), red-teaming and posture management—organizations averaged USD 2.2 million less in breach costs compared to those with no AI use in prevention workflows. This finding was the largest cost savings revealed in the 2024 report.

26.2%

Growth of the cyber skills shortage
More than half of breached organizations are facing high levels of security staffing shortages. This issue represents a 26.2% increase from the prior year, a situation that corresponded to an average USD 1.76 million more in breach costs. Even as 1 in 5 organizations say they used some form of gen AI security tools—which are expected to help close the gap by boosting productivity and efficiency—this skills gap remains a challenge.

1 in 3

Share of breaches involving shadow data
35% of breaches involved shadow data, showing the proliferation of data is making it harder to track and safeguard. Shadow data theft correlated to a 16% greater cost of a breach. Researchers found storing data across environments proved to be a common storage strategy, accounting for 40% of breaches. These breaches also took longer to identify and contain. In contrast, data stored in just 1 type of environment was breached less often, whether that environment was public cloud (25%), on premises (20%) or private cloud (15%).

USD 4.99M

Average cost of a malicious insider attack
Compared to other vectors, malicious insider attacks resulted in the highest costs, averaging USD 4.99 million. Among other expensive attack vectors were business email compromise, phishing, social engineering and stolen or compromised credentials. Gen AI may be playing a role in creating some of these phishing attacks. For example, gen AI makes it easier than ever for even non-English speakers to produce grammatically correct and plausible phishing messages.

46%

Share of breaches involving customer personal data
Nearly half of all breaches involved customer personal identifiable information (PII), which can include tax identification (ID) numbers, emails, phone numbers and home addresses. Intellectual property (IP) records came in a close second (43% of breaches). The cost of IP records jumped considerably from last year, to USD 173 per record in this year's study from USD 156 per record in last year's report.

USD 1M

Cost savings when law enforcement is involved in ransomware attacks
Ransomware victims that involved law enforcement ended up lowering the cost of the breach by an average of nearly USD 1 million, and that excludes the cost of any ransom paid. Involving law enforcement also helped shorten the time required to identify and contain breaches from 297 days to 281 days.

292

Days to identify and contain breaches involving stolen credentials
Breaches involving stolen or compromised credentials took the longest to identify and contain (292 days) of any attack vector. Similar attacks that involved taking advantage of employees and employee access also took a long time to resolve. For example, phishing attacks lasted an average of 261 days, while social engineering attacks took an average of 257 days.

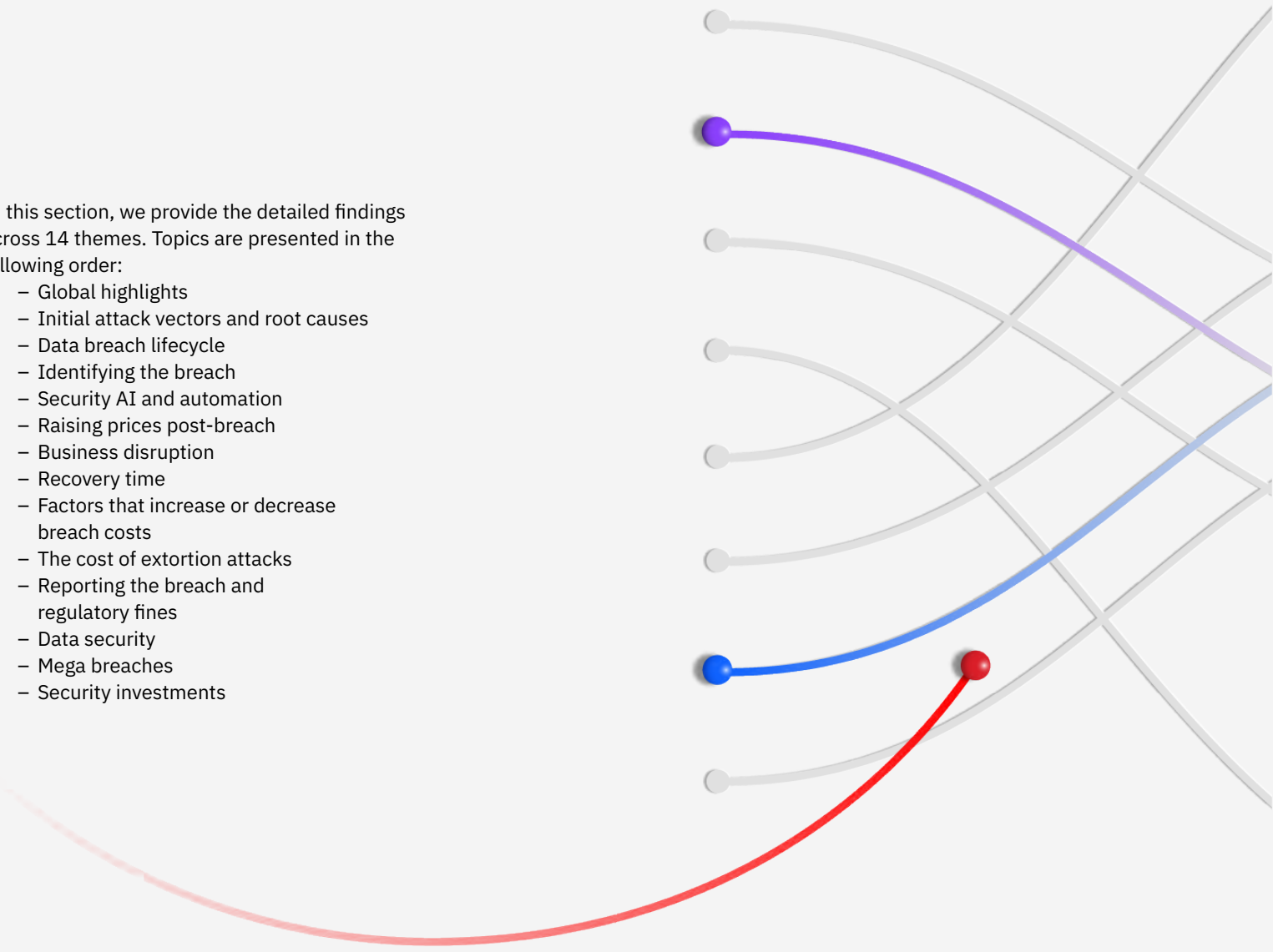
USD 830,000

Largest average cost increase among all industries
The industrial sector experienced the costliest increase of any industry, rising by an average USD 830,000 per breach over last year. This cost spike could reflect the need for industrial organizations to prepare for a more rapid response, as organizations in this sector are highly sensitive to operational downtime. Still, the time to identify and contain a data breach at industrial organizations was above the median industry, at 199 days to identify and 73 days to contain.

Complete findings

In this section, we provide the detailed findings across 14 themes. Topics are presented in the following order:

- Global highlights
- Initial attack vectors and root causes
- Data breach lifecycle
- Identifying the breach
- Security AI and automation
- Raising prices post-breach
- Business disruption
- Recovery time
- Factors that increase or decrease breach costs
- The cost of extortion attacks
- Reporting the breach and regulatory fines
- Data security
- Mega breaches
- Security investments



USD 4.88M

The global average cost of a data breach spikes

Global highlights

Globally, security teams are doing a much better job of detecting and containing breaches, despite a stubborn skills shortage. More than half of breached organizations are facing security staffing shortages, and security leaders are, in turn, marshalling AI and automation solutions to close the skills gap. Despite their efforts, breach costs are rising, mostly from expenses related to business disruption and post-breach responses. In the following section, we look at these issues and others, across industries, countries and regions, to provide security leaders with a view of the risks out there so you can learn from them.

The global average cost of a data breach spiked

The global average cost of a data breach increased 10% in one year, reaching USD 4.88 million, the biggest jump since the pandemic. Business disruption and post-breach response activities drove most of this yearly cost increase. See Figure 1.

Global average total cost of a data breach

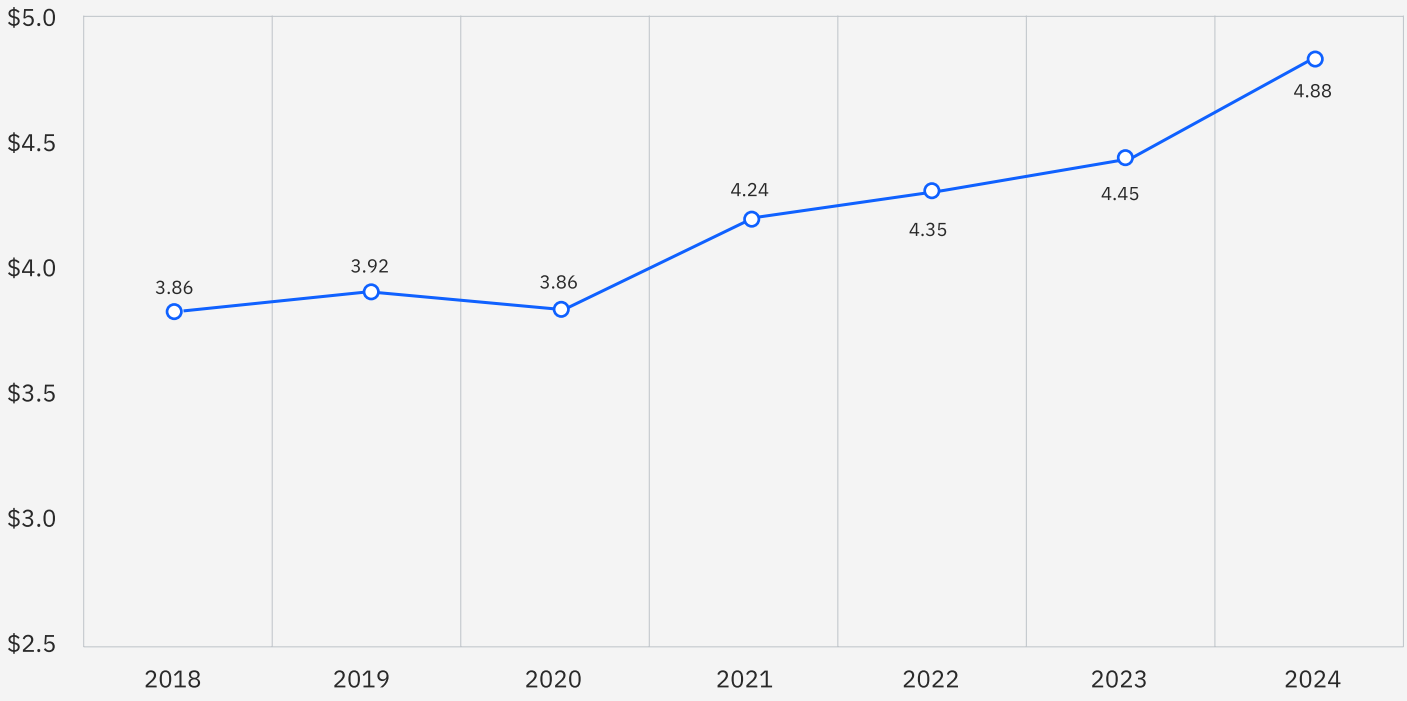


Figure 1. Measured in USD millions

The United States led the world in average breach cost
For the 14th year, the United States had the highest average data breach cost—USD 9.36 million—among the 16 countries and regions studied. Rounding out the top 5 were the Middle East, Germany, Italy and Benelux. Benelux is the economic union of Belgium, the Netherlands and Luxembourg, and it's a new addition this year. Notably, Canada and Japan saw average costs drop, while Italy and the Middle East saw significant increases. See Figures 2A and 2B.

Cost of a data breach by country or region

#	Country	2024	2023
1	United States	$9.36	$9.48
2	Middle East	$8.75	$8.07
3	Benelux	$5.90	—
4	Germany	$5.31	$4.67
5	Italy	$4.73	$3.86
6	Canada	$4.66	$5.13
7	United Kingdom	$4.53	$4.21
8	Japan	$4.19	$4.52
9	France	$4.17	$4.08
10	Latin America	$4.16	$3.69
11	South Korea	$3.62	$3.48
12	ASEAN	$3.23	$3.05
13	Australia	$2.78	$2.70
14	South Africa	$2.78	$2.79
15	India	$2.35	$2.18
16	Brazil	$1.36	$1.22

Figure 2A. Measured in USD millions

Top 5 countries and regions 2024 vs 2023

#	Cost change	2024	2023
1	↓	**United States** $9.36	**United States** $9.48
2	↑	**Middle East** $8.75	**Middle East** $8.07
3	↑	**Benelux** $5.90	**Canada** $5.13
4	↑	**Germany** $5.31	**Germany** $4.67
5	↑	**Italy** $4.73	**Japan** $4.52

