Cost of a Data Breach Report 2025

The AI Oversight Gap

think report

IBM

Table of contents

Executive summary

Welcome to IBM's annual Cost of a Data Breach Report. With this edition, we mark 20 years of data breach research. This year, we set our sights on the most fundamental technological shift in a generation: the adoption of AI.

With the 2025 report, we begin chronicling and quantifying the risks associated with AI. What we've found is concerning: organizations are skipping over security and governance for AI in favor of do-it-now AI adoption. Those ungoverned systems are more likely to be breached—and more costly when they are. We're not surprised.

Since 2005, this report has tracked an ever expanding technology landscape and the threats that follow it. Our research partners at Ponemon Institute have not only documented the emergence of new threats and attack surfaces, but also quantified these threats in financial terms security and business leaders can understand and act on. All told, their researchers have studied more than 6,485 breaches and interviewed over 34,652 technology, security and business leaders involved in their organization's response to the breach.

20 Years of Data Breach Research

Obviously, security threats have changed through the years. Two decades ago, nearly half of all data breaches (45%) were caused by a lost or stolen computing device, such as a laptop or thumb drive, while only 10% of breaches were attributed to "hacked electronic systems." Today, most breaches are caused by a range of malicious activities, from phishing to insider threats.

Ten years ago, breaches due to cloud misconfiguration weren't even a categorized threat. Today, the cloud and the data in it are a prime target. And it was only during the COVID-19 lockdowns in 2020 that ransomware began to surge. A year later, those attacks accounted for an average USD 4.62 million in breach costs, a figure that hit USD 5.08 million in this year's report.

However, one constant has been the work of Ponemon. This year's research—conducted independently by Ponemon Institute and sponsored, analyzed and published by IBM—studied 600 organizations impacted by data breaches between March 2024 and February 2025. Together, we looked at organizations across 17 industries, in 16 countries and regions, and breaches that ranged from 2,960 to 113,620 compromised records. To gain on-the-ground insights, Ponemon researchers interviewed 3,470 security and C-suite business leaders with firsthand knowledge of the data breach incidents at their organizations. These leaders included CEOs, CISOs, heads of operations, controllers or heads of finance, IT practitioners, business unit leaders and general managers, and risk management and cybersecurity practitioners.

The result is a benchmark report that business, technology and security leaders can use to strengthen their defenses, inform resource allocation and drive innovation, particularly around securing and governing their AI initiatives.

This year's headline: global data breach costs have declined for the first time in five years, dropping to USD 4.44 million, due to faster breach containment that was driven by AI-powered defenses. But as defenders move smarter and faster, so do attackers—16% of breaches reportedly involved attackers using AI, often used in phishing and deepfake attacks. While this escalating AI arms race has benefitted organizations by pushing global breach costs lower, the US is bucking the trend. Breach costs there have surged past USD 10 million, driven by steeper regulatory penalties and rising detection costs.

We also found AI adoption is outpacing oversight. We found 97% of AI-related security breaches involved AI systems that lacked proper access controls. And most breached organizations reported they have no governance policies in place to manage AI or prevent shadow AI—the use of AI without employer approval or oversight. Both the covert use of shadow AI and the lack of governance are driving up breach costs.

What's new in the 2025 report

As always, the Cost of a Data Breach Report reflects new technologies, emerging tactics and recent events. For the first time, this year's research explores the:

- State of security and governance for AI
- Prevalence and risk profile of shadow AI
- Type of data targeted in security incidents involving AI
- Length of breach disruptions to organizations
- Cost savings from using quantum security tools
- Breach costs associated with AI-driven attacks
- Amount of breach costs passed on to customers

Key findings

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

USD 4.44M

The global average cost of a data breach

The global average breach cost dropped to USD 4.44 million from USD 4.88 million in 2024, a 9% decrease and a return to 2023 cost levels. Faster identification and containment of breaches—much of it from organizations' own security and security service teams, with help from AI and automation—drove this decline. The global average would have been lower were it not for the United States, where the average cost surged by 9% to USD 10.22 million, an all-time high for any region. Higher regulatory fines and higher detection and escalation costs in the United States contributed to this surge.

97%

Share of organizations that reported an AI-related breach and lacked proper AI access controls

Security incidents involving an organization's AI remain limited—for now. On average, 13% of organizations reported breaches that involved their AI models or applications. However, among those that did, almost all (97%) lacked proper AI access controls. The most common of these security incidents occurred in the AI supply chain, through compromised apps, APIs or plug-ins. These incidents had a ripple effect: they led to broad data compromise (60%) and operational disruption (31%). The findings suggest AI is emerging as a high-value target.

USD 4.92M

Average cost of malicious insider attacks

For the second year in a row, malicious insider attacks resulted in the highest average breach costs among initial threat vectors: USD 4.92 million. Third-party vendor and supply chain compromise followed closely at USD 4.91 million. Other expensive attack vectors included vulnerability exploitation and phishing. However, the most frequent type of attack vector on organizations was phishing, at 16%, which averaged USD 4.8 million.

USD 670K

Added breach cost for shadow AI

Among the organizations studied this year, 20% said they suffered a breach due to security incidents involving shadow AI. For organizations with high levels of shadow AI, those breaches added USD 670,000 to the average breach price tag compared to those that had low levels of shadow AI or none. These incidents also resulted in more personal identifiable information (65%) and intellectual property (40%) data being compromised. And that data was most often stored across multiple environments, revealing just one unmonitored AI system can lead to widespread exposure. The swift rise of shadow AI has displaced security skills shortages as one of the top three costly breach factors tracked by this report.

USD 1.9M

Cost savings from extensive use of AI in security

Security teams using AI and automation extensively shortened their breach times by 80 days and lowered their average breach costs by USD 1.9 million compared to organizations that didn't use these solutions. Nearly a third of organizations said they used these tools extensively across the security lifecycle—in prevention, detection, investigation and response. However, that figure is up only slightly from the previous year, suggesting AI adoption may have stalled. It also shows the majority are still not using AI and automation and, therefore, aren't seeing the cost benefits.

63%

Share of organizations that refused to pay ransomware attackers

More ransomware victims refused to pay a ransom in 2025 (63%) than 2024 (59%). However, the average cost of an extortion or ransomware incident remains high, particularly when disclosed by an attacker (USD 5.08 million). At the same time, fewer ransomware victims reported involving law enforcement—40% of organizations this year versus 53% last year.

49%

Share of organizations investing in security post breach

There was a significant reduction in the number of organizations that plan to invest in security following a breach, 49% this year compared to 63% last year. Less than half of those who plan to invest in a security plan to focus on AI-driven security solutions or services, such as threat detection and response, incident response (IR) planning and testing, and data security or protection tools.

63%

Share of organizations that lack AI governance policies

A majority of breached organizations (63%) either don't have an AI governance policy or are still developing one. Even when they have a policy, less than half have an approval process for AI deployments, and 61% lack AI governance technologies. Among organizations that have governance polices in place, only a minority (34%) perform regular audits for unsanctioned AI. It shows AI remains largely unchecked as adoption outpaces both security and governance.

1 in 6

Number of breaches involving AI-driven attacks

Attackers can use generative AI (gen AI) to both perfect and scale their phishing campaigns and other social engineering attacks. IBM previously found gen AI reduced the time needed to craft a convincing phishing email from 16 hours down to only five minutes. This year's report shows the impact: on average, 16% of data breaches involved attackers using AI, most often for AI-generated phishing (37%) and deepfake impersonation attacks (35%).

Complete findings

The complete findings from this year's survey address 16 themes, presented in the following order:

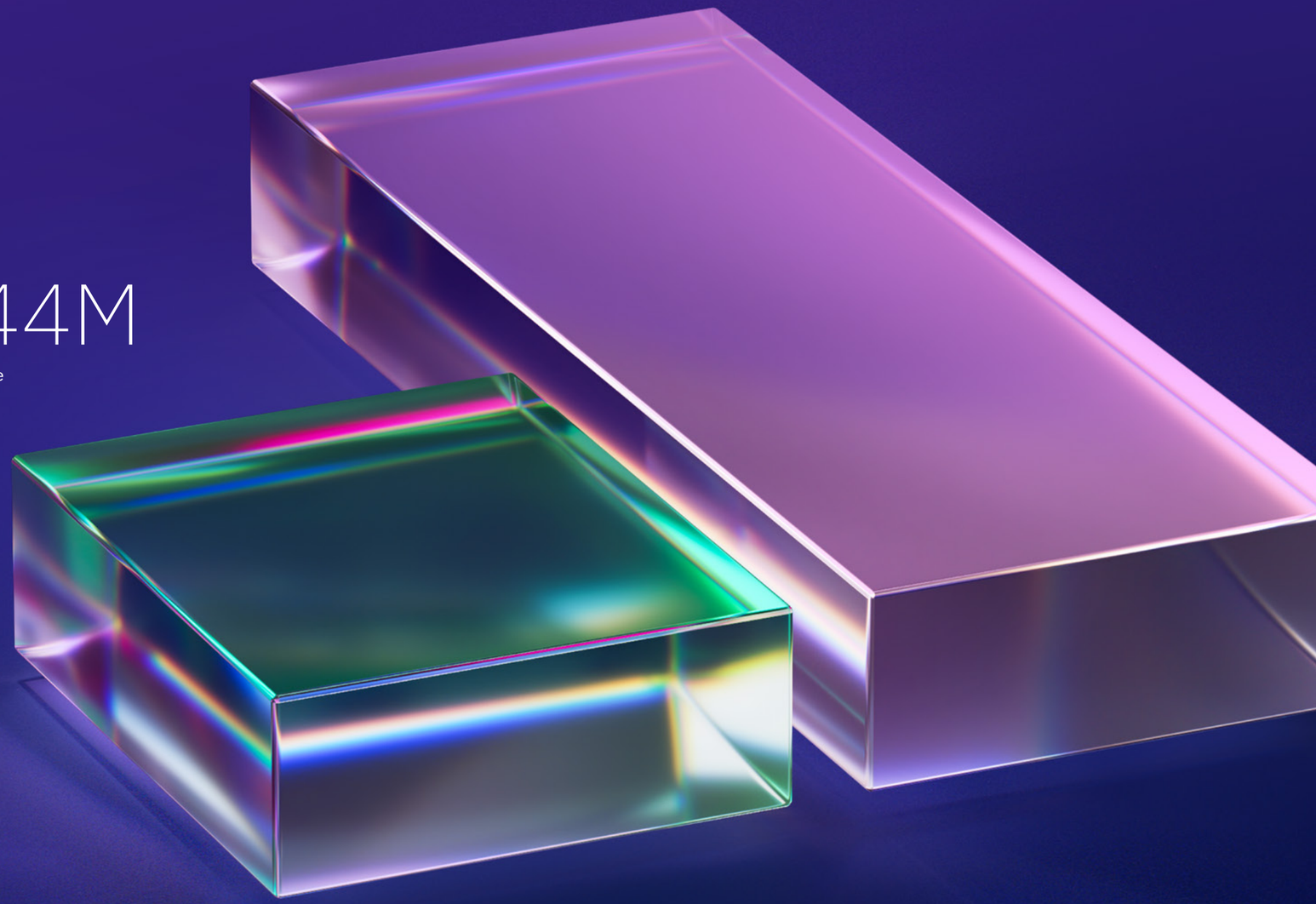
- Global highlights
- Data security
- Initial attack vectors and root causes
- Data breach lifecycle
- Identifying the breach
- Regulatory fines
- Recovery time
- Breaches involving AI
- AI governance
- AI-driven attacks
- Ransomware attacks
- Raising prices post-breach
- Business disruption
- Factors that increase or decrease breach costs
- Security AI and automation
- Security investments

10.22M

United States average

4.44M

Global average



Globally, the average cost of a data breach fell while it hit a record high in the US.

Measured in USD

Global highlights

While the cybersecurity skill shortage continues to grow, security teams are managing to identify and contain beaches faster, with the help of AI and automation. That approach is helping drive down data breach costs globally. These teams are doing so even as attackers use gen AI to create and scale realistic phishing and deepfake attacks. Despite the overall global decrease, the United States saw breach costs rise, driven by higher regulatory fines and increased detection and escalation costs. Healthcare continues to top the list of costliest industries for breaches. The following section provides a look at these and other issues across industries, countries and regions.

The global average cost of a data breach fell
For the first time in five years, the global average cost of a data breach dropped, reaching USD 4.44 million. Globally, shorter breach investigations are pushing down detection and escalation costs, which can include assessment and audits, crisis management, and communications to executive leadership and boards. See Figure 1.

Figure 1.
Measured in USD millions

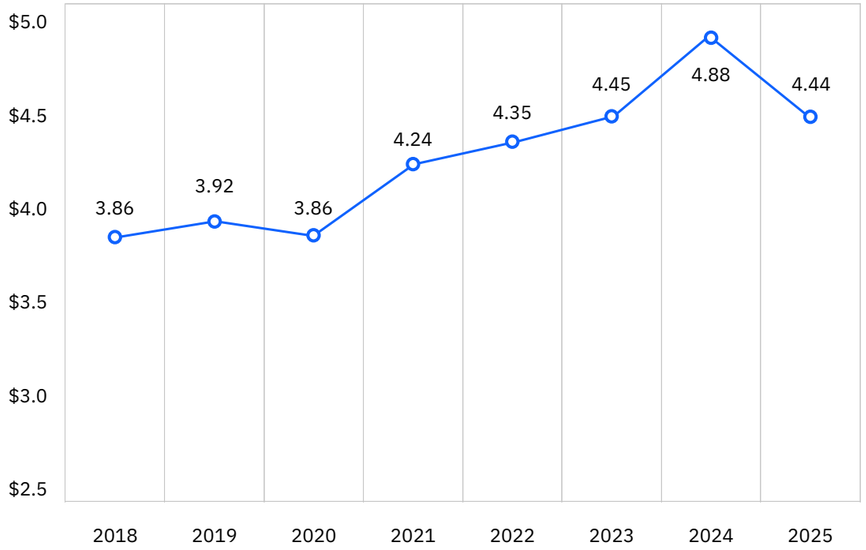


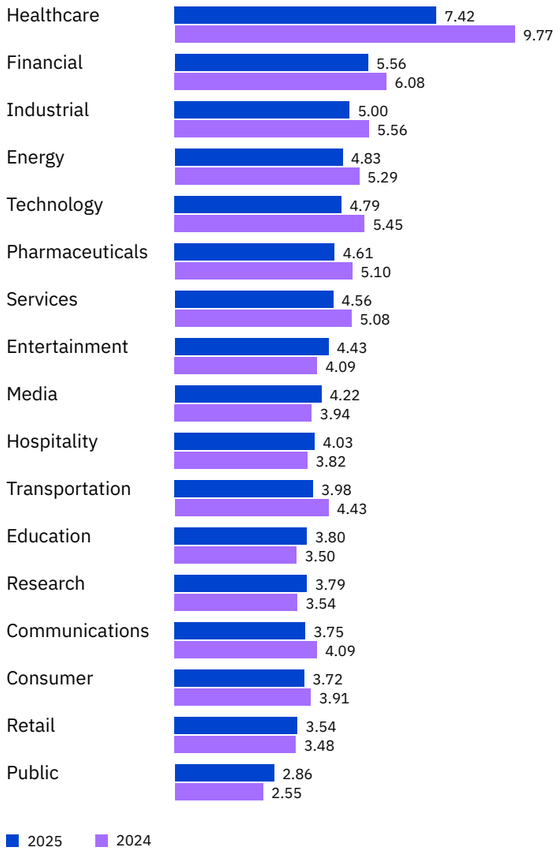
Figure 2.
Measured in USD millions

#	Country		2025	2024
1	United States	↑	$10.22	$9.36
2	Middle East	↓	$7.29	$8.75
3	Benelux	↑	$6.24	$5.90
4	Canada	↑	$4.84	$4.66
5	United Kingdom	↓	$4.14	$4.53
6	Germany	↓	$4.03	$5.31
7	Latin America	↓	$3.81	$4.16
8	France	↓	$3.73	$4.17
9	ASEAN	↑	$3.67	$3.23
10	Japan	↓	$3.65	$4.19
11	Italy	↓	$3.44	$4.73
12	South Korea	↓	$2.84	$3.62
13	Australia	↓	$2.55	$2.78
14	India	↑	$2.51	$2.35
15	South Africa	↓	$2.37	$2.78
16	Brazil	↓	$1.22	$1.36

The United States breaks a breach cost record
Average breach costs in the United States reached a record USD 10.22 million, a 9% increase over last year, driven in part by higher regulatory fines and detection and escalation costs. Most countries or regions recorded a decrease, due to lower detection and escalation costs. Some places, such as Saudi Arabia, were likely assisted by increased security spending and maturing security frameworks. Among the decliners were Italy (-27%), Germany (-24%) and South Korea (-21.5%). On the increase list were Canada, India, the Association of Southeast Asian Nations (ASEAN) and Benelux—the economic union of Belgium, the Netherlands and Luxembourg. Benelux made its debut in the 2024 study and witnessed a 6% increase in average breach cost. See Figure 2.

Healthcare remained the most expensive industry for breaches
At USD 7.42 million, healthcare recorded the highest average breach cost among industries for the 12th consecutive year—even as it saw a sharp reduction from last year (USD 9.77 million). Attackers continue to value and target the industry's patient personal identification information (PII), which can be used for identity theft, insurance fraud and other financial crimes. Healthcare breaches took the longest to identify and contain at 279 days. That's more than five weeks longer than the global average. See Figure 3.

Figure 3.
Measured in USD millions



Time to identify and contain a breach decreased
The mean time organizations took to identify and contain a breach fell to 241 days, reaching a nine-year low and continuing a downward trend that started after a 287-day peak in 2021. As noted in last year's report, security teams continue to improve their mean time to identify (MTTI) and mean time to contain (MTTC) with the help of AI-driven and automation-driven defenses. See Figure 4.

Figure 4.
Measured in days

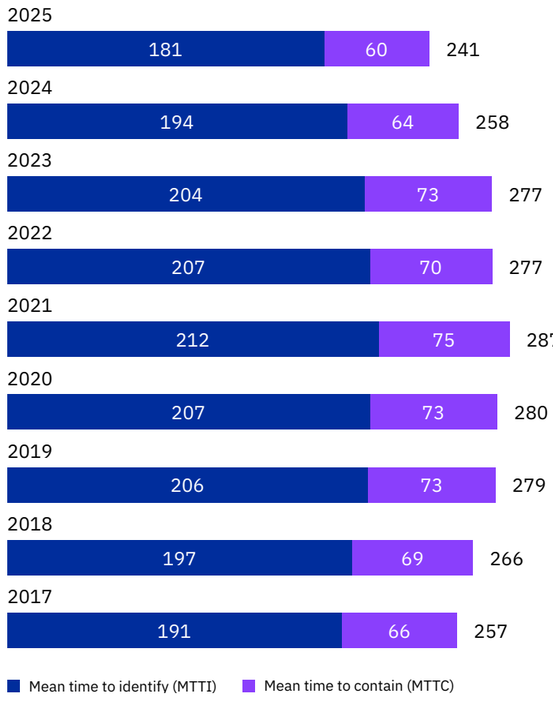
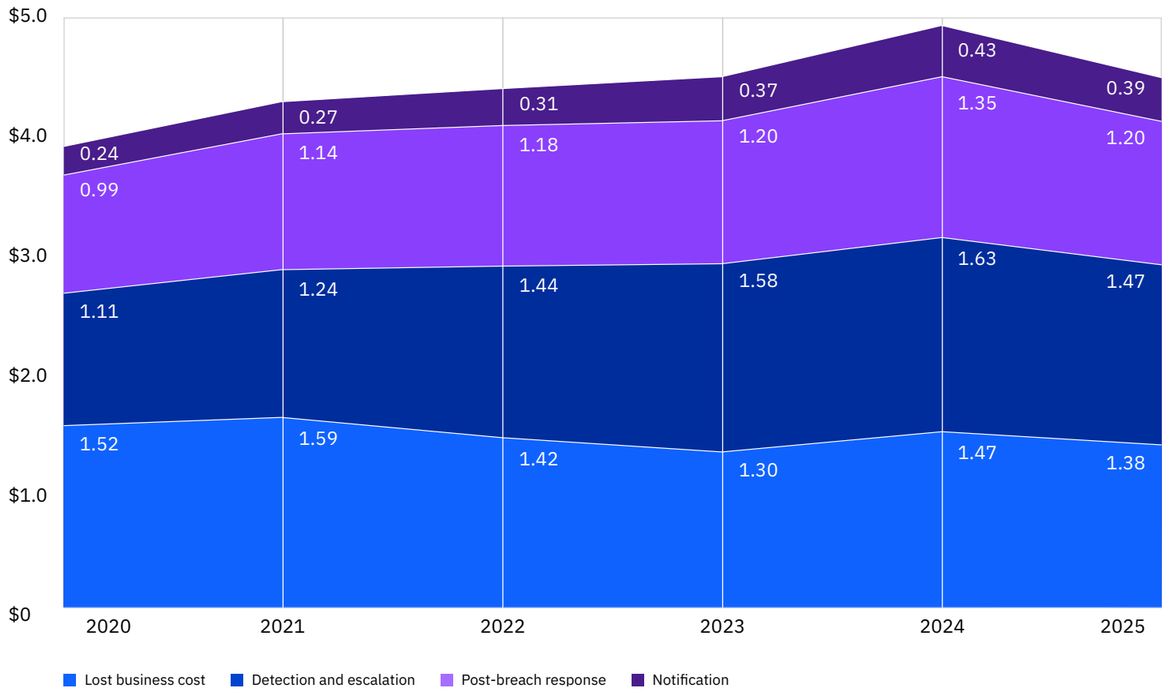
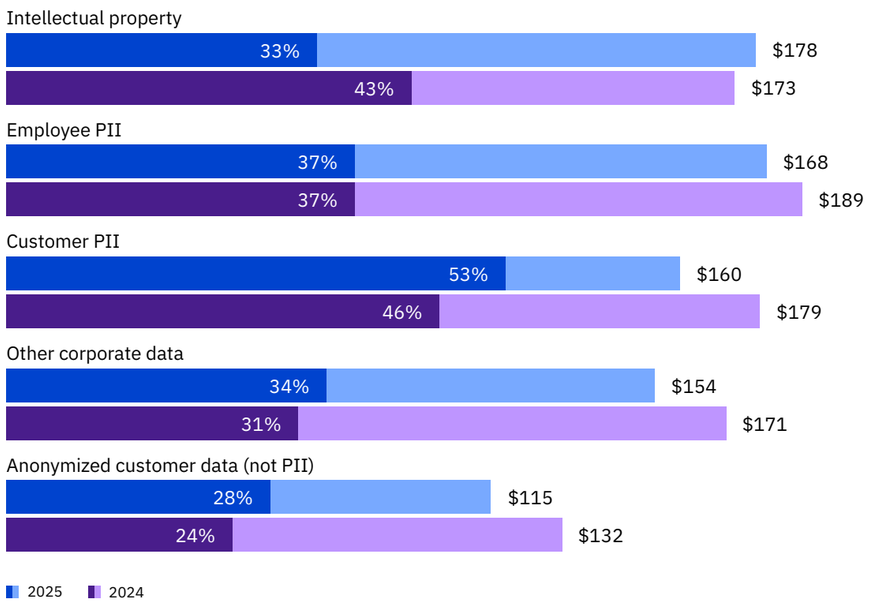


Figure 5.
Measured in USD millions



Detection and escalation costs plunged
Average costs for detection and escalation fell to USD 1.47 million, a nearly 10% drop from last year. These costs were the top decliners among four cost categories. Still, the other three categories—notification, ex-post response and lost business costs—also fell. Lost business, which includes revenue from system downtime, lost customers and reputation damage, dropped 6% after an 11% surge last year that helped drive total breach costs higher. See Figure 5.