Figure 2B. Measured in USD millions

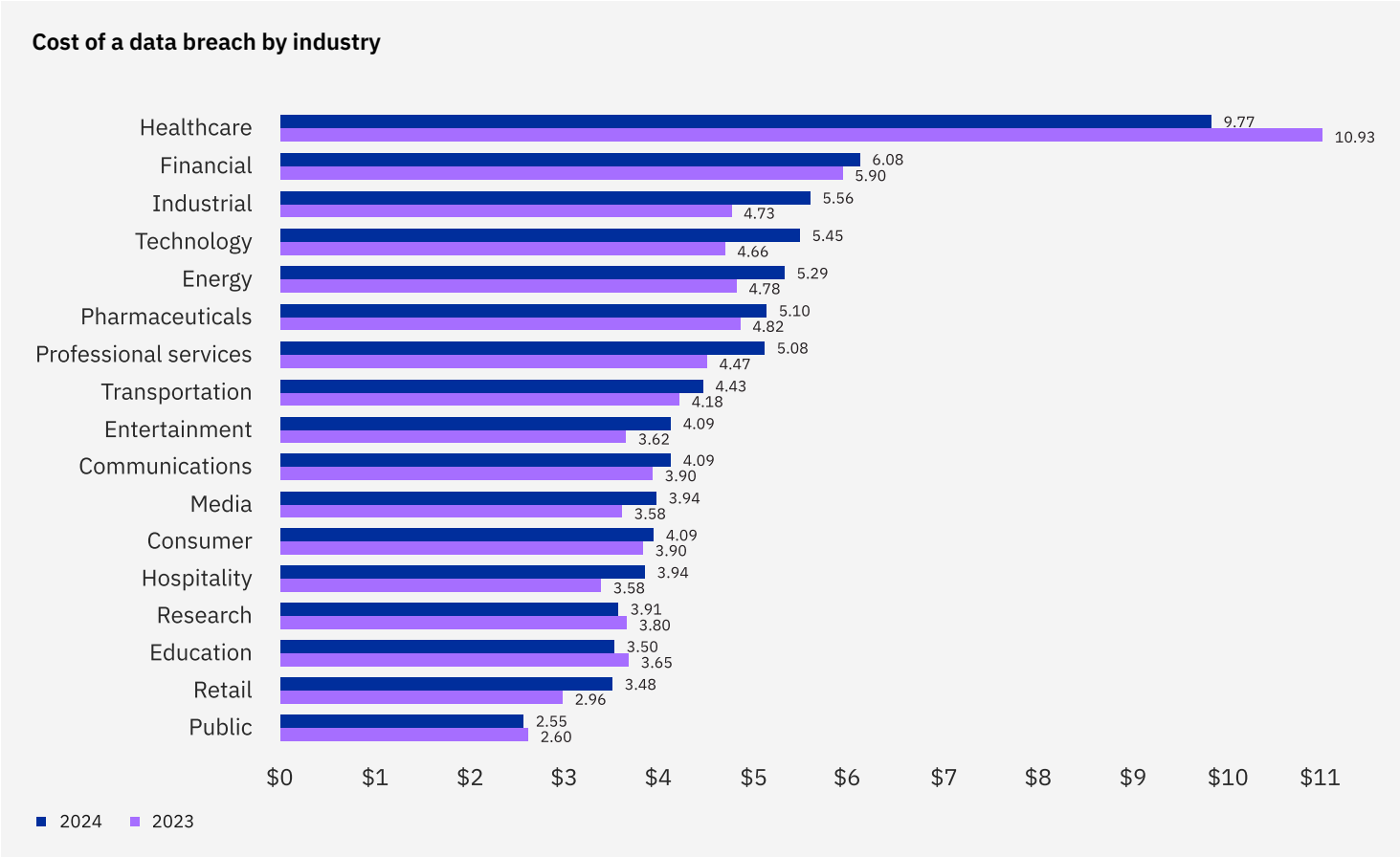


Figure 3. Measured in USD millions

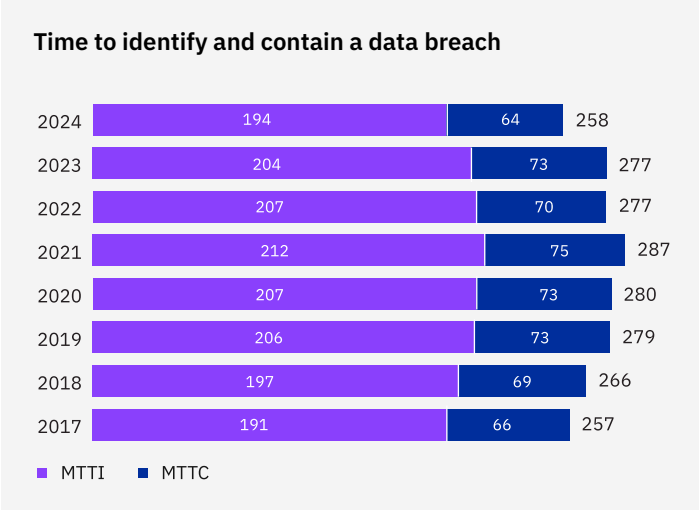


Figure 4. Measured in days

Healthcare topped industry costs, again

The average breach cost for healthcare fell 10.6%, to USD 9.77 million. But that factor wasn't enough to remove it from the top costliest industry for breaches—a spot it's held since 2011. Healthcare remains a target for attackers since the industry often suffers from existing technologies and is highly vulnerable to disruption, which can put patient safety at stake. See Figure 3.

Average time to identify and contain a breach fell

The mean time it took defenders to identity and contain a breach dropped to 258 days, reaching a 7-year low, compared to 277 days the previous year. Note: this global average of mean time to identify (MTTI) and mean time to contain (MTTC) excludes Benelux because, as a new region in the study, it was having outsized influence and skewed results much more than the average. See Figure 4.

Lost business costs and post-breach response costs soared
Costs from lost business and post-breach response rose nearly 11% over the previous year, which contributed to the significant rise in overall breach costs. Lost business costs include revenue loss due to system downtime, and the cost of lost customers and reputation damage. Post-breach costs can include the expense of setting up call centers and credit monitoring services for impacted customers, and paying regulatory fines. See Figure 5.

Average cost of a data breach in 4 components

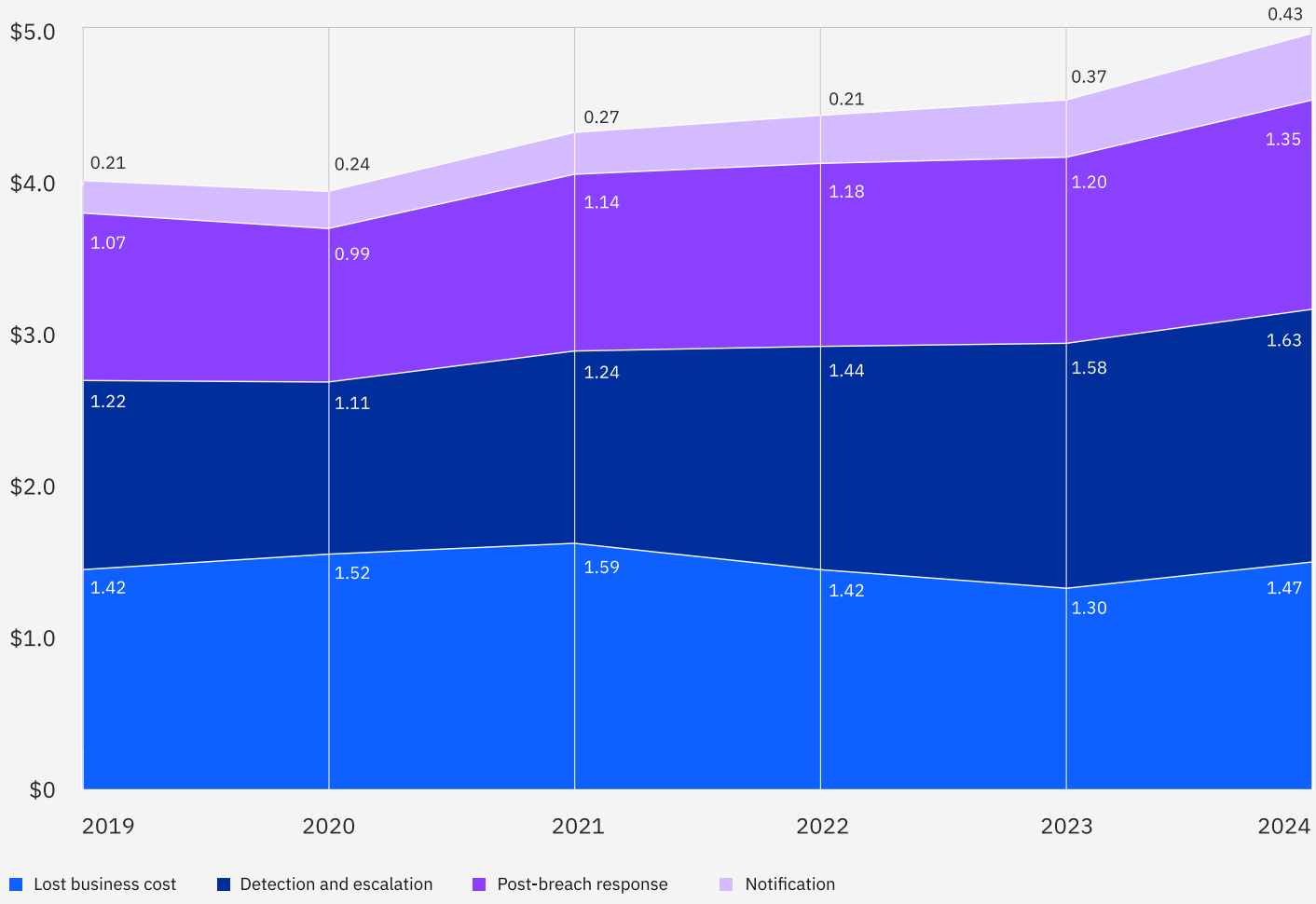


Figure 5. Measured in USD millions

Most breaches involved customer PII
The most common type of data stolen or compromised was customer PII, at 46%. PII can include tax ID numbers, emails and home addresses, and can be used in identity theft and credit card fraud. The global average for all stolen record types rose to a high of USD 169, with employee PII the costliest. See Figures 6A and 6B.

Type of data compromised by percentage

Figure 6A. More than 1 response permitted

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

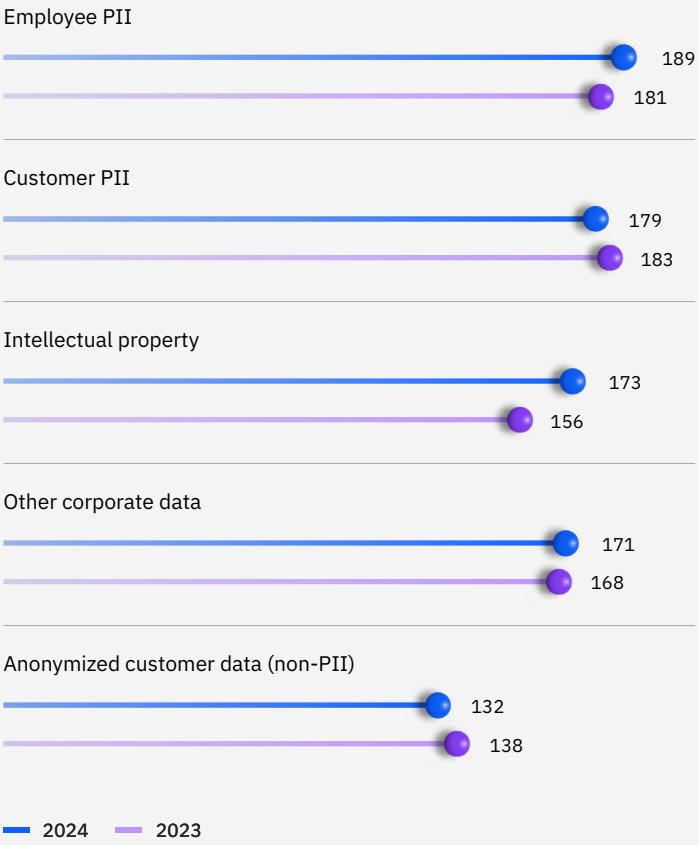


Figure 6B. Measured in USD millions

USD 4.81M

The average cost of a breach when attackers used compromised credentials, which happened in 16% of the breach cases studied.

Initial attack vectors and root causes

For the 2nd year in a row, phishing and stolen or compromised credentials were the 2 most prevalent attack vectors. Both also ranked among the top 4 costliest incident types. In addition to identifying the most common root causes for breaches, the study compared the average cost for each category, as well as the average time to identify and contain those breaches.

Compromised credentials topped initial attack vectors
Using compromised credentials benefited attackers in 16% of breaches. Compromised credential attacks can also be costly for organizations, accounting for an average USD 4.81 million per breach. Phishing came in a close second, at 15% of attack vectors, but in the end cost more, at USD 4.88 million. Malicious insider attacks cost the most, at USD 4.99 million, but were only 7% of all breach pathways. See Figure 7.

Cost and frequency of a data breach by initial attack vector

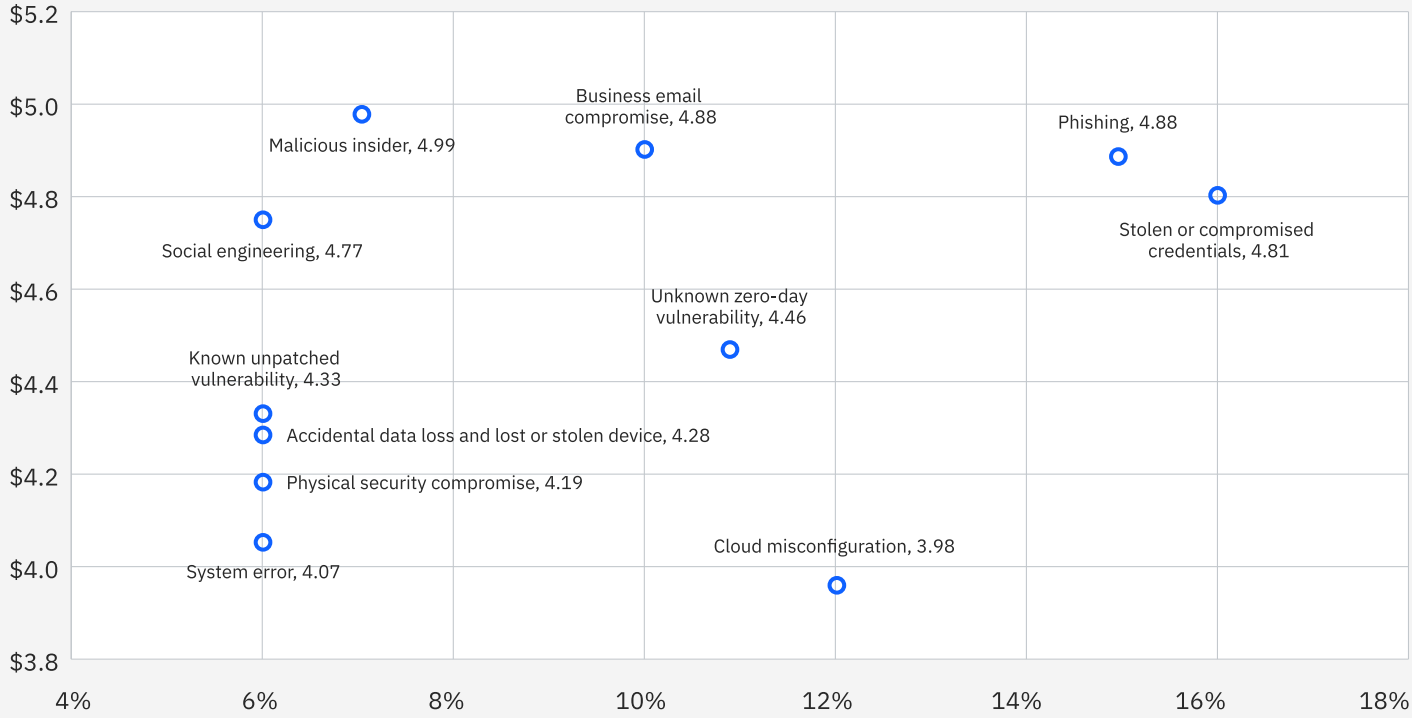


Figure 7. Measured in USD millions; percentage of all breaches

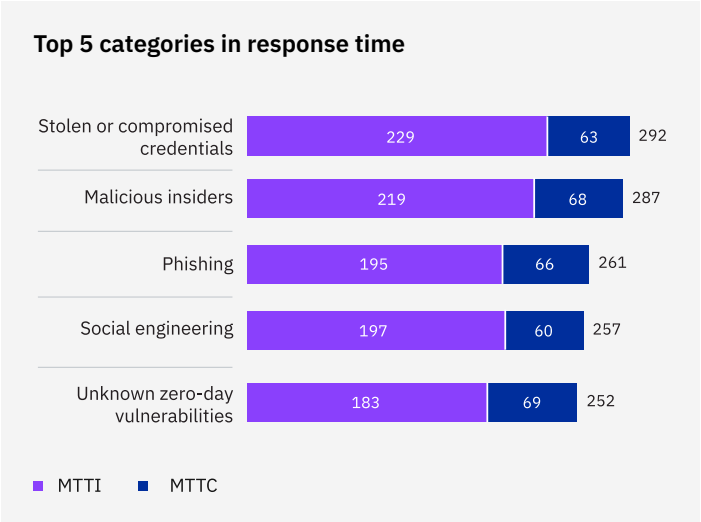


Figure 8. Measured in days

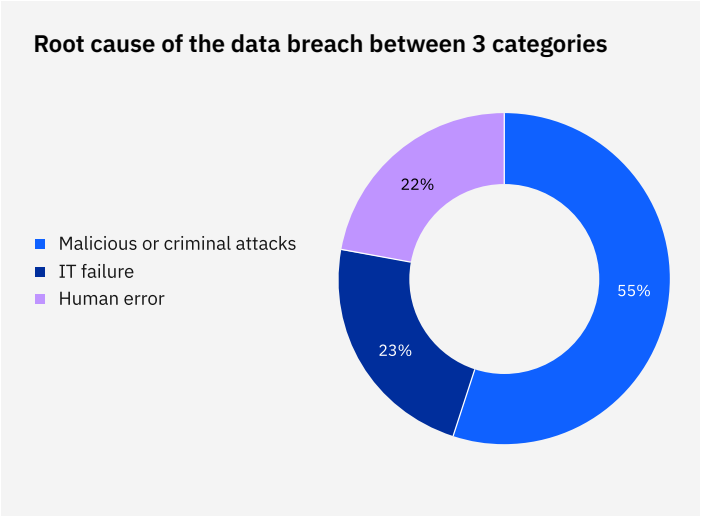


Figure 9.

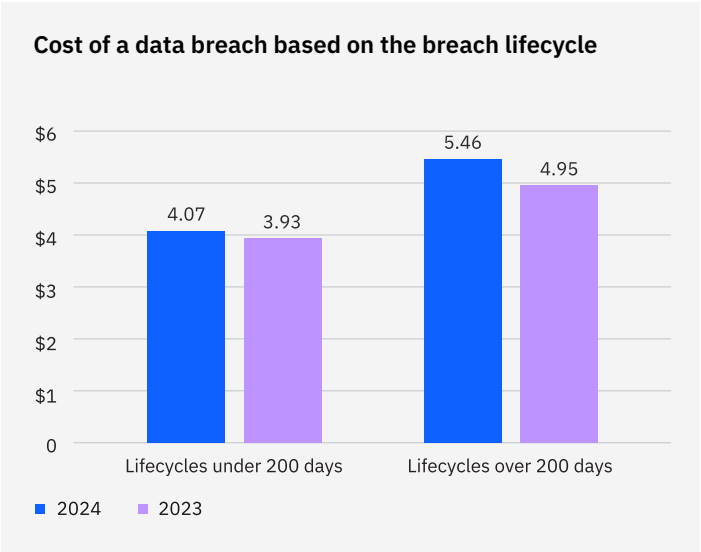


Figure 10. Measured in USD millions

Credential-based attacks took longer to identify and contain
Whether credentials were stolen or used by malicious insiders, attack identification and containment time increased, yielding an average combined time of 292 and 287 days respectively. Defenders needed to distinguish between legitimate and malicious user activity on the network, making threats harder to identify. On the other hand, attacks using zero-day vulnerabilities were the most time-consuming to contain. See Figure 8.

IT failures or human error caused nearly half of all breaches
Malicious attacks—those committed by outside attackers or criminal insiders—made up 55% of all breaches. As concerning as these breaches are, it's important to remember the remaining 23% are due to IT failure and 22% are due to human error. See Figure 9.

Data breach lifecycle

In a data breach, time means money, and breaches with longer lifecycles were more costly, according to our 2024 and 2023 research. A complete breach lifecycle is the combination of the average number of days to identify and contain a breach. In both reports, we compared the average costs of data breaches where the complete breach lifecycle was under 200 days to the average cost of breaches where complete lifecycles exceeded 200 days.

Longer breach lifecycles led to higher costs
In this year's report, researchers found data breaches with a lifecycle exceeding 200 days had the highest average cost, at USD 5.46 million, compared to breaches with lifecycles under 200 days. These findings are consistent with those from the previous year. Notably, while costs for longer data breach lifecycles increased 10.3% this year over last year, costs for shorter lifecycles also increased, but by a smaller amount, 3.6%. See Figure 10.

Identifying the breach

To contain a data breach, it needs to be identified first. Who identifies it, and how quickly, make a difference in the resulting data breach costs. This year, we found security teams working with their own tools improved their performance in this area. In other cases, breaches were identified by benign third parties, such as security researchers, law enforcement and consultants, or the attackers themselves.

Security teams identified most breaches
Security teams and their tools detected breaches far more often, at 42% of the time, than did benign third parties, at 34%, and attackers themselves, at 24%. This figure was an improvement over the 2023 report when security teams discovered breaches only one-third of the time. The change shows security teams were able to speed up detection. See Figure 11.

How was the breach identified?

Figure 11. Only 1 response permitted

USD 5.53M

The average cost of a breach when the breach was disclosed by an attacker.

Breaches disclosed by attackers cost more

By the time an attacker discloses a breach, they'll likely have already achieved their objective and done considerable damage, raising the overall costs of the breach. When a breach was disclosed by an attacker, the average cost was USD 5.53 million. On the other hand, when a security team identified a breach, the average cost was USD 4.55 million. See Figure 12.

Faster breach identification and containment

The report found regardless of how a breach was discovered, organizations identified and contained them more quickly on average in 2024 than the previous year. The use of AI and automation likely contributed to this acceleration, as the next section of this report shows. See Figure 13.

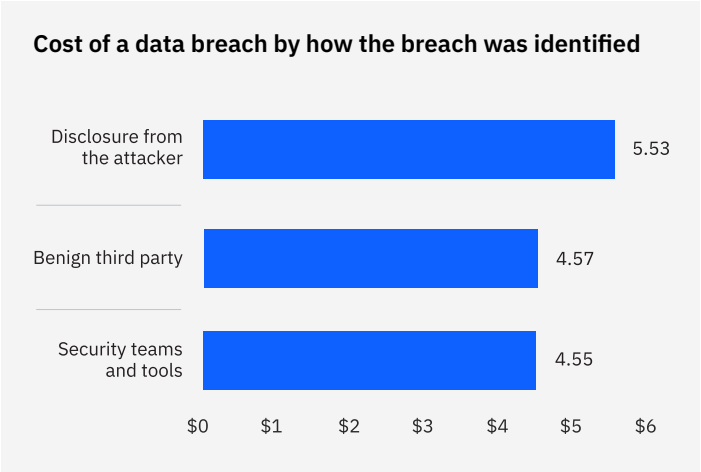


Figure 12. Measured in USD millions

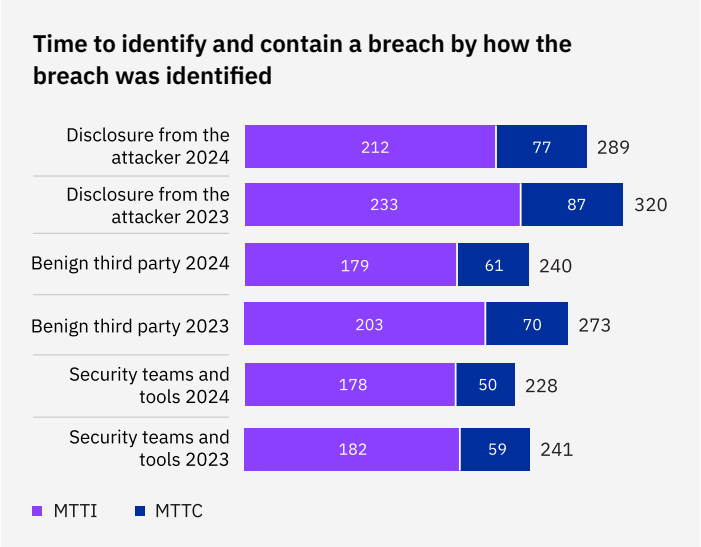


Figure 13. Measured in days

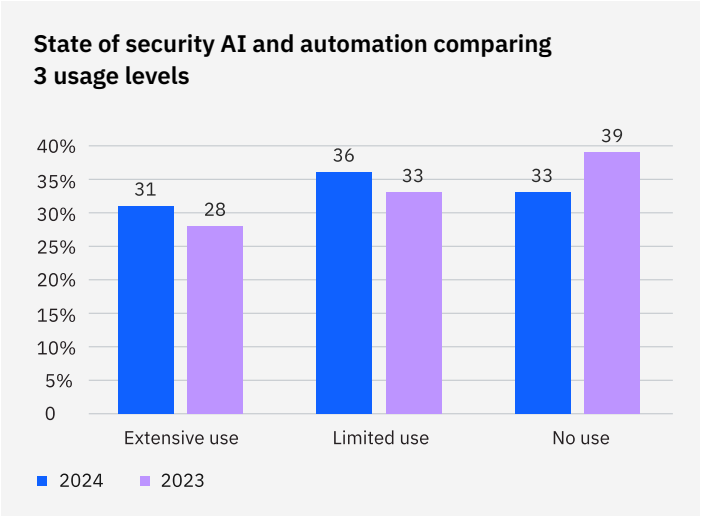


Figure 14. Percentage of organizations per usage level

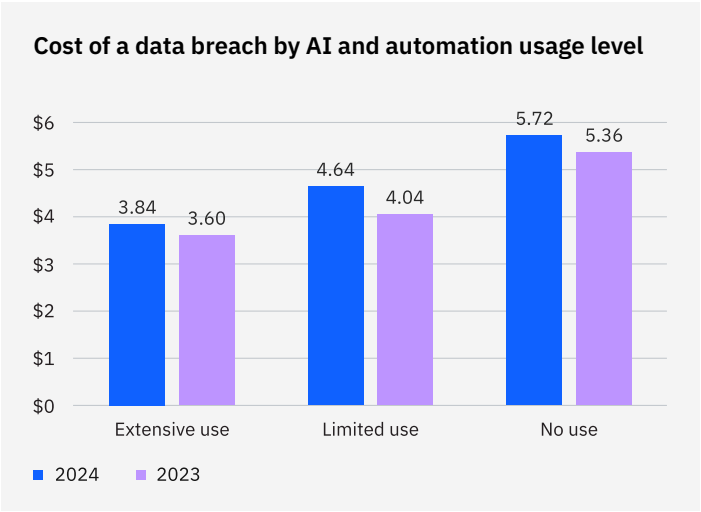


Figure 15. Measured in USD millions

Security AI and automation

AI and automation are transforming the world of cybersecurity. They make it easier than ever for bad actors to create and launch attacks at scale and provide defenders with new tools for rapidly identifying threats and automating responses to those threats. This year's report found these technologies accelerated the work of identifying and containing breaches and reducing costs.

AI and automation use grew

The number of organizations that used security AI and automation extensively grew to 31% in this year's study from 28% last year. Although it's just a 3 percentage point difference, it represents a 10.7% increase in use. The share of those using AI and automation on a limited basis also grew from 33% to 36%, a 9.1% increase. See Figure 14.

More AI and automation meant lower breach costs

The more organizations used AI and automation, the lower their average breach costs. That correlation is striking and one of the key findings of this year's report. Organizations not using AI and automation had average costs of USD 5.72 million, while those making extensive use of AI and automation had average costs of USD 3.84 million, a savings of USD 1.88 million. See Figure 15.

27%

Share of organizations that used AI and automation across 4 security categories.

More AI equaled faster identification and containment
Organizations extensively using security AI and automation identified and contained data breaches nearly 100 days faster on average than organizations that didn't use these technologies at all. See Figure 16.

Security teams applied AI and automation evenly across functions
Among organizations that stated they used AI and automation extensively, about 27% used AI extensively in each of these categories: prevention, detection, investigation and response. Roughly 40% used AI technologies at least somewhat. See Figure 17.