Figure 6.
Measured in USD; more than one response permitted



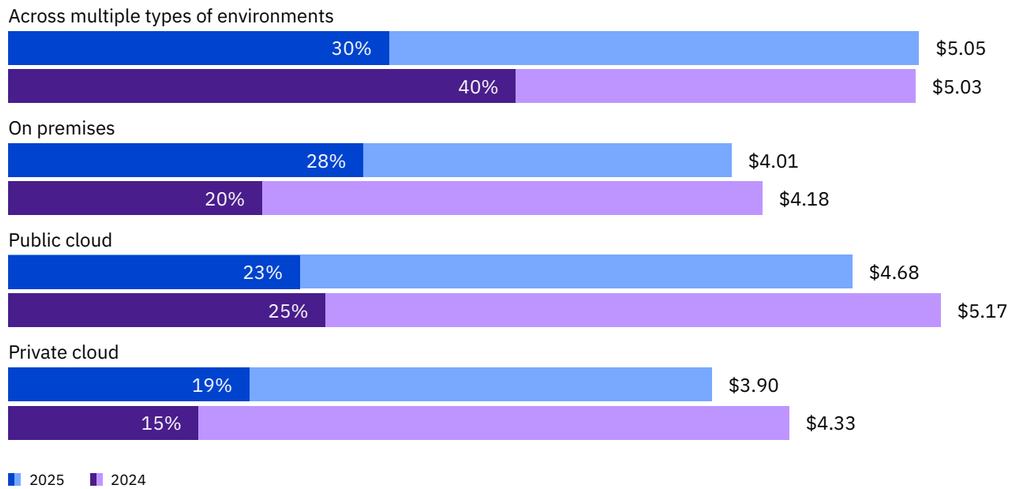
Most breaches targeted customer PII
Attackers targeted customer PII over other types of data by a wide margin. At 53%, it was the most stolen or compromised data type. Customer PII can include tax identity (ID) numbers, emails and home addresses, and can be used in identity theft and credit card fraud. On the other hand, company intellectual property (IP), while less commonly stolen or compromised, was the most costly (USD 178 per record). See Figure 6.

Data security

Data can be vulnerable wherever it's stored. Last year, most breaches involved data distributed across multiple environments, such as public clouds, private clouds and on premises. That finding remained true this year, but the share of those breaches fell, while the share of breaches involving data stored solely on premises grew. Meanwhile, the average costs associated with each location type was drastically different.

The effect of storage location on cost and frequency of a data breach
30% of all breaches involved data distributed across multiple environments, down from 40% last year. Meanwhile, breaches involving data stored on premises increased sharply to 28% from 20% last year. However, costs for each category differed. Data breaches involving multiple environments cost an average USD 5.05 million, while data breached on premises cost an average USD 4.01 million. See Figure 7.

Figure 7.
Measured in USD millions; more than one response permitted

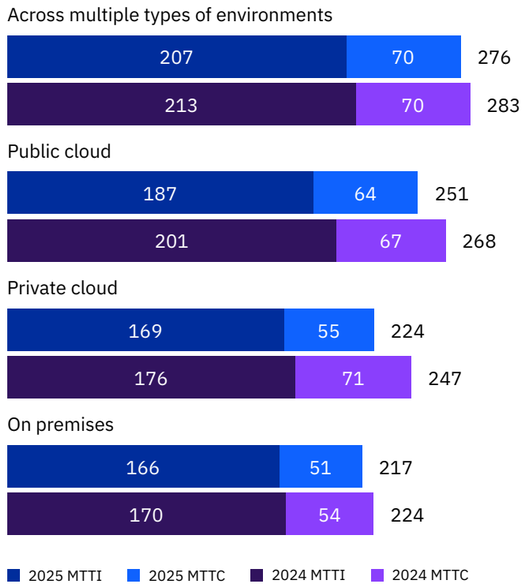


276

Days it took to identify and contain a data breach across various environments

Breaches of cross-environment data took longer to resolve
Breached data stored across multiple environments took the most time to identify and contain (276 days), the longest of the four storage locations. It reflects the increased complexity and uncertainty of such breaches. Compared to 2024, resolution times decreased for all categories. On-premises breaches were the quickest to resolve at 217 days. See Figure 8.

Figure 8.
Measured in days



Initial attack vectors and root causes

For the third year in a row, phishing was among the top attack vectors. Vendor and supply chain compromise followed closely behind, overtaking compromised credentials as the number two attack vector. All three vectors, which can be gained through malware, data breaches and credential stuffing, carried heavy costs for breached organizations. Our research also compared the average time to identify and contain those breaches, with supply chain compromise taking the longest to resolve.

Phishing topped initial attack vectors
Phishing replaced stolen credentials this year as the most common initial vector (16%) attackers used to gain access to systems. At an average USD 4.8 million per breach, it was also one of the costliest. Meanwhile, supply chain compromise surged to become the second most prevalent attack vector (15%), and second costliest (USD 4.91 million) after malicious insider threats (USD 4.91 million). See Figure 9.

Figure 9.
Measured in USD millions; percentage of all breaches

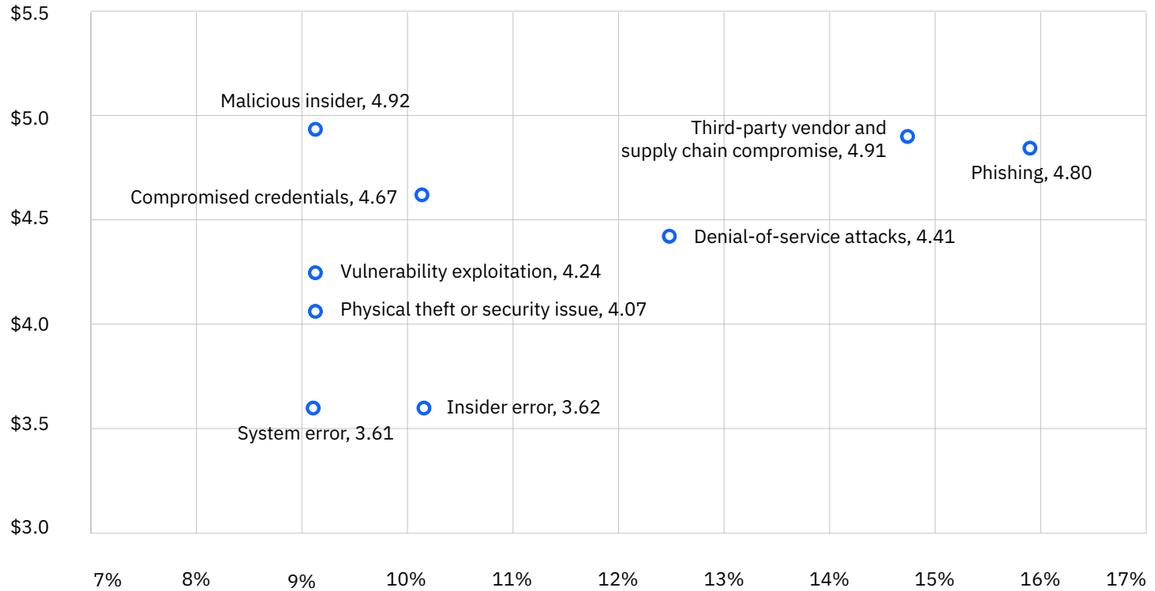


Figure 10.
Measured in days

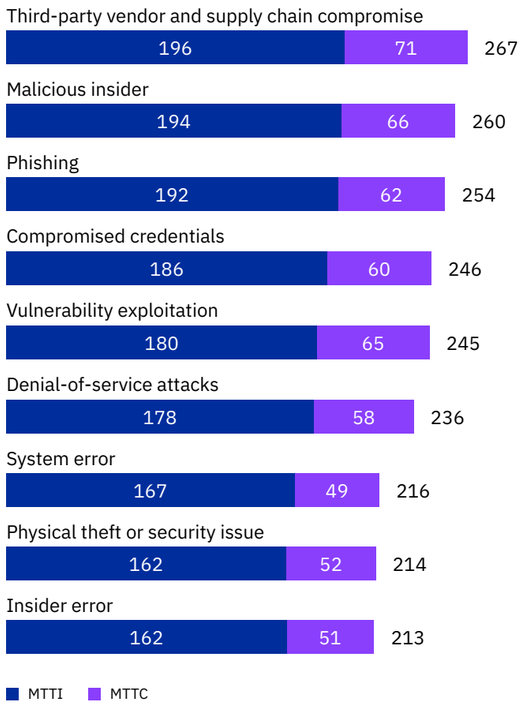
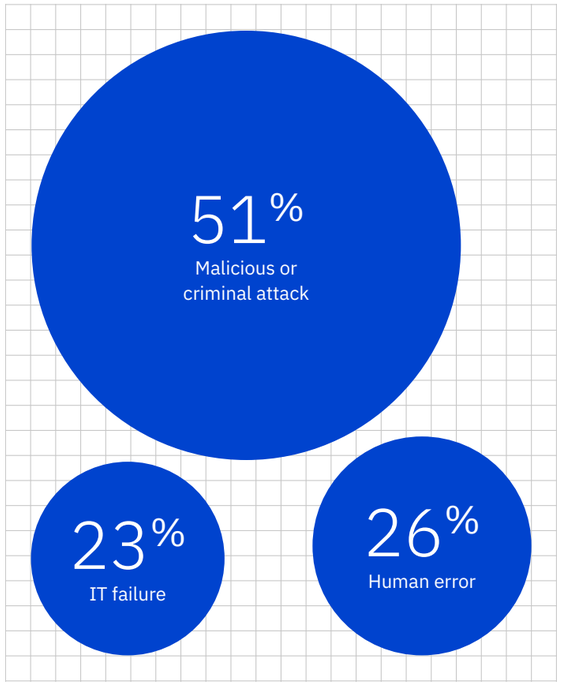


Figure 11.
Share of all breached organizations



Supply chain compromise took longest to resolve
Supply chain attacks are hard to detect because they exploit trust between vendor-and-customer and computer-to-computer communications. At a combined 267 days, they took the longest to detect and contain. Likewise, another trust-based attack, malicious insiders, took the second longest, with a combined 260 days to resolve. Compromised credentials, on the other hand, took the fourth longest to identify (186 days) but were less time-consuming to contain (60 days). See Figure 10.