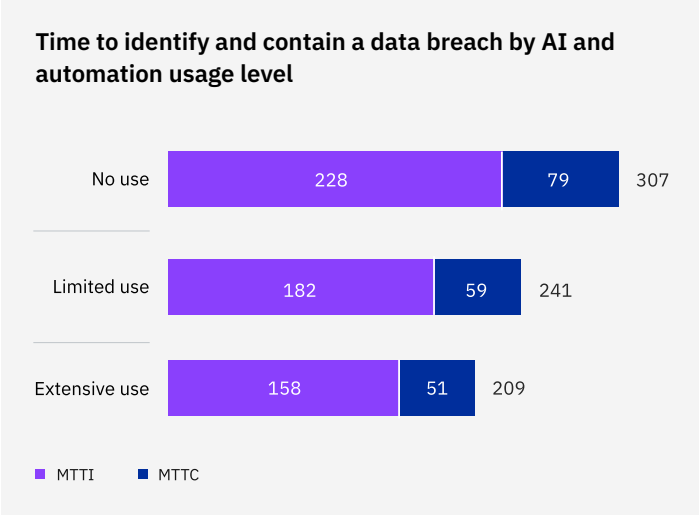


Figure 16. Measured in days

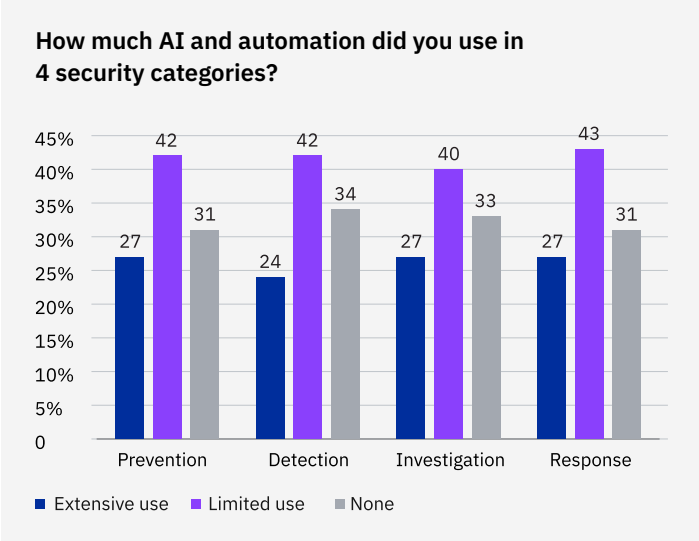


Figure 17. From the respondents that reported extensive use of AI and automation; reference chart 14

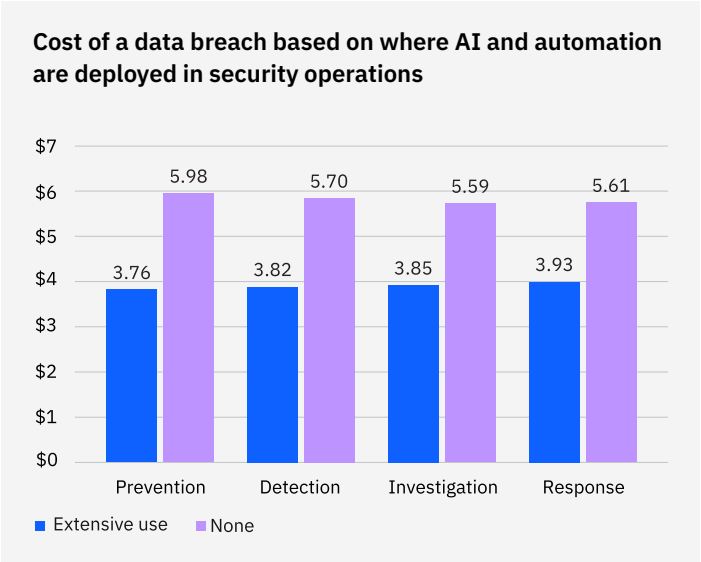


Figure 18. From the organizations that reported extensive use of AI and automation, measured in USD millions; reference chart 14

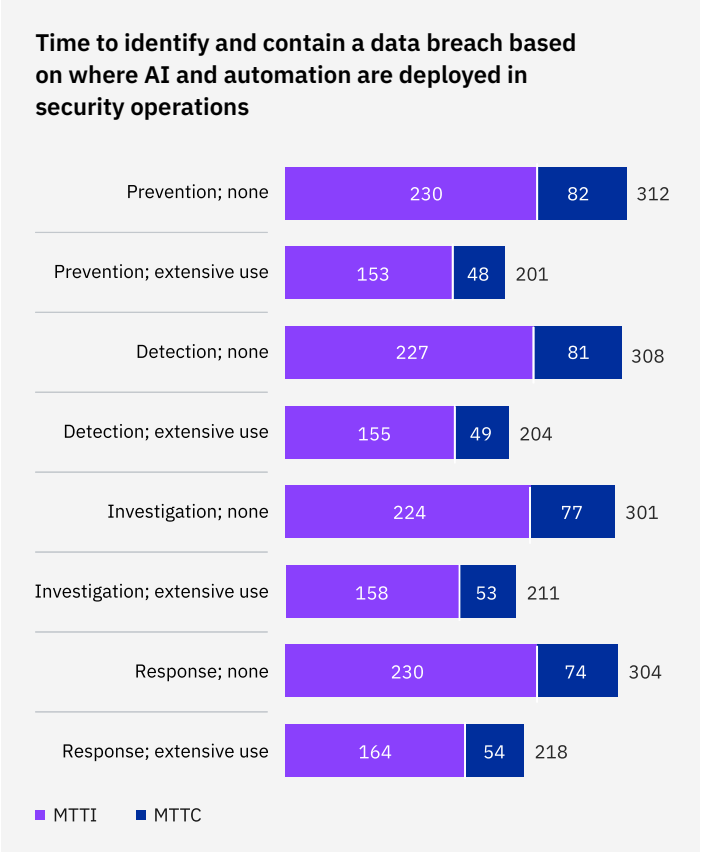


Figure 19. From the organizations that reported extensive use of AI and automation, measured in days; reference chart 14

Extensive use of AI and automation lowered costs

When AI and automation were used extensively in each of the 4 areas of security, it dramatically lowered average breach costs compared to organizations that didn't use these technologies in those areas. For example, when organizations used AI and automation extensively for prevention, their average breach cost was USD 3.76 million. Meanwhile, organizations that didn't use these tools in prevention saw USD 5.98 million in costs, a 45.6% difference. See Figure 18.

AI and automation accelerated the time to identify and contain a breach

Wherever AI and automation were applied, they accelerated the work of identifying and containing breaches. Extensive use of AI and automation in any security function—prevention, detection, investigation or response—reduced the average MTTI and MTTC for data breaches by 33% for response and 43% for prevention. See Figure 19.

70%

Share of organizations that experienced a significant or very significant disruption to business as a result of a breach.

Raising prices post-breach

By their nature, data breaches are expensive. When organizations find themselves saddled with multimillion-dollar costs, they may look to recoup those costs elsewhere. One option is to pass them along to their own customers in the form of price hikes, which is an increasing trend. Raising prices can be risky in a market already facing pricing pressure.

Organizations passed breach costs to customers
Most organizations said they planned to increase prices of goods and services following a data breach, passing costs along to customers. The share of organizations that planned to do so increased to 63% this year from 57% last year, representing a 10.5% increase. See Figure 20.

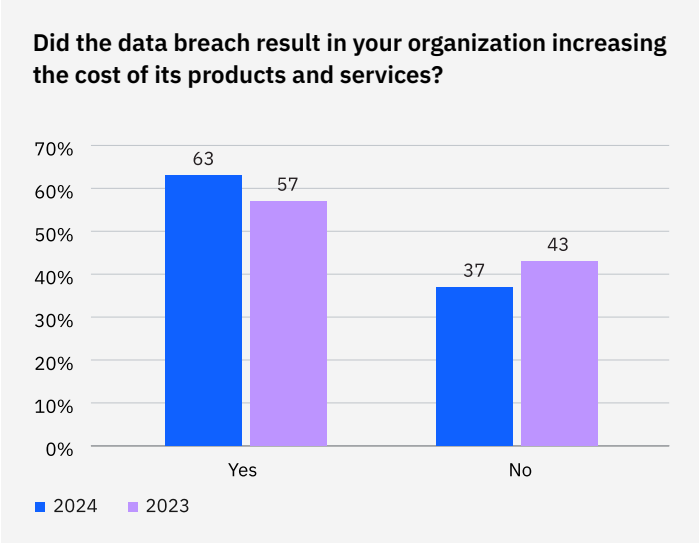


Figure 20. Share of all organizations

Business disruption

Business runs on data. When data is breached, business is disrupted. These disruptions can vary from small breaches that affect only a few systems to long-lasting, organization-wide, operational shutdowns. Our research explored how minor or significant those disruptions were, and how the severity of a disruption correlated with data breach costs.

Business disruption was substantial
70% of organizations in this year's study experienced a significant or very significant disruption to business resulting from a breach. Only 1% described their level of disruption as low. See Figure 21.

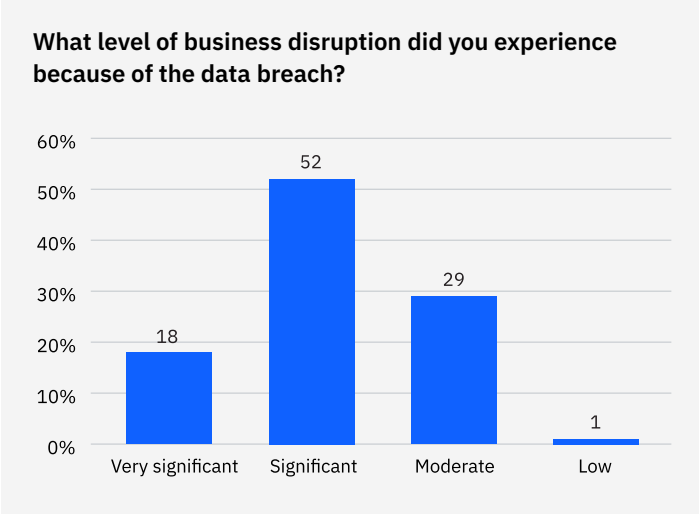


Figure 21. Only 1 response permitted

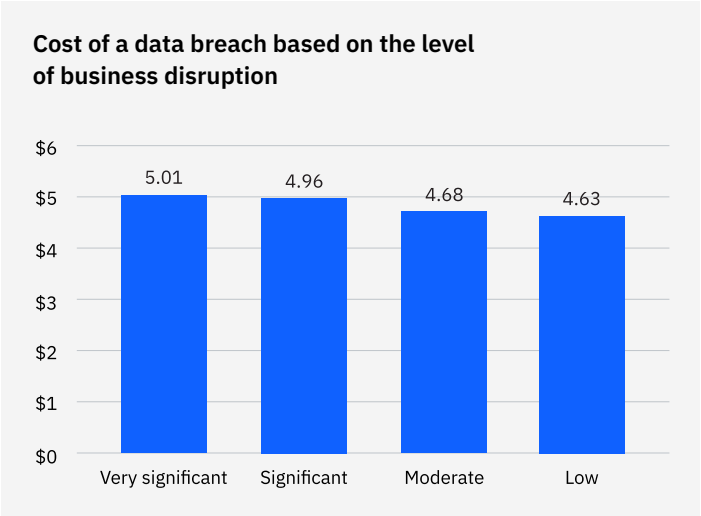


Figure 22. Measured in USD millions

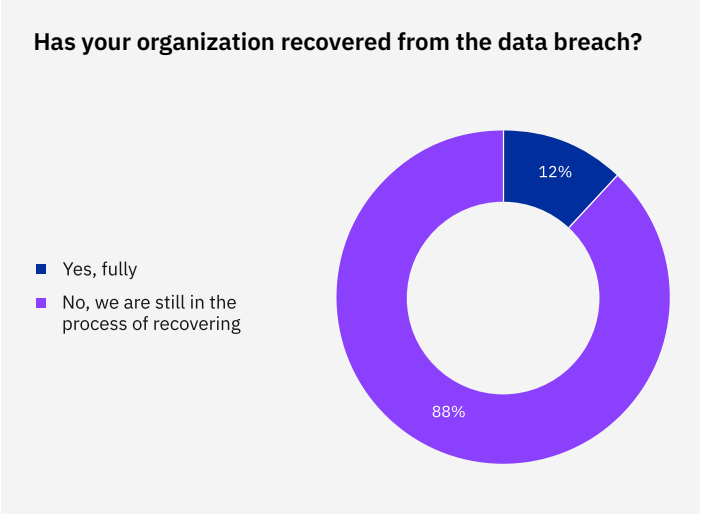


Figure 23. Share of all breached organizations

Average cost of a breach increased with disruption
Average breach costs were higher when business disruption was greater. Even organizations that reported low levels of disruption incurred average data breach costs of USD 4.63 million. For organizations that reported very significant disruptions, average costs were 7.9% higher, at USD 5.01 million. See Figure 22.

Recovery time

Even after a breach is contained, the work of recovery goes on. In this study, recovery means:

- Business operations are back to normal in areas affected by the breach.
- Organizations have met compliance obligations, such as paying fines.
- Customer confidence and employee trust have been restored.
- Organizations have put controls, technologies and expertise in place to avoid future data breaches.

Much of this work, such as re-establishing customer confidence, involves factors beyond technology. For most organizations, the hard work of recovery can be months away.

Breach recovery rates were low
Only 12% of organizations queried during this year's report said they had fully recovered from their data breaches. Most organizations said they were still working on them. See Figure 23.

Full recovery took longer than 100 days
Among the share of organizations that had fully recovered, more than three-quarters said they took longer than 100 days. Recovery is a protracted process. Roughly one-third of organizations that had fully recovered said they required more than 150 days to do so. A small share, 3%, of fully recovered organizations were able to do so in less than 50 days. See Figure 24.

Average time to recover from a data breach

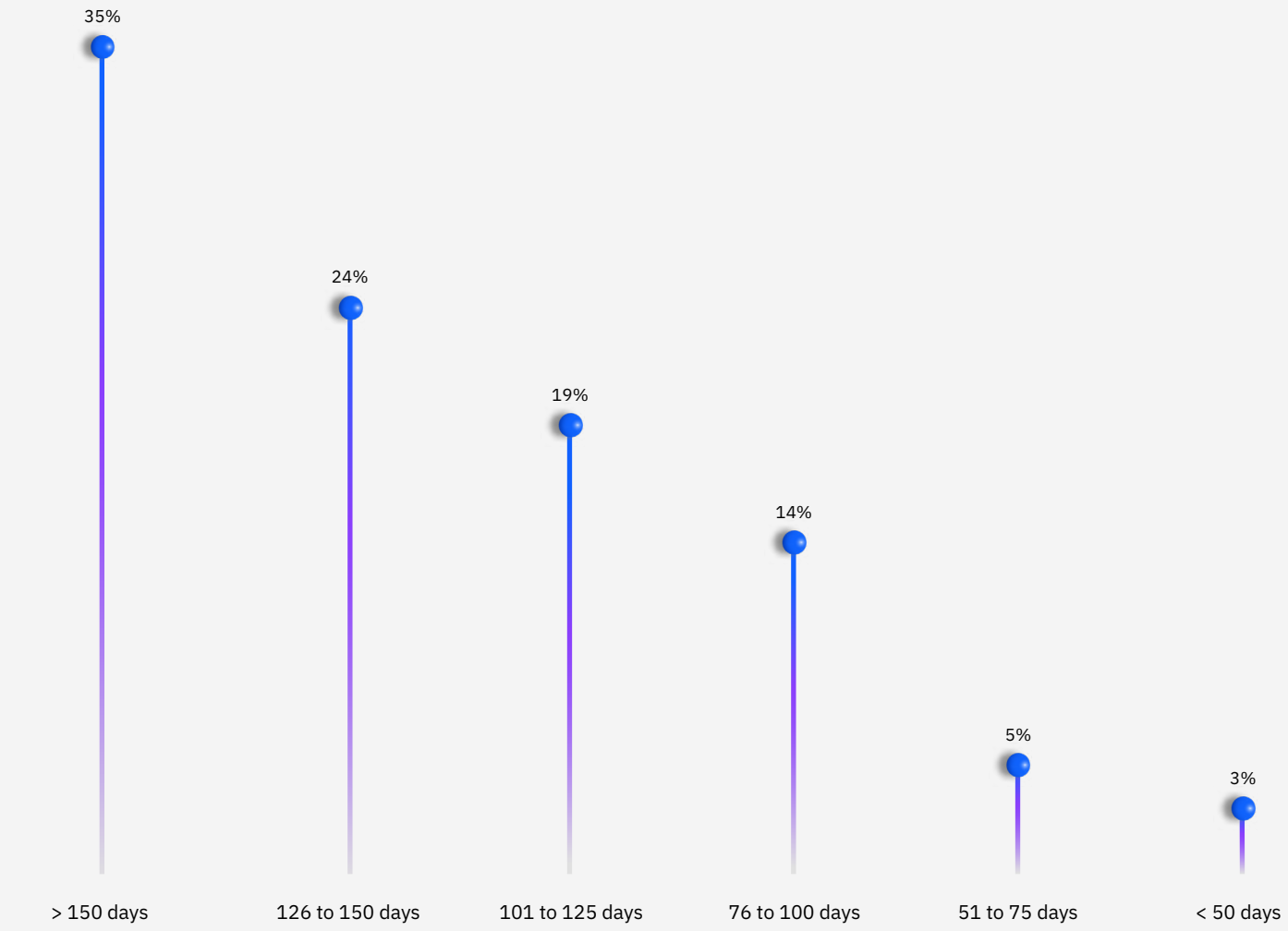


Figure 24. From the organizations that reported they had recovered fully from the incident, measured in days (reference chart 23)

Figure 25. Cost difference from USD 4.88M breach average; measured in USD

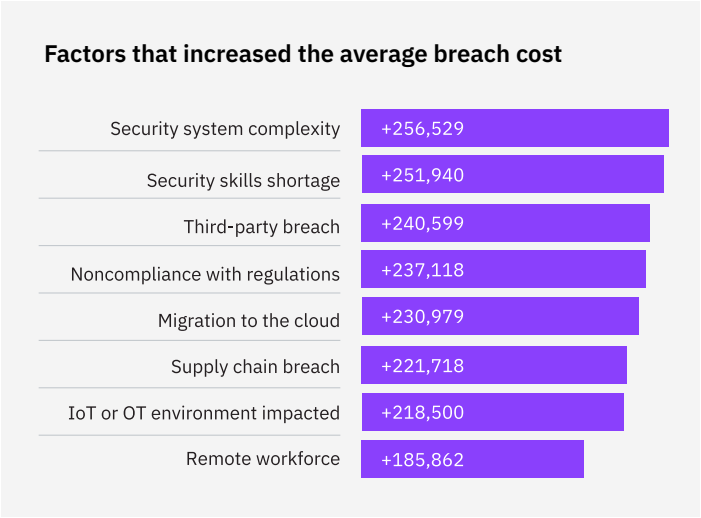


Figure 26. Cost difference from USD 4.88M breach average; measured in USD

Factors that decreased or increased the average breach cost

When analyzing costs, it's helpful to know which technologies or events tend to lower or raise them. One constant we found: AI and automation lowers costs, while a high level of cyber skills shortage raises them. In this analysis, we looked at 28 contributing factors. We examined the impact of each in isolation against the global average. We then looked at the top 3 factors found to amplify or mitigate the average data breach cost.

Key factors that reduced costs
Employee training and the use of AI and machine learning insights were the top factors mitigating average data breach costs in this analysis. Employee training continues to be an essential element in cyberdefense strategies, specifically for detecting and stopping phishing attacks. AI and machine learning insights closely followed in second place. See Figure 25.

Key factors that increased costs
The top 3 factors that amplified breach costs in this analysis were security system complexity, security skills shortage and third-party breaches, which can include supply chain breaches. See Figure 26.

USD 5.74M

Average breach costs for organizations experiencing a high-level shortage of security skills.

High versus low levels of key cost amplifying factors
When organizations suffered from a high-level shortage of security skills, average breach costs were USD 5.74 million, compared to organizations with a low-level skills shortage, with USD 3.98 million. Similar disparities were seen across 2 other key cost factor areas. See Figure 27.

High versus low levels of key cost mitigating factors
When organizations suffered from low levels of employee training, average breach costs were USD 5.10 million, compared to organizations with high levels of employee training, with USD 4.15 million. Similar disparities were seen across 2 other key cost factor areas. See Figure 28.

Cost of a data breach for organizations with a high level versus low level of 3 cost amplifying factors

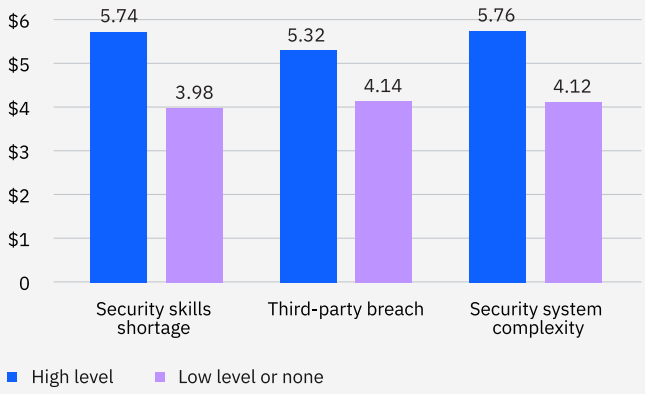


Figure 27. Measured in USD millions

Cost of a data breach for organizations with a high level versus low level of 3 cost mitigating factors

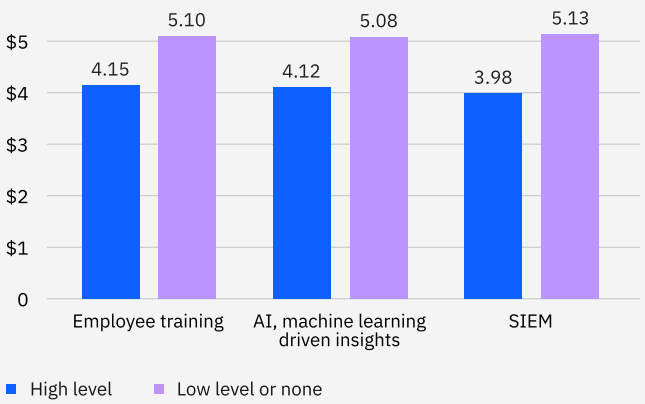


Figure 28. Measured in USD millions

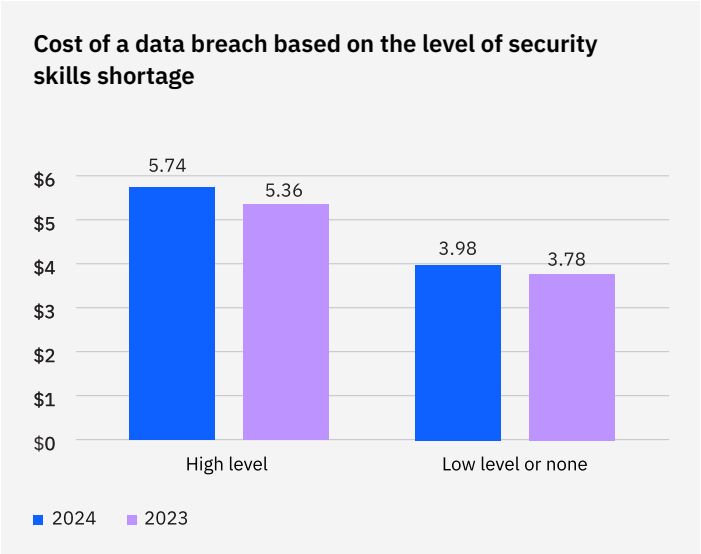


Figure 29. Measured in USD millions

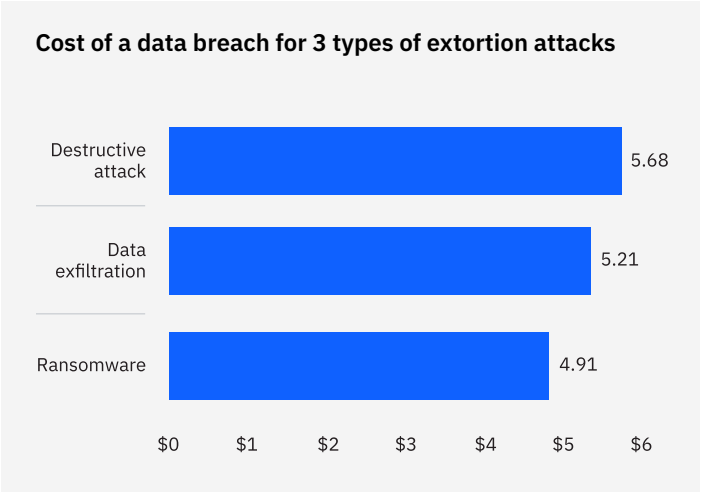


Figure 30. Measured in USD millions

Security skills shortage

The number of organizations facing a critical lack of skilled security workers rose dramatically, to 53% in 2024 compared to 42% last year. This year's research found a strong link between the worsening skills shortage and higher data breach costs.

Skills shortage equated to higher breach costs
In 2024, the average cost of breaches associated with a high-level skills shortage jumped to USD 5.74 million from USD 5.36 million last year, a 7.1% rise. This increase was USD 860,000 higher than the global average breach cost. See Figure 29.

The cost of extortion attacks

The amount an organization spends on extortion attacks can vary based on type—ransomware, data exfiltration and destructive—as well as the way the organization responds. This factor is particularly true if law enforcement is called in, as this year's study shows, where costs dropped dramatically when law enforcement investigators were involved. All 3 types of attacks were examined, including ransomware, where data is encrypted and a ransom demanded; data exfiltration, where data is stolen and the organization sometimes extorted; and destructive, where attackers delete data and destroy systems for their own objectives.

Cost of destructive attacks outpaced other extortion
Destructive attacks, or those attacks that are intended to cause lasting and expensive damage, reached an average of USD 5.68 million, and proved more costly than either ransomware attacks or data exfiltration attacks. See Figure 30.

63%

Share of ransomware victims that involved law enforcement and avoided paying a ransom.

Time to identify and contain 3 types of extortion attacks
All 3 types of attacks required between 284 and 294 days to identify and contain. See Figure 31.

Paying the ransom
When organizations fell victim to ransomware, 52% called in law enforcement. The majority of those that did, 63%, ended up not paying the ransom. See Figure 32.

Time to identify and contain a data breach based on the occurrence of 3 types of extortion attack

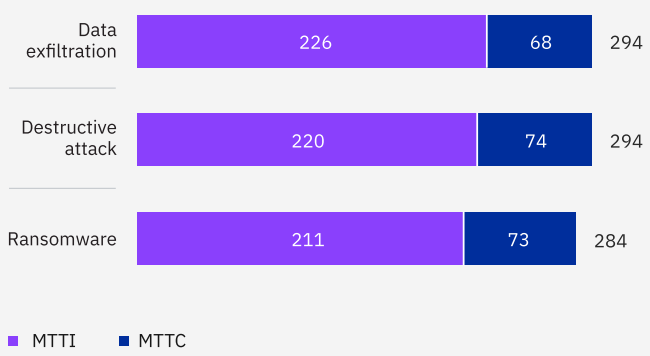


Figure 31. Measured in days

Share of ransomware victims with law enforcement involved that paid a ransom

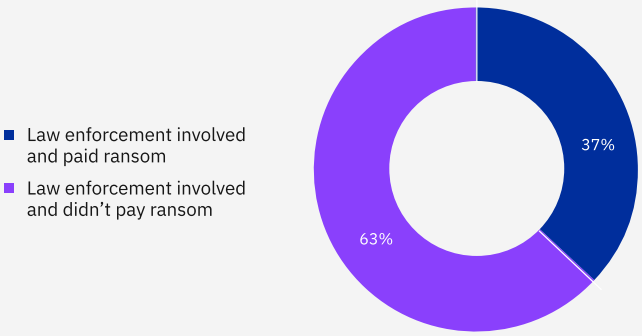


Figure 32.