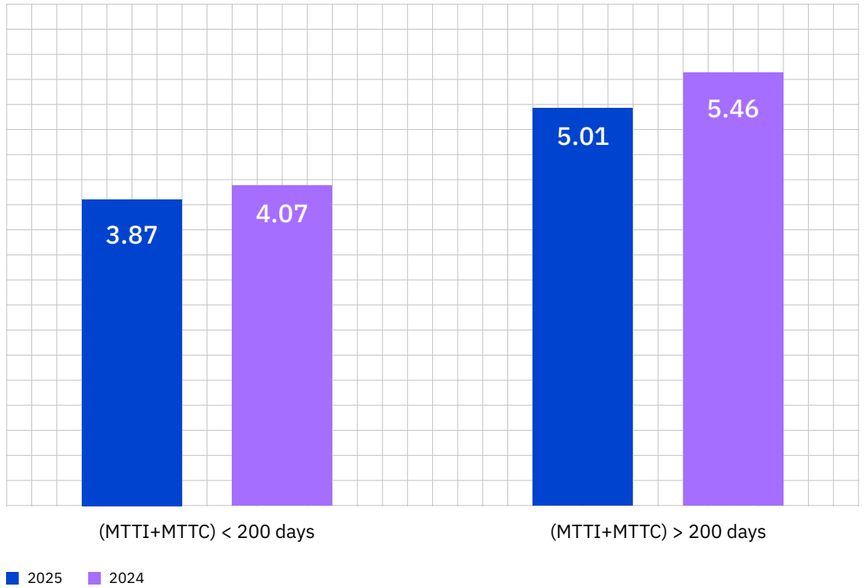
Malicious attacks dominate root cause of breaches
At 51%, malicious or criminal attacks, whether launched within or outside an organization, continue to dominate and occupy security teams. Human error and IT failure, which are preventable with robust employee training and proactive security measures, account for the rest, at 26% and 23% respectively. See Figure 11.

Data breach lifecycle

When an attacker breaches an organization, costs go up by the day. Each year, researchers analyze the average costs of the complete breach lifecycle—the total average number of days to identify and contain the breach—by breaking them into two categories: those that took less than 200 days and those that exceeded 200 days. While the costs for both categories rose in the previous two years, they declined this year. It was likely due to the lower costs of AI-driven and automation-driven detection and response.

Shorter breach lifecycles led to lower costs
Data breaches with a lifecycle under 200 days saw a drop in average costs, to USD 3.87 from USD 4.07 last year, a nearly 5% decline. Meanwhile, data breaches with a lifecycle exceeding 200 days had the highest average cost, at USD 5.01 million, compared to breaches with lifecycles under 200 days. It's nearly an 8% decrease from last year. See Figure 12.

Figure 12.
Measured in USD millions



Identifying the breach

Breach costs rise or fall depending on how they're identified: who detects them and when. This year, like last year, in-house security teams continued to increase the share of breaches they identified. Researchers looked at the prevalence of breach disclosures by outsiders, such as benign third parties, security researchers, law enforcement and consultants, and by the attackers themselves. They also examined the costs associated with each type of breach identification.

Security teams improved their breach identification
In the past two years, security teams and their tools have improved their performance in breach detection. This year, researchers found these teams and tools detected 50% of breaches, a vast leap over last year's tally of 42%, which was itself was a jump from 33% in 2023. Correspondingly, fewer breaches this year were identified by third parties and attackers. See Figure 13.

Figure 13.
Only one response permitted

Breaches identified by internal security teams cost less
By detecting a breach first—before third parties or attacker disclosure—security teams can move fast and limit potential damage. When security teams identified a breach, the average cost was USD 4.18 million, down from USD 4.55 million last year. By comparison, when the attacker disclosed the breach, and presumably had more time to do damage and steal or compromise data, the average cost was far greater (USD 5.08 million). However, that cost decreased from last year (USD 5.5 million). See Figure 14.

Figure 14.
Measured in USD millions

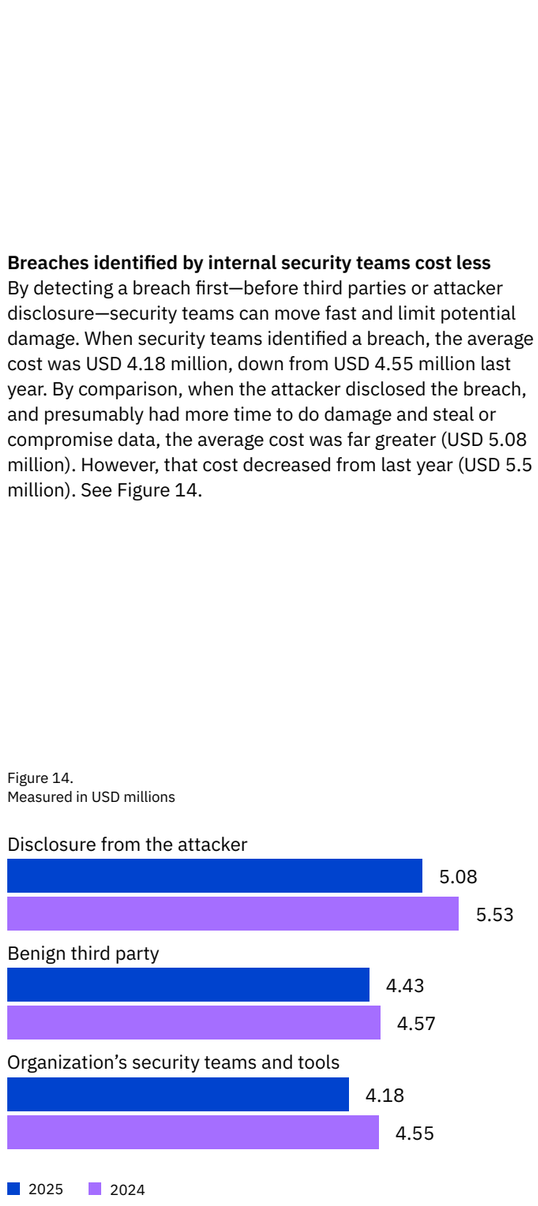
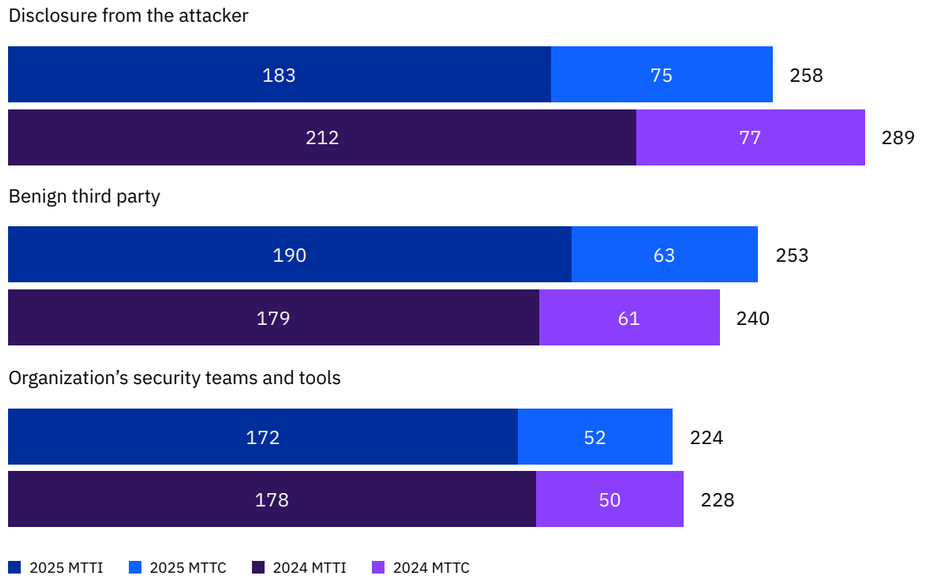


Figure 15.
Measured in days



Faster breach identification and containment
Not only did internal security teams identify more breaches, they did it in record time: 172 days, six days faster than last year. They also contained those breaches two days faster. The use of AI and automation is likely contributing to this acceleration, as the next section in the report shows. See Figure 15.

Recovery time

Recovery from a breach can continue after containment. In this study, recovery means:

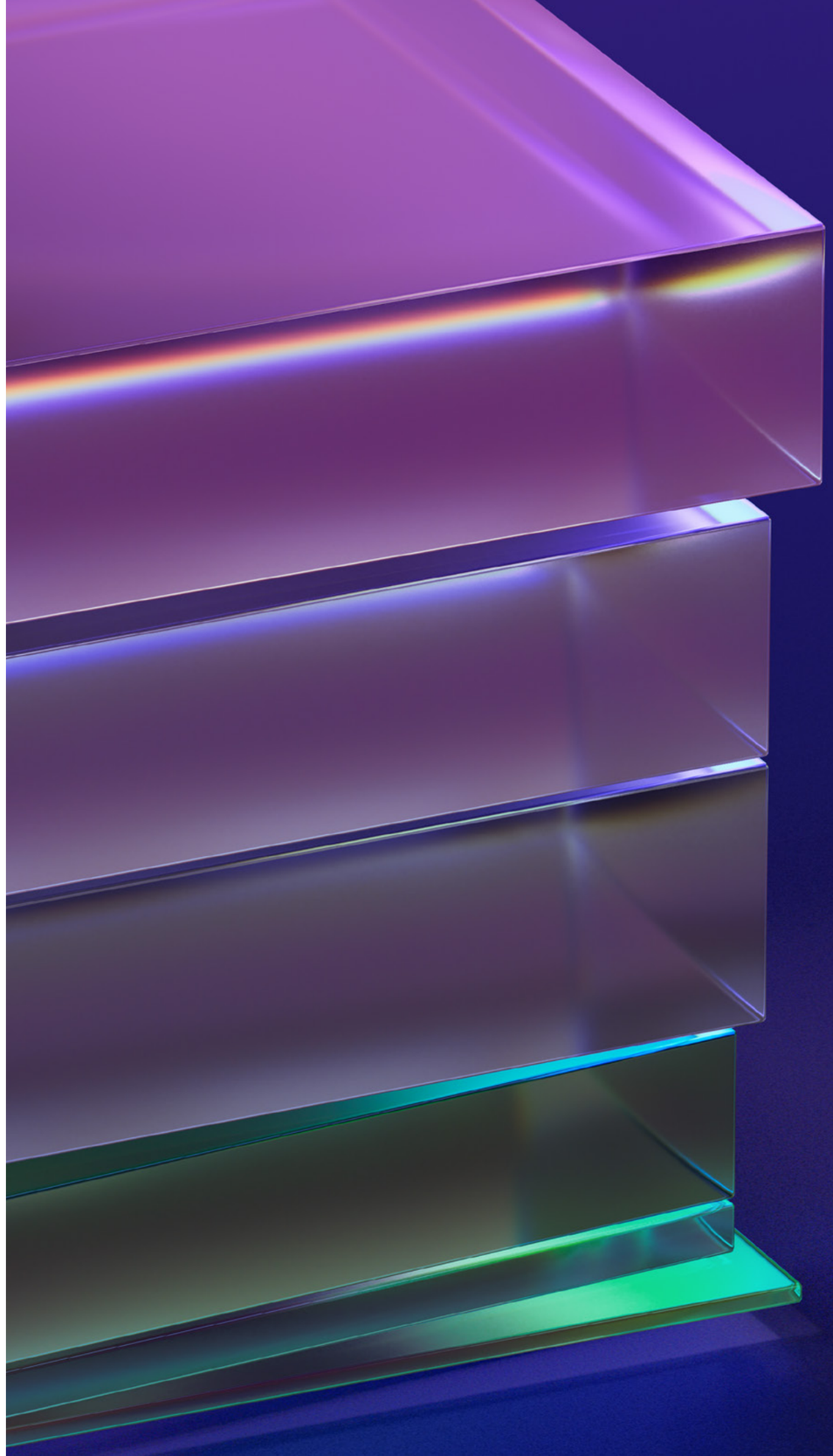
- Business operations are back to normal in areas affected by the breach.
- Organizations have met compliance obligations, such as paying fines.
- Customer confidence and employee trust have been restored.
- Organizations have put controls, technologies and expertise in place to avoid future data breaches.

Much of this work, such as re-establishing customer confidence, involves factors beyond technology. Despite progress compared to 2024, only a minority of organizations reported complete recovery. For most organizations, the hard work of recovery can take months or even years.

Breach recovery rates improved
Most organizations in this year's survey (65%) said they were still recovering from the data breach. However, 35% said they had fully recovered, nearly tripling the response from last year (12%). This improvement coincided with a nine-year low for faster identification and containment of breaches.

65%

Share of organizations that have not fully recovered from a data breach



Recovery typically took more than 100 days

Among the organizations that had fully recovered, 76% said the recovery took longer than 100 days. Roughly a quarter (26%) said recovery took more than 150 days. Only 2% said recovery was possible within as little as 50 days.
See Figure 16.

Figure 16.
From organizations that reported fully recovering from a data breach; measured in days

26%
>150 days

24%
126 – 150 days

26%
101 – 125 days

17%
76 – 100 days

5%
51 – 75 days

2%
< 50 days

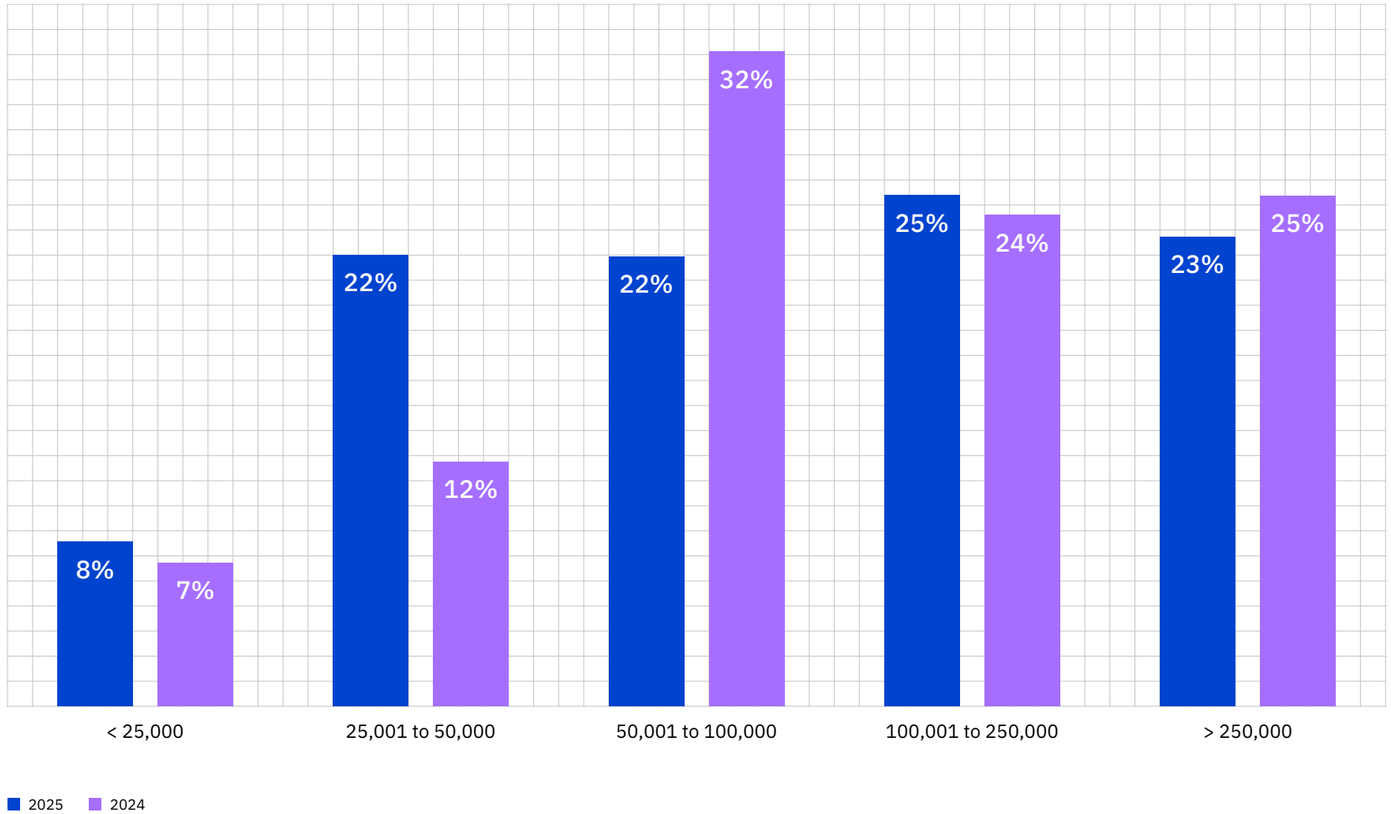
Regulatory fines

Reporting a breach to regulators and other government agencies has become a common part of post-breach responses. This year's report found a third of organizations paid a regulatory fine because of breaches. The study looked at the size of fines, which varied across countries and regions. Organizations in the United States paid the highest fines, which, in turn, drove up total United States breach costs.

32%

Share of data breaches that resulted in fines

Figure 17.
Among those organizations that experienced fines; measured in USD



Distribution of regulatory fine costs
The share of organizations that paid fines after a breach remained the same as last year, about one third. A total of 48% of those fines were above USD 100,000. However, the distribution of fine costs grew in some categories and shrank in others. For instance, the share that paid a fine of up to USD 50,000 grew by 45% while those that paid USD 50,001 to USD 100,000 decreased by 31%. Organizations that paid over USD 250,000 remained approximately the same.
See Figure 17.

Breaches involving AI

Security for AI is lacking. This year's report quantifies the extent to which attackers are taking advantage of this deficiency and successfully targeting AI models and applications. While the share of breaches involving AI security incidents are small, IBM researchers expect them to grow as AI vendors gain greater market share and penetration into enterprise systems. Shadow AI is of particular concern. As AI becomes integral to operations, AI security incidents have the potential to disrupt a range of business activities, including compromising sensitive data.

97%

Share of organizations that had an AI-related security incident to their models or applications and had lacked proper AI access controls

Security incidents involving AI

AI models and applications are emerging as an attack surface, especially in cases of shadow AI. This year, 13% of organizations reported a security incident on an AI model or application that resulted in a breach. But 97% of those breached organizations said they lacked proper AI access controls. An additional 8% of breached organizations were unsure if their breach involved an AI security incident.
See Figure 18.

Figure 18.
From organizations that reported a security incident on an AI model or application

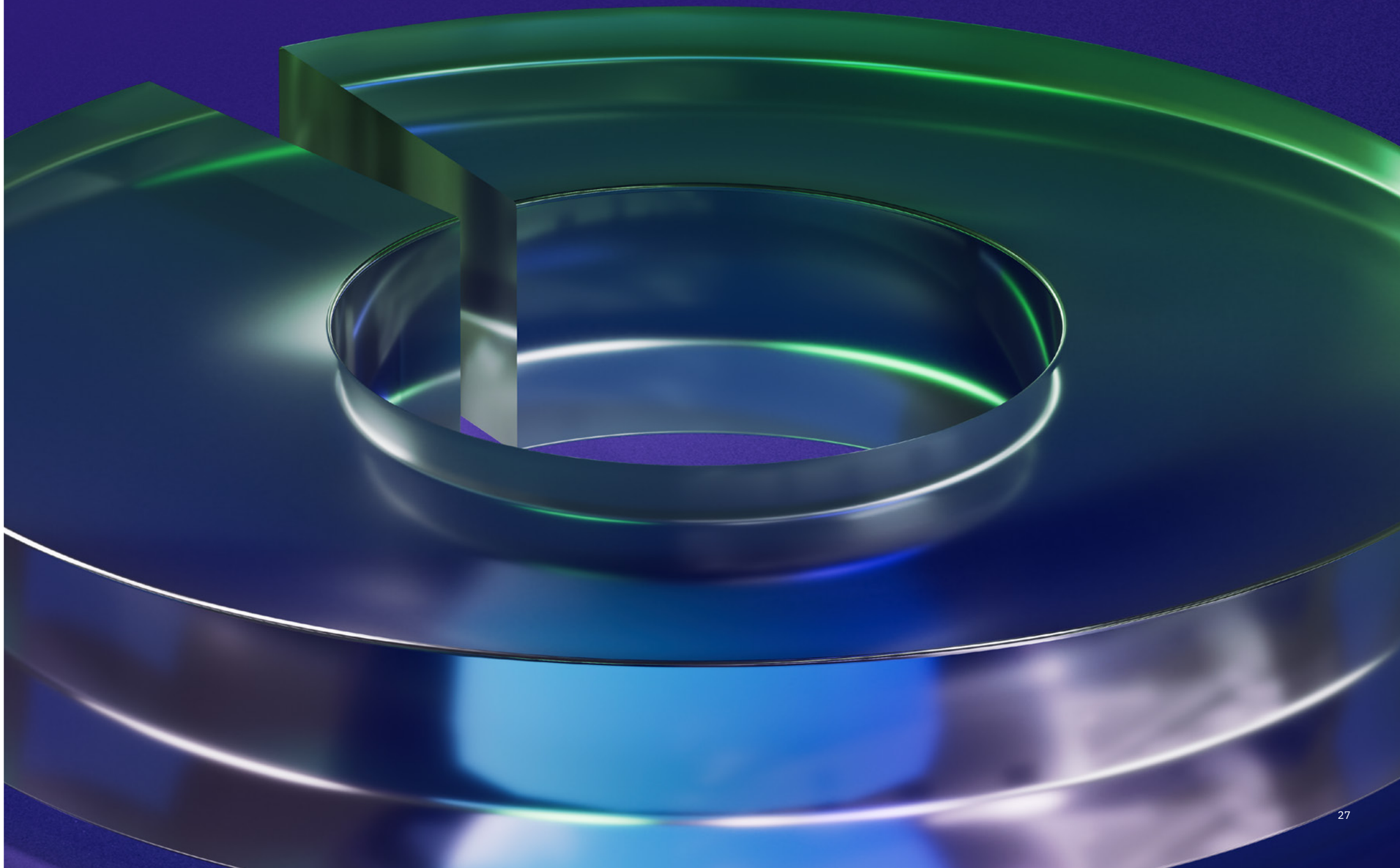
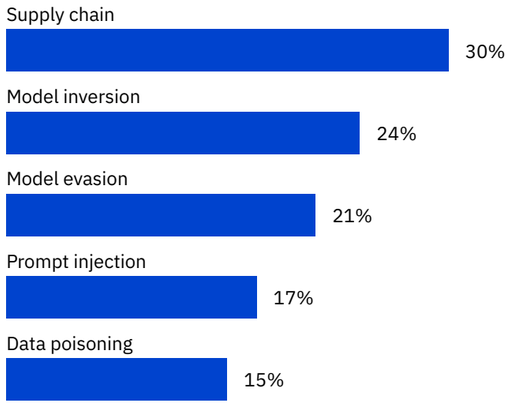
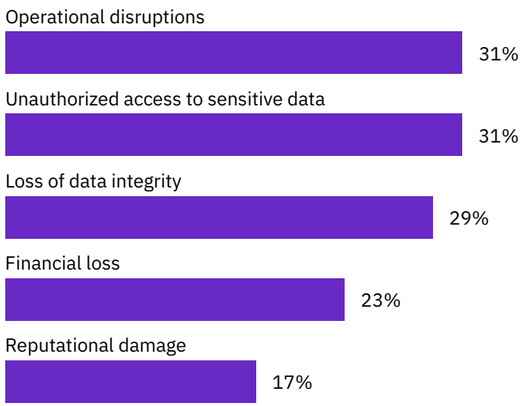


Figure 19.
From organizations that reported a security incident involving an AI model or application; more than one response permitted



Supply chain compromise was the most common cause of AI security incidents
Security incidents involving AI models and applications were varied, but one type clearly claimed the top ranking: supply chain compromise (30%), which includes compromised apps, APIs and plug-ins. Following supply chain compromise were model inversions (24%) and model evasions (21%). Incidents involving prompt injections and data poisonings made up 17% and 15% of cases respectively. See Figure 19.