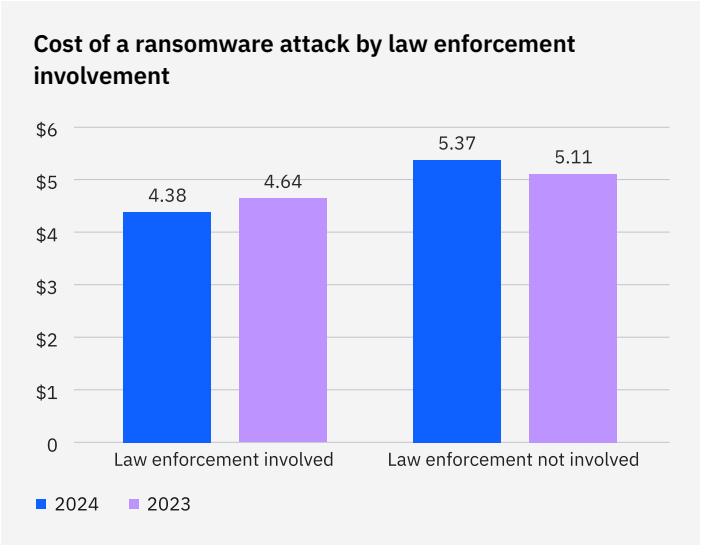


Figure 33. Measured in USD millions

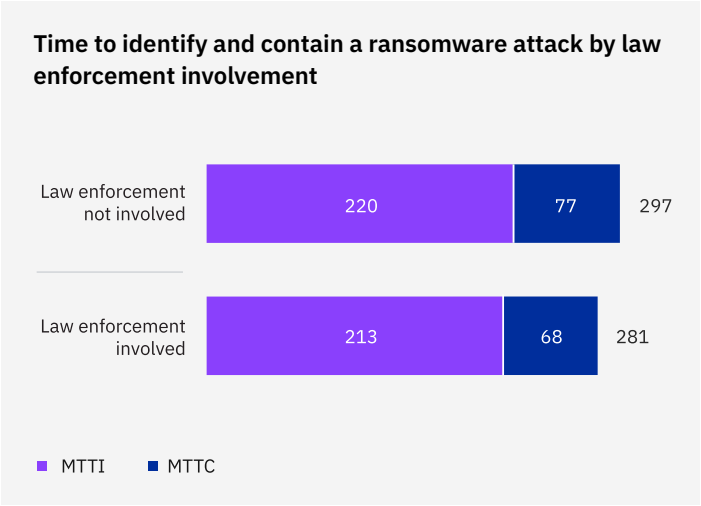


Figure 34. Measured in days

Law enforcement involvement lowered breach costs
Average breach costs ranged from USD 4.38 million with law enforcement involved to USD 5.37 million without law enforcement, a cost difference of more than 20%, or nearly USD 1 million. Note: those cost figures didn't include ransom payments. See Figure 33. Law enforcement involvement also sped up the time it took to identify and contain a breach. See figure 34.

↑22.7%

Increase in the share of organizations paying fines of more than USD 50,000.

Reporting the breach and regulatory fines

This year's report found most organizations reported their breaches to regulators or other government agencies. About a third also paid fines. As a result, reporting and paying fines have become common parts of post-breach responses. The study looked at the size of fines, as well as how long it took organizations to disclose the breach to regulators. Most organizations reported the breach within a few days.

Average breach reporting times
Over half of organizations reported their data breach in under 72 hours, while 34% took more than 72 hours to report. Just 11% were not required to report the breach at all. See Figure 35.

Amount of regulatory fines are rising
More organizations paid higher regulatory fines, with those paying more than USD 50,000, rising 22.7% over last year, and those paying more than USD 100,000, rising 19.5%. See Figure 36.

Did you have to report the breach due to regulatory mandates and if so, how long did it take you to report after discovery?

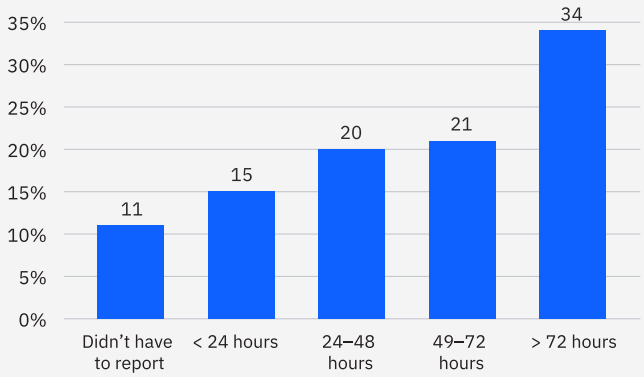


Figure 35. Share of all breaches, only 1 response permitted

Distribution of cost of fines incurred from a data breach

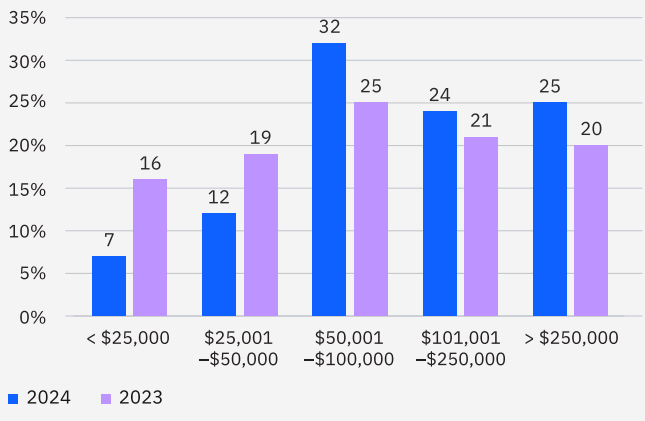


Figure 36. Among those that experienced fines, measured in USD

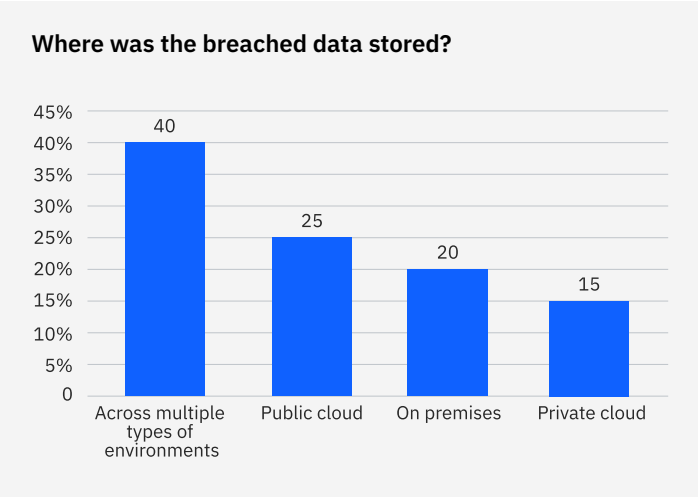


Figure 37. Share of all organizations; 1 response permitted

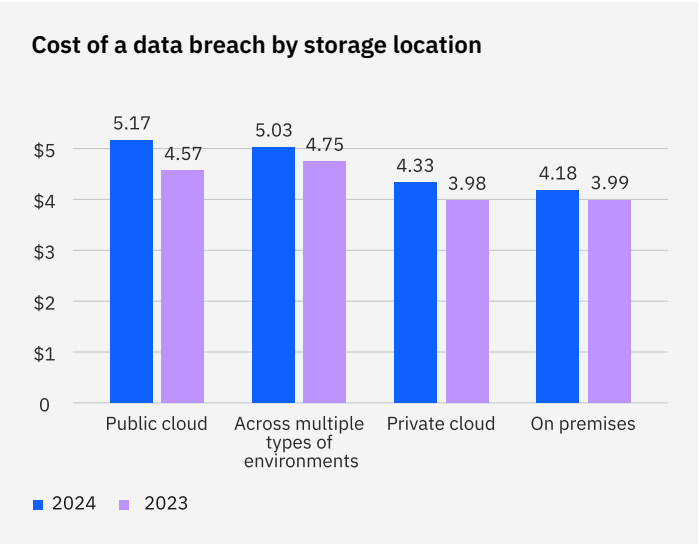


Figure 38. Measured in USD millions

Data security

No matter where data is stored, it can be vulnerable to a breach. This year's study shows some places are more vulnerable and costly per breach than others. Most breaches involved data distributed across multiple environments or public clouds. Both storage options were associated with longer breach lifecycles and higher breach costs.

Even as organizations expand and refine their data management strategies, they often overlook shadow data—data that's unmanaged and likely invisible to the IT department. It could be the result of workers sharing data through unauthorized applications or uploading it to unofficial cloud buckets. The report found when breaches involved shadow data, they lasted longer and led to greater costs.

Cloud breaches

Breaches by data location
About 40% of all breaches involved data distributed across multiple environments, such as public clouds, private clouds and on premises. Fewer breaches in the study involved data stored solely in a public cloud, private cloud or on premises. With data becoming more dynamic and active across environments, it's harder to discover, classify, track, and also secure. See Figure 37.

Breaches by location and cost
Data breaches solely involving public clouds were the most expensive type of data breach, costing USD 5.17 million on average, a 13.1% increase from last year. Breaches involving multiple environments were more common but slightly less expensive than public cloud breaches. On-premises breaches were the least costly. See Figure 38.

USD 5.27M

Average cost of a data breach involving shadow data.

Centralized control related to faster remediation
The more centralized control organizations had over their data, the quicker on average they could identify and contain a breach. Breaches involving data stored solely on premises took an average of 224 days to identify and contain, 23.3% less time than data distributed across environments, which took 283 days. The same pattern of local control and shortened breach lifecycles showed up in the comparison between private cloud architectures and public cloud architectures. See Figure 39.

Shadow data

Breach costs for shadow data
The average cost of a data breach involving shadow data was USD 5.27 million, 16.2% higher than the average cost without shadow data. See Figure 40.

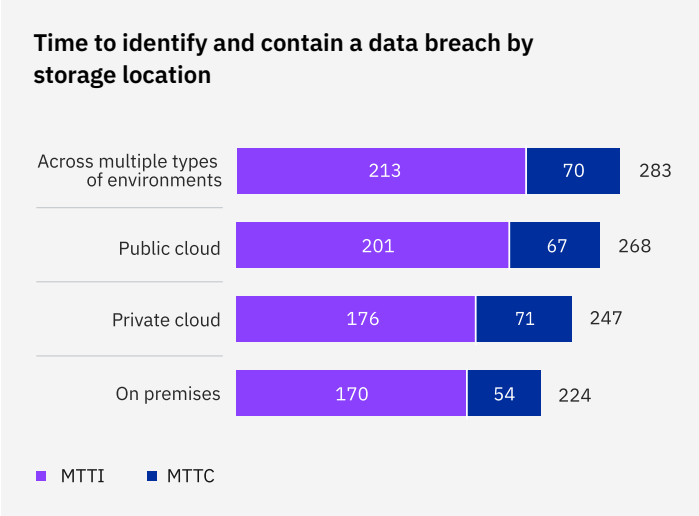


Figure 39. Measured in days

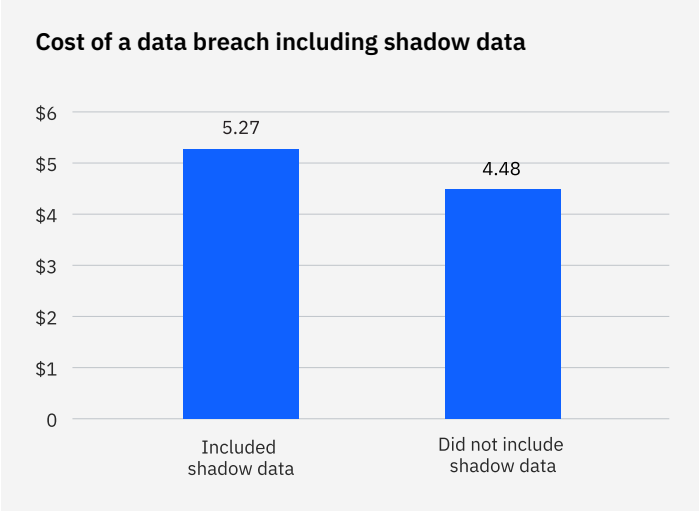


Figure 40. Measured in USD millions

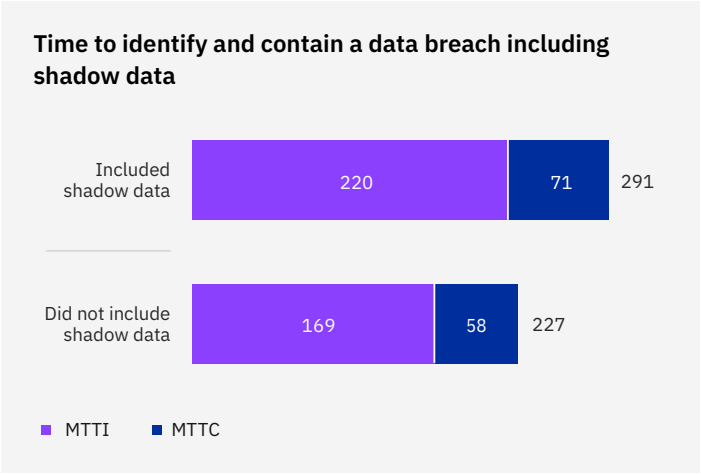


Figure 41. Measured in days

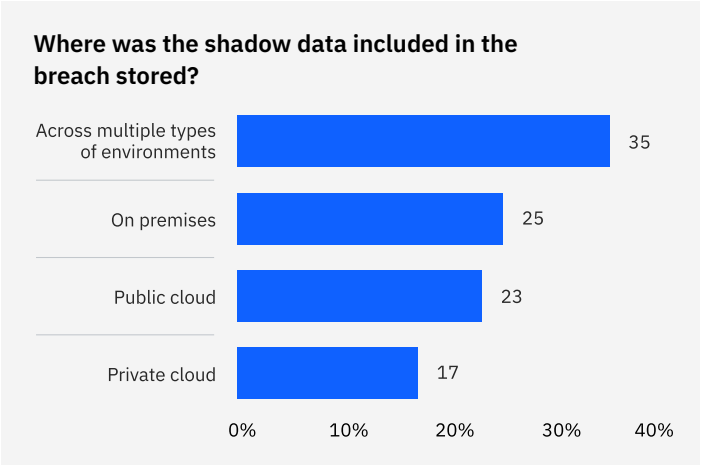


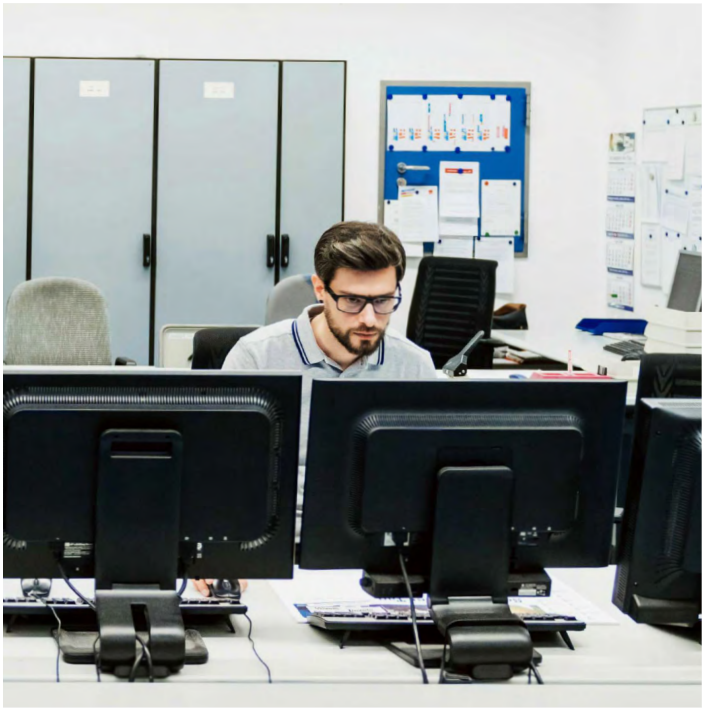
Figure 42. Percentage of breaches involving shadow data; 1 response permitted

Breach lifecycles for shadow data

Breaches involving shadow data took 26.2% longer on average to identify and 20.2% longer on average to contain than those that didn't. These increases resulted in data breaches lasting an average lifecycle of 291 days, 24.7% longer than data breaches without shadow data. See Figure 41.

Shadow data across environments

While shadow data was found in every type of environment—public and private clouds, on premises and across multiple environments—25% of breaches involving shadow data were solely on premises. That finding means shadow data isn't strictly a problem related to cloud storage. See Figure 42.



Mega breaches

Mega breaches, characterized by more than 1 million compromised records, are relatively rare. Accordingly, the research treats them separately from most other breaches, partly so that they don't skew the analysis of more typical data breaches.

Mega breach costs rose

The average cost of all mega breach size categories was higher this year than last. The jump was most pronounced for the largest breaches, affecting between 50 million and 60 million records. The average cost increased by 13%, and these breaches were many times more expensive than a typical breach. For even the smallest mega breach—1 million to 10 million records—the average cost was nearly 9 times the global average cost of USD 4.88 million. See Figure 43.

Cost of a mega breach by number of records lost

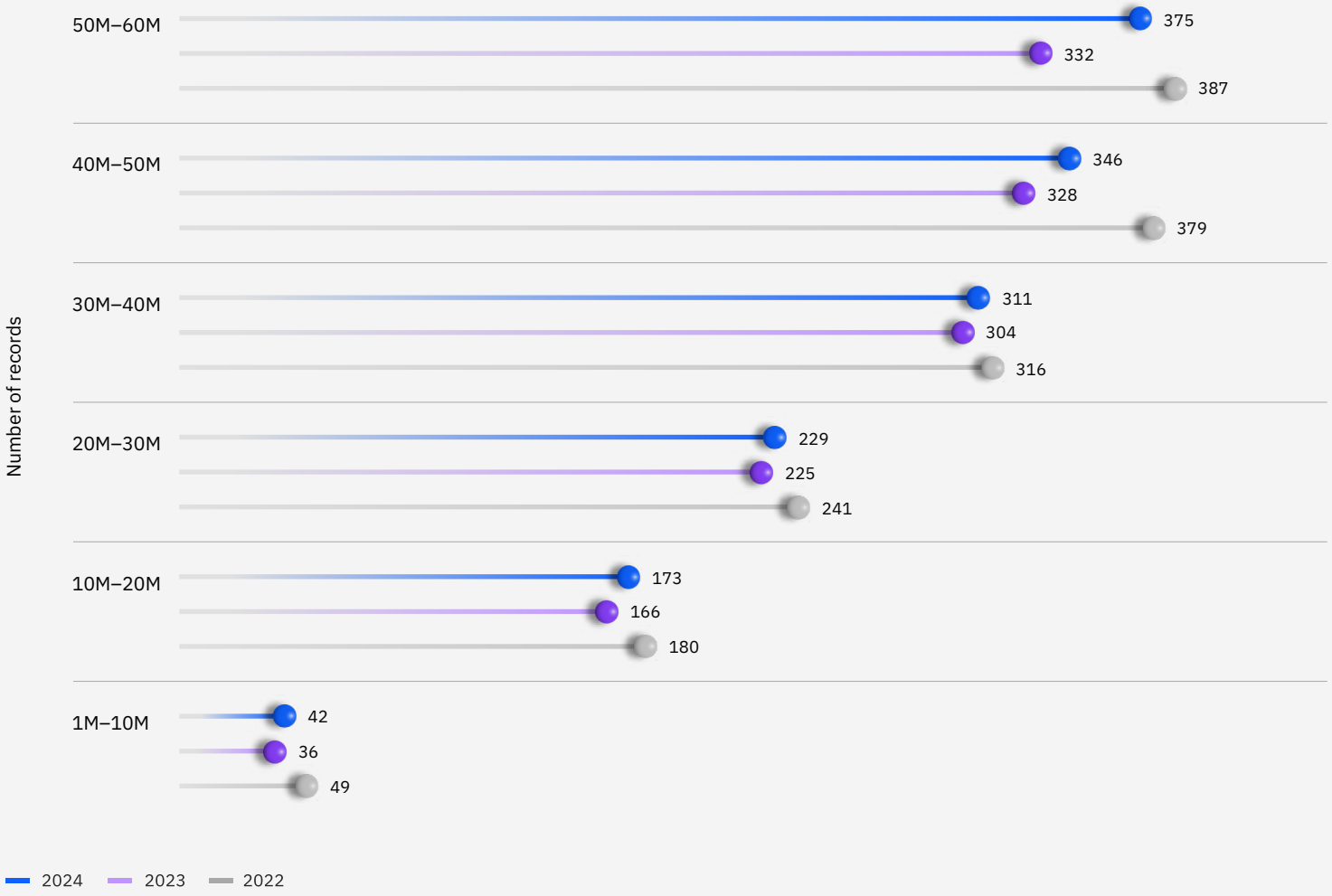


Figure 43. Measured in USD millions

↑23.5%

Increase in share of organizations that plan to boost their security investments following a breach.

Following the data breach, will your organization increase its security investment?

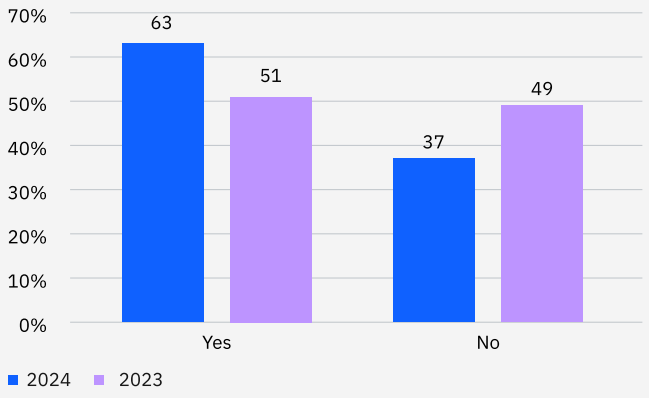


Figure 44. Percentage of all organizations

Most common investment types among those increasing security investments after a data breach

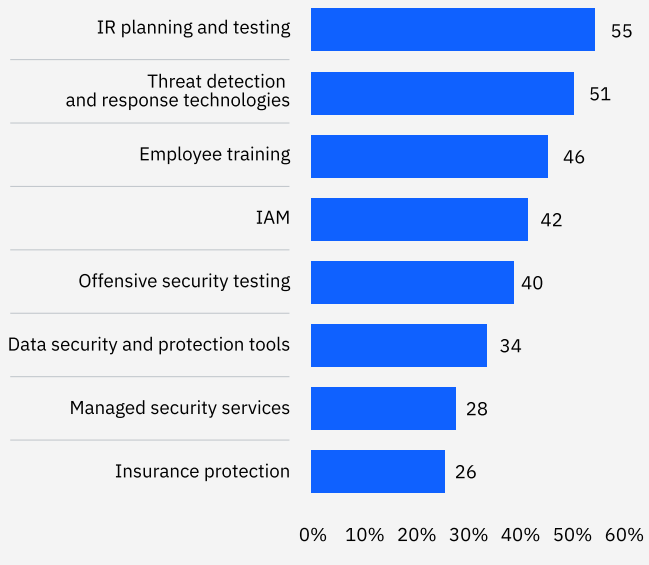


Figure 45. Share among organizations that are increasing security investment; more than 1 response permitted

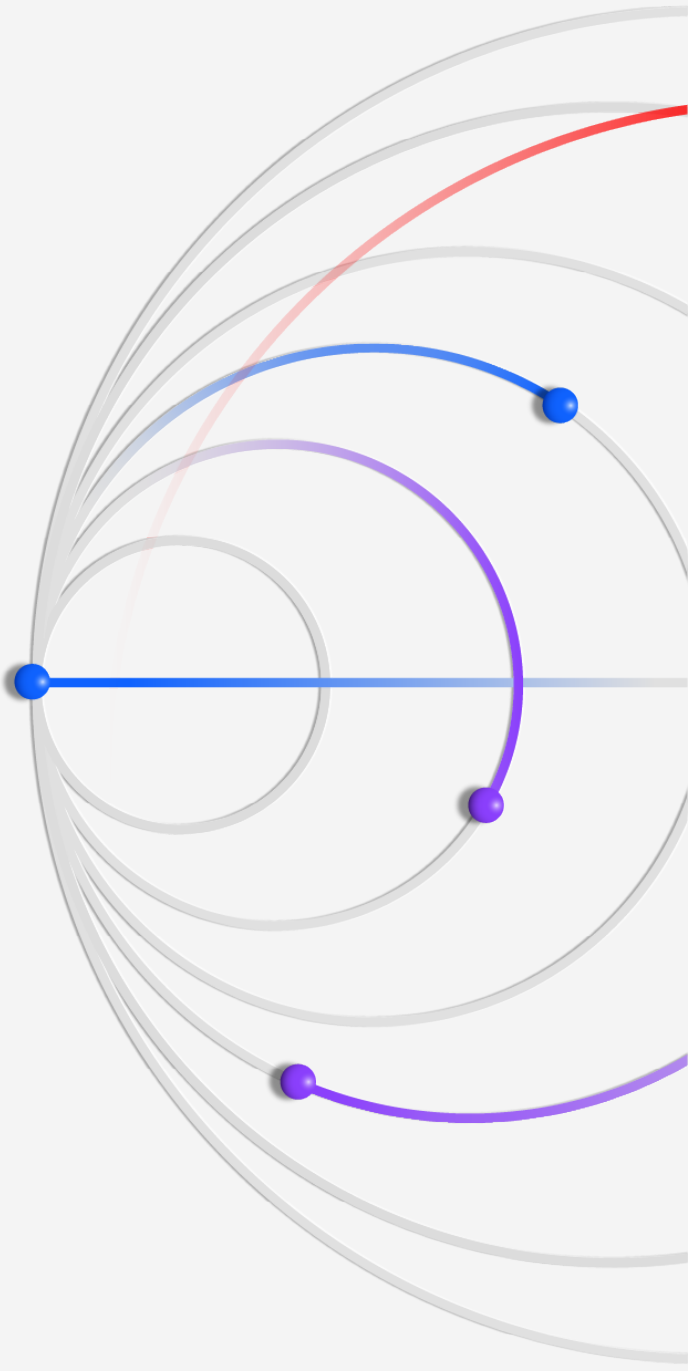
Security investments

When an organization is breached, its business and IT leaders often increase their security investments. This year's study asked organizations about their plans for future security spending. Organizations were permitted to identify more than 1 area of investment.

Share of organizations making security investments rose
Almost two-thirds of organizations planned to increase security investments following a breach, a 23.5% rise over last year. This rise may reflect a realization that breach costs related to lost business and regulatory fines continue to grow, along with the potential for reputational damage. See Figure 44.

Popular areas of security investment
The 2 most popular areas of security investment reported this year were IR planning and testing, at 55%, and threat detection and response technologies, at 51%. The focus of the top 2 investment areas was on detecting suspicious incidents and threats and responding to them more quickly. Many organizations were also planning to invest in data security and protection tools, at 34%, and IAM, at 42%. See Figure 45.

Recommendations to help reduce the cost of a data breach



Our recommendations include successful security approaches that are associated with reduced costs and lower times to identify and contain breaches.

Know your information landscape

Most organizations distribute data across multiple environments, including on-premises data repositories, private clouds and public clouds. However, many organizations have incomplete or out-of-date data inventories, delaying efforts to discover what data has been breached and how sensitive or confidential it is. These delays can complicate the response and raise the cost of a breach.

Security teams should ensure they have comprehensive visibility into all these environments, so they can continuously monitor and protect data regardless of where it resides. Organizations can apply data security posture management (DSPM) and other

solutions, such as identity access management and ASM, across all these environments for consistent and comprehensive protection.

Security teams must pay extra attention to hybrid environments and public clouds. 40% of data breaches involved data stored across multiple environments, and when breached data was stored in public clouds, it incurred the highest average breach cost at USD 5.17 million. It's imperative security teams gain a deeper understanding of the specific risks and controls for each cloud service they employ.

Managing data across environments becomes further complicated by the impact of unmanaged data. More than one-third of data breaches involve shadow data. Security teams must now assume their organizations have unmanaged data sources. Unencrypted data, including data in AI workloads, further exacerbates the risk. Data encryption strategies must consider the types of data, its use and where it resides to lower risk in case of a breach.

Strengthen prevention strategies with AI and automation

The adoption of gen AI models and third-party applications across the organization—as well as the ongoing use of Internet of Things (IoT) devices and SaaS applications—are expanding the attack surface, putting pressure on security teams.

Applying AI and automation that support security prevention strategies—including in the areas of ASM, red-teaming and posture management—can often be addressed by managed security services. Organizations that applied AI and automation to security prevention saw the biggest impact from their AI investments in this year's study compared to 3 other security areas: detection, investigation and response. They saved an average of USD 2.22 million over those organizations that didn't deploy AI in prevention technologies.