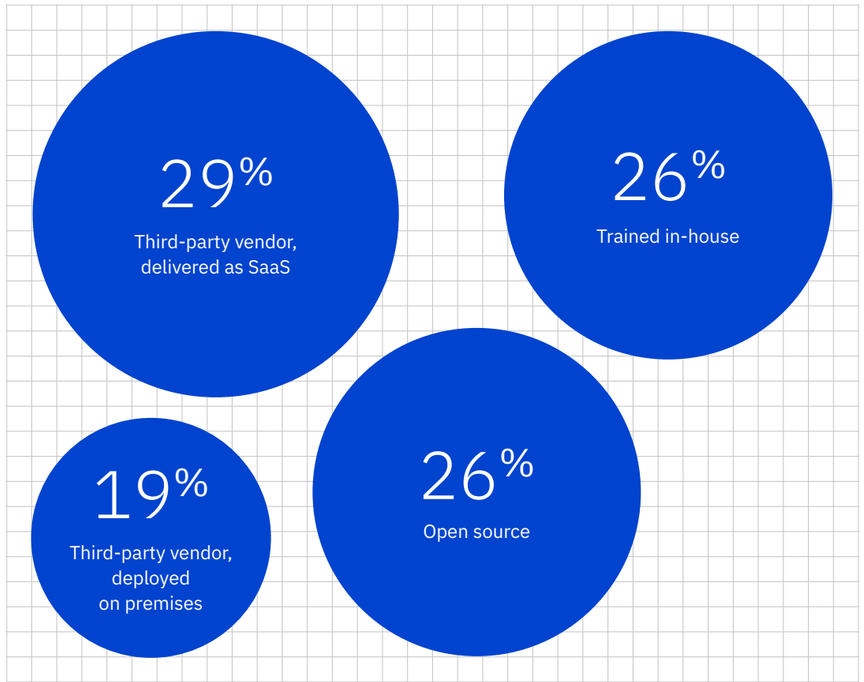
Figure 20.
From organizations that reported a security incident involving an AI model or application; more than one response permitted



Impacts of security incidents on authorized AI
Approximately one-third (31%) of organizations that experienced a security incident involving authorized AI suffered operational disruption and saw attackers gain unauthorized access to sensitive data. 29% of organizations reported a loss of data integrity. The impact of reputational damage (17%) underscores the potential long-tailed effects of these incidents.
See Figure 20.

Most AI security incidents came from AI delivered as software as a service (SaaS)
From a security and governance standpoint, where an AI model or application comes from matters. The majority of organizations that reported a security incident involving AI said the source was a third-party vendor and delivered as SaaS (29%). There were fewer incidents involving AI from third-party vendors that were deployed on premises (19%). However, the risks to in-house and open-source models—at 26%—were a close second to the AI delivered by SaaS. See Figure 21.

Figure 21.
From organizations that experienced a security incident involving an AI model or application



Unsanctioned AI security incidents were more common than sanctioned AI
Shadow AI may go undetected by an organization, and attackers can exploit its vulnerabilities when employees use it. Security incidents involving shadow AI accounted for 20% of breaches, which is 7 percentage points higher than those security incidents involving sanctioned AI. A further 11% of breached organizations were unsure if they experienced a shadow AI incident.
See Figure 22.

Figure 22.
Has your organization experienced a security incident involving shadow AI?

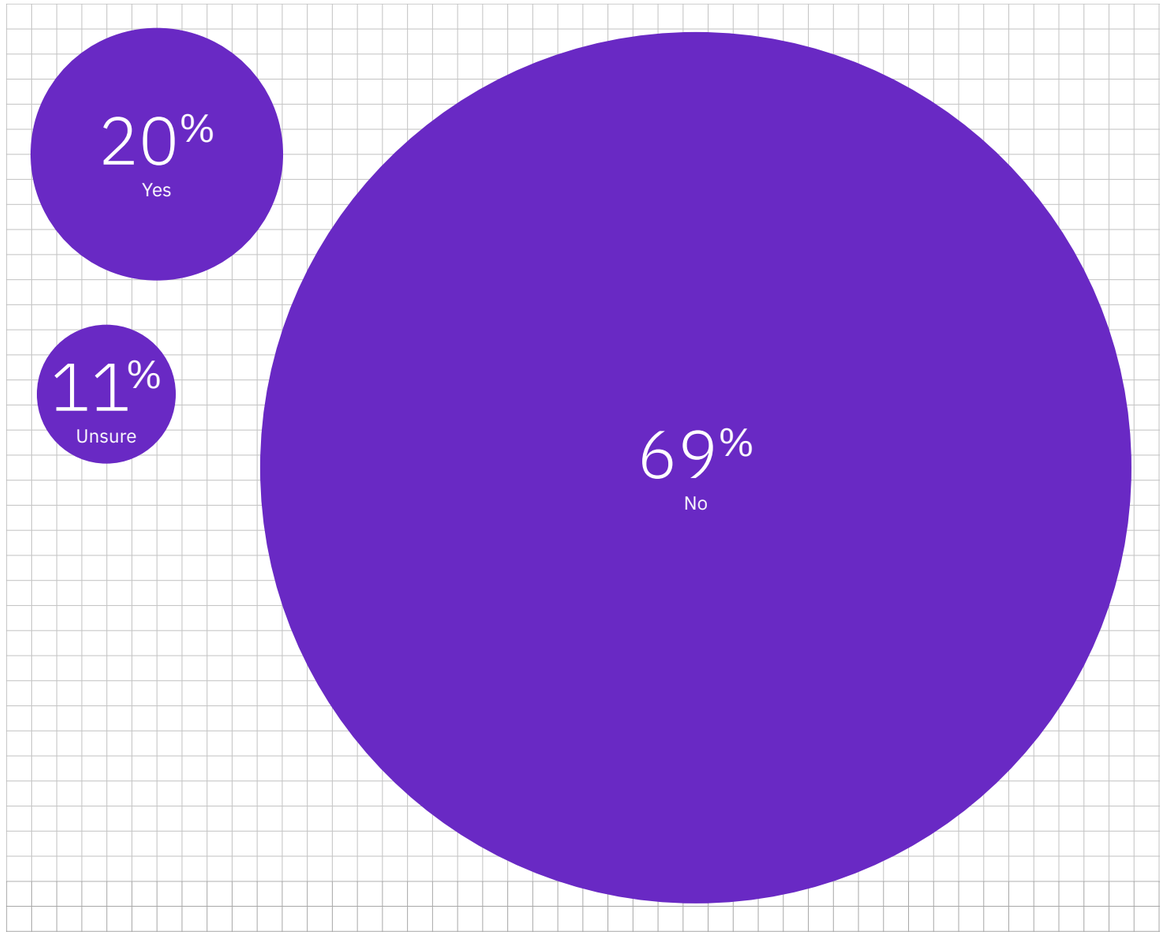


Figure 23.
Percentage of breaches involving shadow AI; only one response permitted

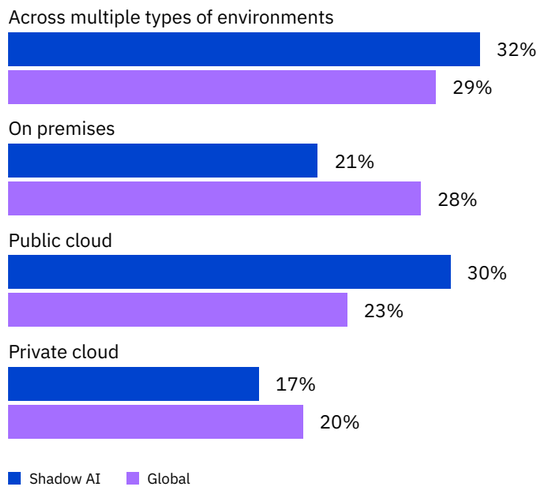
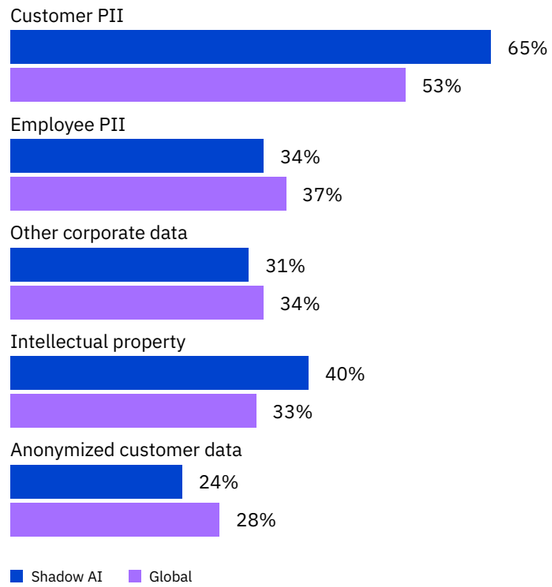


Figure 24.
Percentage of breaches involving shadow AI; more than one response permitted



Data stored across environments was the most breached in shadow AI incidents
Organizations that suffered a shadow AI security incident reported the breached data was most often stored across multiple environments and a public cloud (62%). See Figure 23.

Customer PII was the most common data compromised in shadow AI incidents
One of the most valuable types of data for attackers to target is customer PII. It can be used for financial and insurance fraud or for sale on the dark web. Likely because of those reasons, customer PII was the most compromised data type (65%). That figure is notably higher than the overall global share of PII reported compromised in this year's report (53%).
See Figure 24.

Customer PII was the most valuable record type compromised in a shadow AI incident
In addition to being the most compromised record type in a shadow AI security incident, customer PII was also the most expensive at USD 166 per record. That figure was slightly above the overall global average for this record type at USD 160. The cost of other record types was slightly lower in these security incidents than the overall global average. See Figure 25.

Internal security teams identified more shadow AI security incidents than did third parties
Organizations' security teams and tools identified most AI security incidents (57%), which was better than they did for overall breach discoveries (50%). Meanwhile, the share of AI security incidents attackers disclosed (12%) was lower than the overall global breach disclosure (19%). See Figure 26.

USD
200K
Added cost of a breach involving shadow AI

Shadow AI security incidents cost more
Security incidents involving shadow AI carried an added cost. They contributed USD 200,000 to the global average breach cost. This higher cost was likely driven by longer detection and containment times for these security incidents, approximately a week longer than the global average. See Figure 27.