Take a security-first approach to gen AI adoption

While organizations are moving quickly ahead with gen AI, only 24% of gen AI initiatives are being secured. The lack of security threatens to expose data and data models to breaches, potentially undermining the benefits that gen AI projects are intended to deliver.

As gen AI adoption continues to scale, organizations need a framework for securing gen AI data, models and usage, along with establishing AI governance controls. They'll need to secure the training data by protecting it from theft and manipulation. Organizations can use data discovery and classification to detect sensitive data used in training or fine-tuning. They can also implement data security controls across encryption, access management and compliance monitoring.

With gen AI, not only are organizations faced with the risk of, and growth in, shadow data, but also shadow models. Organizations must extend posture management to the AI models themselves to protect sensitive AI training data, gain visibility into the use of unsanctioned or *shadow AI* models, and AI misuse or data leakage.

Securing gen AI model development requires scanning for vulnerabilities in the pipeline, hardening integrations, and enforcing policies and access. To secure the use of gen AI models requires security teams to monitor for malicious inputs, such as prompt injections, and outputs containing sensitive data. They must also deploy AI security solutions that can detect and respond to AI-specific attacks, such as data poisoning, model evasion and model extraction. Developing response playbooks to deny access, and quarantine and disconnect compromised models is essential as well.

With threat landscapes expanding because of gen AI and other IT initiatives, security training needs to be offered to non-security practitioners, including data scientists and data engineers working in AI teams.

Level up your cyber response training

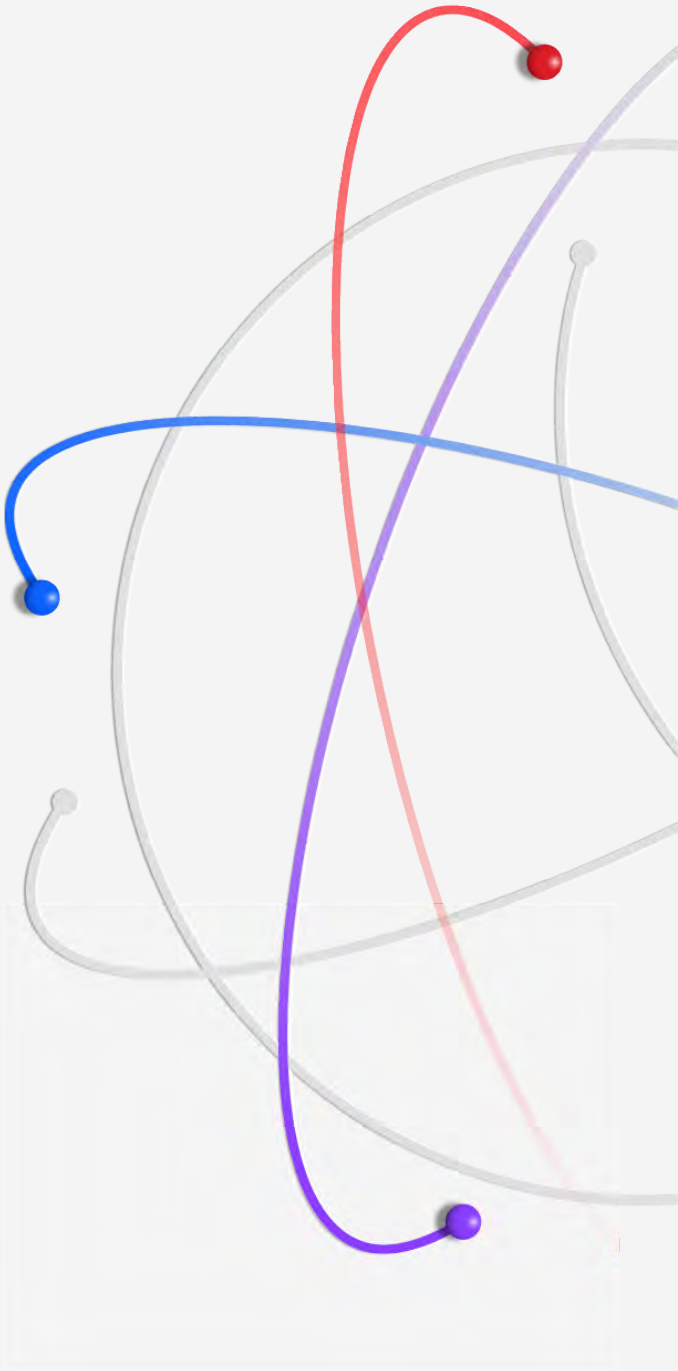
How an organization reacts and communicates during and after a breach—with business leadership, regulators and customers—matters more than ever. To enhance their ability to handle high-impact attacks, organizations can build up their muscle memory for breach responses by participating in cyber range crisis simulation exercises.

These exercises can include security teams as well as business leaders, so the entire organization improves its ability to detect, contain and respond to breaches. Security leaders should work with their business functions across the organization and communications teams ahead of time to draft response plans and test them. With threat landscapes expanding because of gen AI and other IT initiatives, security training needs to be offered to non-security practitioners. These practitioners include data scientists and data engineers working in machine learning and AI teams and those tasked with continuity of AI workloads across on-premises and cloud assets.

By investing in response preparedness, organizations can help reduce the costly, disruptive effects of data breaches, support operational continuity and help preserve their relationships with customers, partners and other key stakeholders. Moreover, rehearsed response reassures employees and reduces stress, distress and friction internally as the acute stages of an attack are handled, controlled and communicated by a well-prepared leadership team.

Organization demographics

This year’s study examined 604 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.



Geographic demographics

The 2024 study was conducted across 16 countries and geographic regions. One new region added this year to the study was Benelux, the economic union of Belgium, the Netherlands and Luxembourg. Scandinavia was dropped from the study.

ASEAN is a cluster sample of organizations located in Singapore, Indonesia, Philippines, Malaysia, Thailand and Vietnam. Latin America is a cluster sample of organizations located in Mexico, Argentina, Chile and Colombia. Middle East is a cluster sample of organizations located in Saudi Arabia and the United Arab Emirates.

Global study at a glance

Countries and regions	2024 sample	% of total sample	Years studied	Currency
ASEAN	25	4%	8	Singapore dollars (SGD)
Australia	27	4%	15	Australian dollars (AUD)
Benelux	32	5%	1	Euro (EUR)
Brazil	45	7%	12	Brazilian real (BRL)
Canada	28	5%	10	Canadian dollars (CAD)
France	36	6%	15	Euro (EUR)
Germany	47	8%	16	Euro (EUR)
India	53	9%	13	Indian rupee (INR)
Italy	29	5%	13	Euro (EUR)
Japan	42	7%	13	Yen (JPY)
Latin America	28	5%	5	Mexican pesos (MXN)
Middle East	39	6%	11	Saudi Arabia riyal (SAR)
South Africa	24	4%	9	South African rand (ZAR)
South Korea	28	5%	7	Won (KRW)
United Kingdom	50	8%	17	Pound sterling (GBP)
United States	71	12%	19	US dollars (USD)
Total	604	100%		

Figure 46. Share of all organizations in the study

Industry demographics

The selection of 17 industries has been consistent across multiple years of the study. This year, the top 4 industries—financial, industrial, professional services and technology—accounted for 47% of the 604 organizations studied.

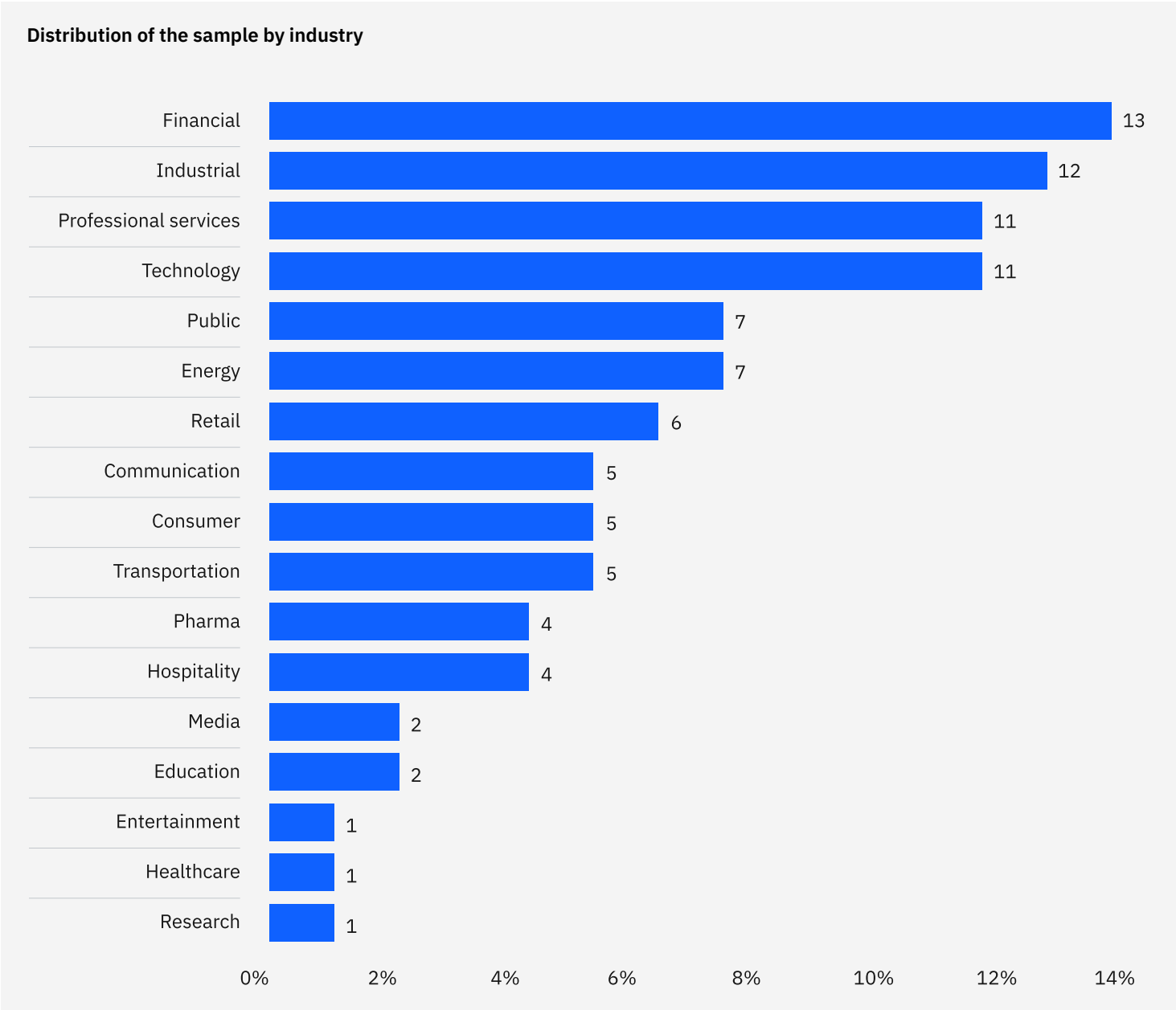


Figure 47. Share of all organizations in the study

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
Pharmaceutical companies, 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

Professional 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

Public
Federal, state and local government agencies, and nongovernmental organizations

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 dataset for benchmarking, the report included only those cost activity centers with a crucial impact on data breach costs. Based on discussions with experts, a fixed set of cost activities was chosen. After collecting benchmark information, each instrument was carefully reexamined for consistency and completeness.

The scope of data breach cost factors was limited 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, we excluded very small and very large breaches. Data breaches examined in the 2024 report ranged in size between 2,100 and 113,000 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.

We used activity-based costing, which identifies activities and assigns a cost according to actual use. Four process-related activities drove 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 an organization to detect the breach include:

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

Notification
Activities that enable an organization to notify data subjects, data protection regulators and other third parties include:

- 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 an organization and conduct redress activities to victims and regulators include:

- 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 include:

- 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 data breach is defined as an event in which records containing 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 between 2,100 and 113,000 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 over 3,556 separate interviews with individuals at 604 organizations that suffered a data breach between March 2023 and February 2024. Interviewees were familiar with their organization's data breach and the costs associated with resolving the breach. These interviewees included CEOs or executives, heads of operations, controllers or heads of finance, IT practitioners, business unit leaders and general managers, and risk management and cybersecurity practitioners. For privacy purposes, we didn't collect organization-specific information.

What's included in the 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 604 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 a maximum of 113,000 compromised records. To measure the impact of mega breaches that involve 1 million or more records, the study instead uses a simulation framework based on a sample of 17 events of that size.

Why did you use simulation methods to estimate the cost of a mega data breach?
The sample size of 17 organizations 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 269,000 trials. The grand mean of all sample means provided a most likely outcome at each size of data breach, ranging from 1 million to 53 million compromised records.

Are you tracking the same organizations each year?
Each annual study involves a different sample of organizations. To be consistent with previous reports, we recruit and match organizations each year with similar characteristics, such as the organization'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 6,184 organizations.

Research limitations

Our study used a confidential and proprietary benchmark method that was 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 organizations 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 organizations being studied. We believe the current sampling frame was biased toward organizations with more mature privacy or information security programs.

Organization-specific information
The benchmark didn't capture organization-identifying information. Individuals could use categorical response variables to disclose demographic information about the organization 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 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 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 4 March 2024.

About IBM and Ponemon Institute

IBM

IBM is a leading global hybrid cloud, AI and business services provider, helping clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. All of it is backed by IBM's legendary commitment to trust, transparency, responsibility, inclusivity and service. For more information, visit www.ibm.com.

Learn more about advancing your security posture:

Visit ibm.com/security

Join the conversation in the IBM Security Community

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 personally identifiable information (PII) from individuals or company-identifiable information in business research. Furthermore, strict quality standards ensure subjects aren't asked extraneous, irrelevant or improper questions.

If you have questions or comments about this research report, including requests for permission to cite or reproduce the report, contact us by letter, phone call or email:

Ponemon Institute LLC
Research Department
1-800-887-3118
research@ponemon.org

© Copyright IBM Corporation 2024

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2024

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

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

THE 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: 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 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.