Figure 25.
Measured in USD; more than one response permitted

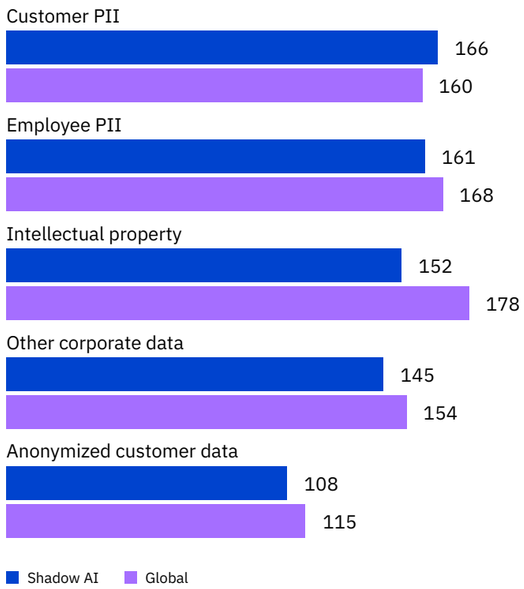


Figure 26.
Identification of breaches involving shadow AI

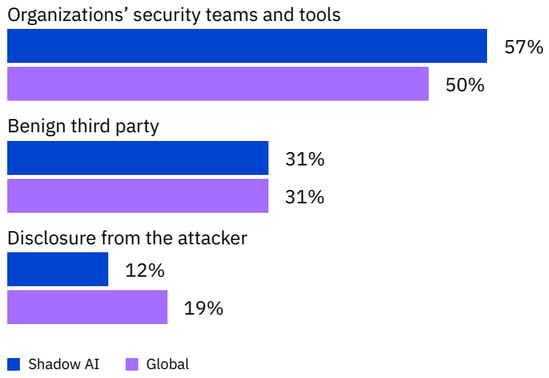
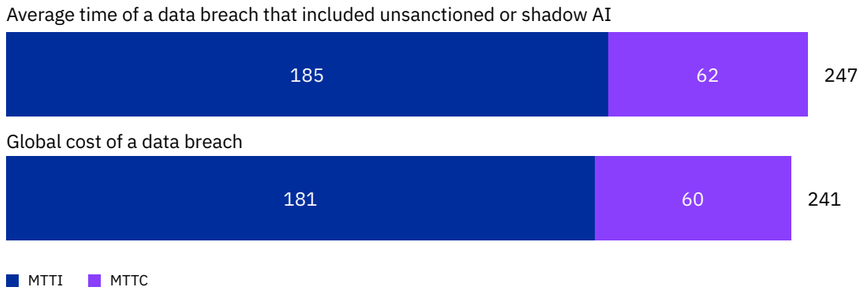


Figure 27.
Measured in days



AI governance

AI adoption has outpaced oversight. This year's research quantifies that governance gap and the costs it carries. Most organizations said they didn't have governance policies to mitigate or manage the risk to AI. For those that do, less than half have strict approvals for AI deployments. That deficiency had consequences. Not only do these organizations leave themselves open to security, operational and reputational risks, but they've paid a steeper cost than average when breached.

63%

Share of organizations that lacked AI governance policies

Most organizations lacked governance to manage AI or detect shadow AI

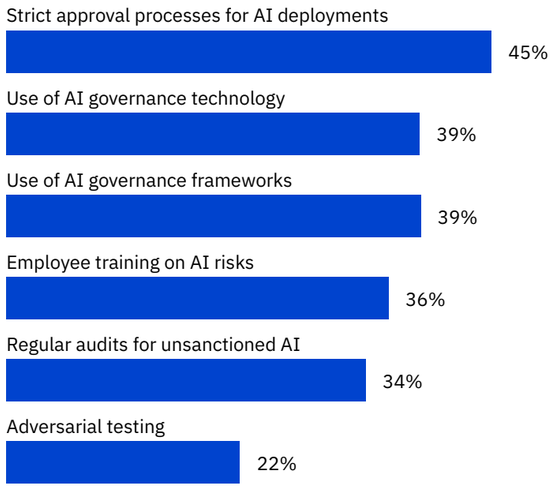
Oversight of AI—and the ability for IT and security teams to identify shadow AI—is essential for organizations to ensure the ethical, legal and responsible development and use of AI among employees. However, nearly two-thirds of organizations (63%) said they don't have governance policies in place to manage AI or detect shadow AI. See Figure 28.

Figure 28.
From all organizations

37%

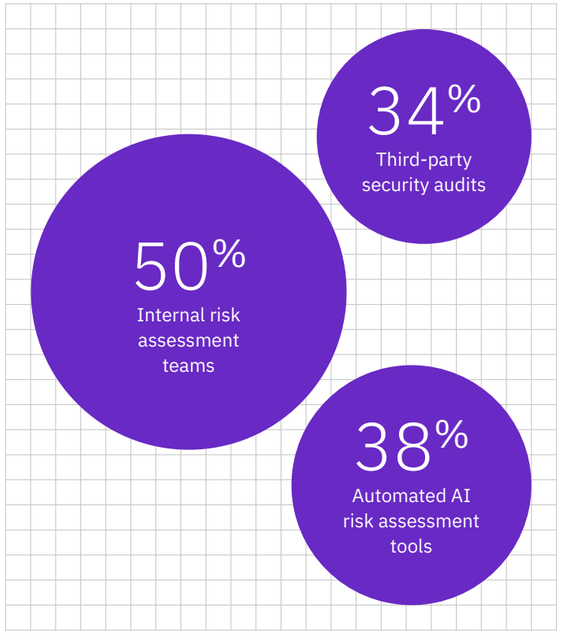
Share of organizations that had AI governance policies in place

Figure 29.
From organizations that had AI governance policies in place; more than one response permitted



Approval processes for AI were the top type of governance policy
AI governance technology, frameworks and employee training all play important roles in ensuring trustworthy and ethical AI. Among the 37% minority of organizations that had AI governance policies, these three areas had a nearly equal share of approximately one-third. But the most common AI governance policy reported among this group was strict approval procedures for AI deployments (45%). See Figure 29.

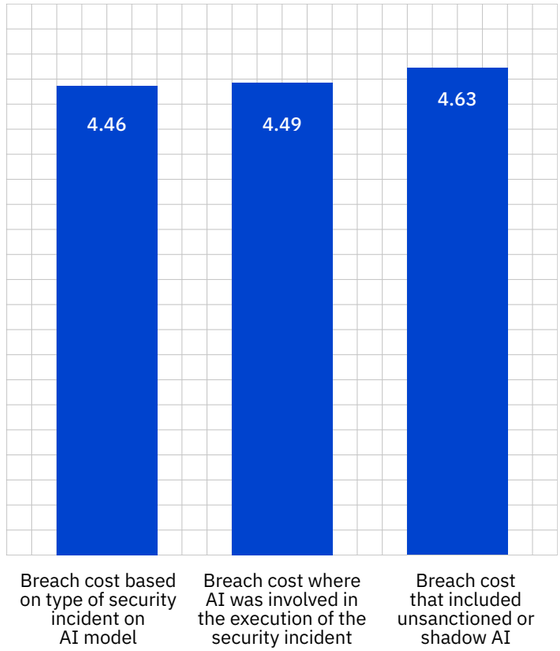
Figure 30.
From organizations that had AI governance policies in place; more than one response permitted



Half of all AI model evasion assessments come from internal teams
AI model evasion attacks—which attempt to make the AI model misbehave by manipulating data inputs—are relatively rare, but they carry a heavy risk. Researchers have previously shown these attacks can lead to financial loss, reputational damage and even endanger lives in critical applications, such as autonomous vehicles and medical diagnosis. This report found four out of five organizations have processes in place to assess the risk of these attacks, and half use internal risk assessment teams to do so. A further 38% use automated risk assessment tools, while 34% rely on third-party security audits. See Figure 30.

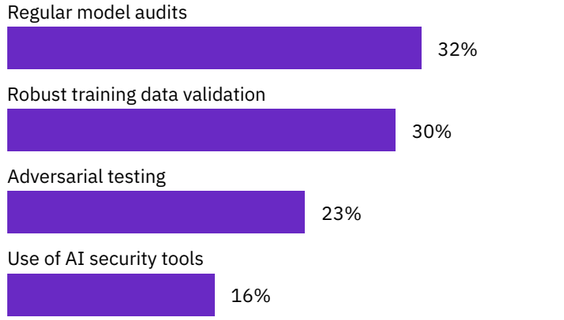
Effect of AI on data breach costs
Whether an attacker used AI against an organization—through phishing, for example—or targeted the organization's AI, the average cost of the breach was similar (USD 4.49 million and USD 4.46 million, respectively). However, if the breach involved a security incident with shadow AI, the average cost was higher (USD 4.63 million). See Figure 31.

Figure 31.
Measured in USD millions



Most organizations have no governance in place to mitigate AI risk
87% of organizations said they have no governance policies or processes to mitigate AI risk. Nearly two-thirds of breached organizations didn't perform regular audits on their AI models to mitigate risk. And over three-quarters reported not performing adversarial testing on their AI models. See Figure 32.

Figure 32.
Percentage of breaches involving an AI model; more than one response permitted



AI-driven attacks

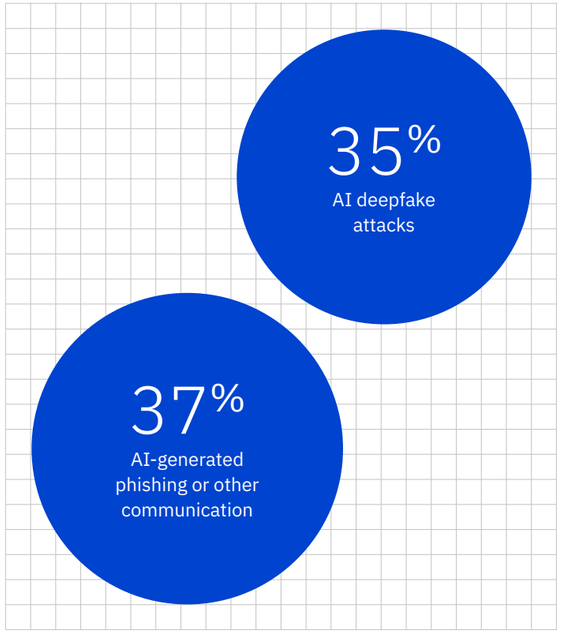
Attackers are using gen AI to improve and scale their creative writing and image generation. By crafting highly personalized emails, voices and videos mimicking real people or brands, attackers can make their fake appeals harder to detect. For the first time, this report's research analyzed the prevalence of those AI-driven attacks.

Attackers are using AI to manipulate humans
Researchers found 16% of breaches involved attackers using AI. Most of these breaches focused on human manipulation through phishing (37%) or deepfake attacks (35%). See Figure 33.

16%

Share of breaches that involved attackers using AI

Figure 33.
Types and percentages of AI-driven attacks used on organizations that experienced a breach

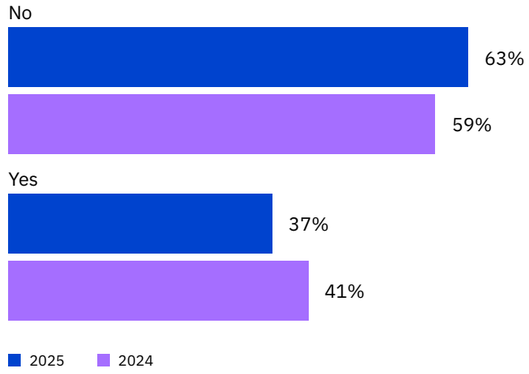


Ransomware attacks

Ransomware fatigue appears to be growing. More organizations are opting not to pay the ransom demands, even as the cost of an extortion or ransomware incident remains high. Also, more organizations are deciding against involving law enforcement, even as researchers found last year that calling in law enforcement dramatically reduced the global average cost of a breach.

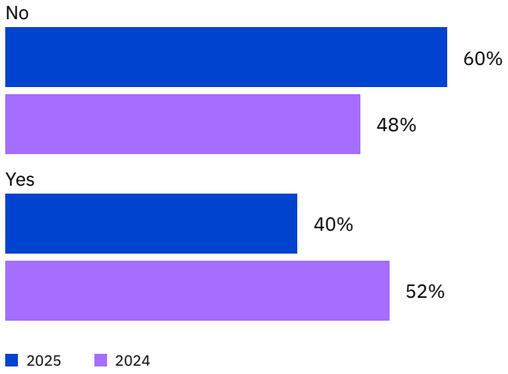
Nearly two-thirds of ransomware victims refused to pay the ransom
Organizations pushed back against ransom demands, with more opting not to pay (63%) compared to the previous year (59%). However, even though more organizations refuse to pay ransom demands, the average cost of an extortion or ransomware incident remained high, particularly when disclosed by an attacker. See Figure 34.

Figure 34.
If your organization was hit with a ransomware attack, did your organization pay the ransom?



Fewer organizations involved law enforcement
Last year, organizations saw an average cost savings of USD 1 million when they involved law enforcement in ransomware attacks. However, they didn't see—or realize—that benefit this year: the share of organizations that involved law enforcement fell to 40%, down from 52% in 2024. See Figure 35.

Figure 35.
Was law enforcement contacted and involved following the ransomware attack?



Raising prices post-breach

By nature, data breaches are costly. Organizations looking to recover those costs might choose to pass them on to customers. However, in price-sensitive markets or moments, that strategy may backfire. In this year's report, compiled during a period when inflation was—and is—top of mind for many consumers, organizations appeared less likely than before to pass along breach costs in the form of price hikes.

Fewer organizations plan to pass breach costs to customers
The share of organizations that said they would pass breach costs on to customers fell by nearly a third to 45% in this year's report, down from 63% last year. However, approximately a third said they would hike prices more than 15%. See Figures 36 and 37.

Figure 36.
Did the data breach result in your organization increasing the cost of its services and products?

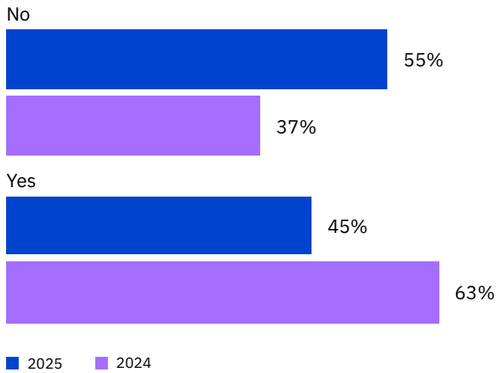
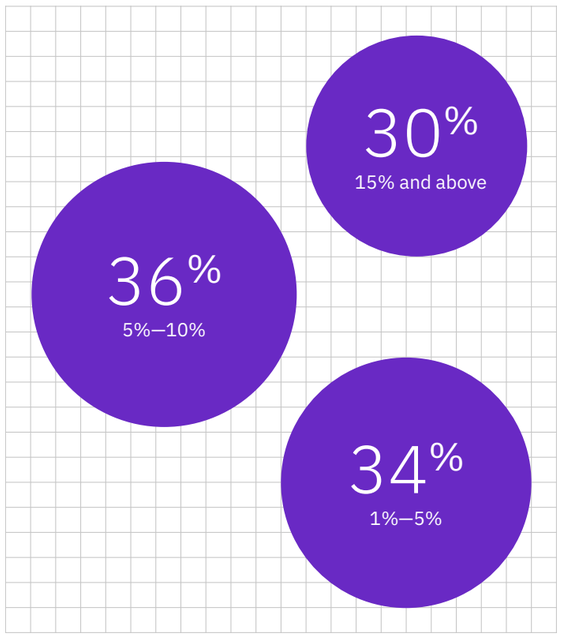


Figure 37.
If yes, by what percent were costs increased?



Business disruption

Breaches can happen in seconds, but the ripple effect can last for months or even years. As a result, most breached organizations in this year's report suffered operational disruption. The growth of AI complicates this picture further by expanding and introducing new and potentially fragile interdependent and interconnected systems that are linked to operational activities.

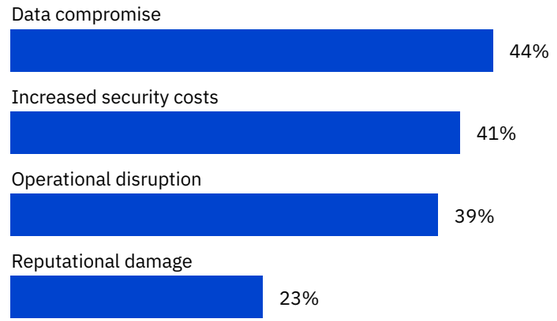
A majority of data breaches disrupted operations
Data breaches can disrupt the ability of organizations to process sales orders, provide customer services and keep their production lines running. This year's report found 86% of organizations experienced this sort of operational disruption.

86%

Share of businesses that experienced a disruption due to a data breach

Impacts of security incidents involving shadow AI
Among organizations that experienced a security incident involving shadow AI, 44% suffered data compromise. Another 41% reported increased security costs as a result of those incidents. Operational disruption was more widespread than incidents involving authorized AI. These results suggest shadow AI incidents have an outsized impact on downstream breach issues that extend beyond data security. See Figure 38.

Figure 38.
Impact of a shadow AI incident; more than one response permitted



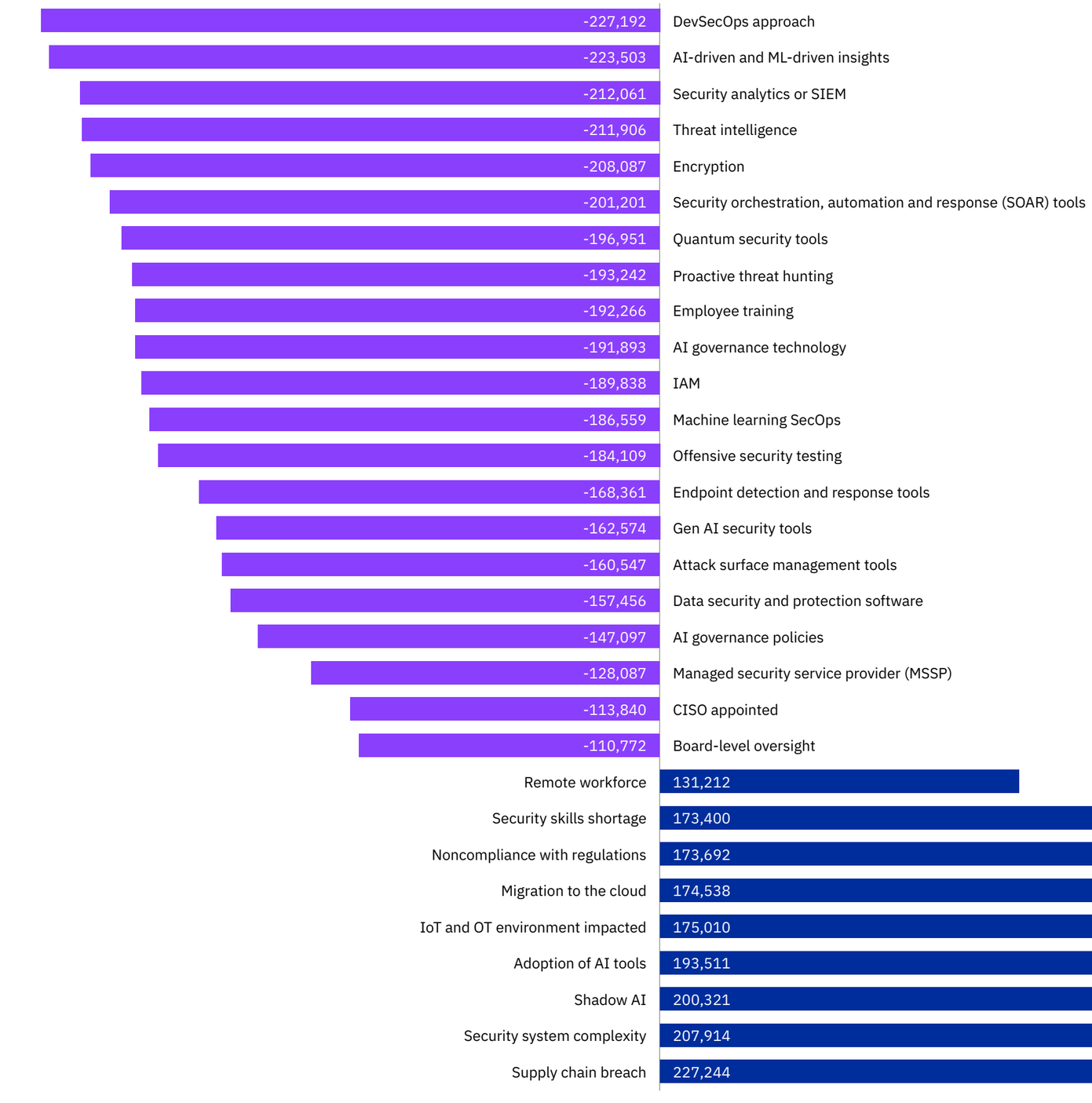
Factors that increase or decrease breach costs

When analyzing breach costs, it's important security leaders understand which technologies or events tend to lower or raise those costs. One constant we've found year over year: security AI and automation lowers costs. This year we also found the use of shadow AI raises costs. Our analysis examined 30 contributing factors and the impact of each in isolation against the global average. Also included are the top three factors found to amplify or mitigate the average data breach cost.

Key factors that reduced costs
Taking a DevSecOps approach to software development was the number one factor that reduced breach costs in this year's report. The use of AI and machine-learning insights, as well as having a security information and event management (SIEM) platform for detecting and responding to threats, rounded out the top three cost-reducing factors. All three of these security approaches center around and strengthen insight, intelligence and coordination. See Figure 39.

Key factors that increased costs
Security system complexity and supply chain breaches continue to challenge security teams and add to the average cost of a data breach. Both involve systems, networks and workflows with potential blind spots that can lead to vulnerability. The new addition to this year's top three costliest factors is shadow AI. Its presence within an organization is an added blind spot, another attack surface that is hard to police. As we've shown elsewhere in this report, organizations often don't look for shadow AI, so it remains undetected. See Figure 39.

Figure 39.
Cost difference from USD 4.88M breach average; measured in USD

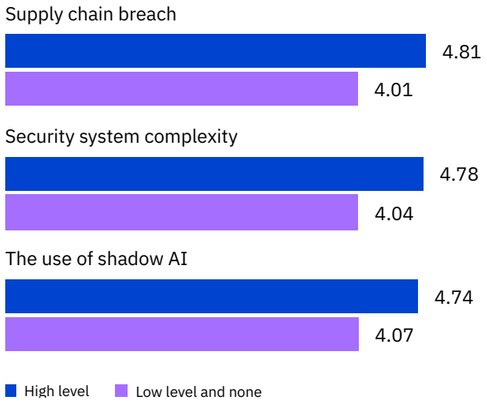


670K

Added cost of a breach, in USD, for organizations with high levels of shadow AI versus those that had low levels or none

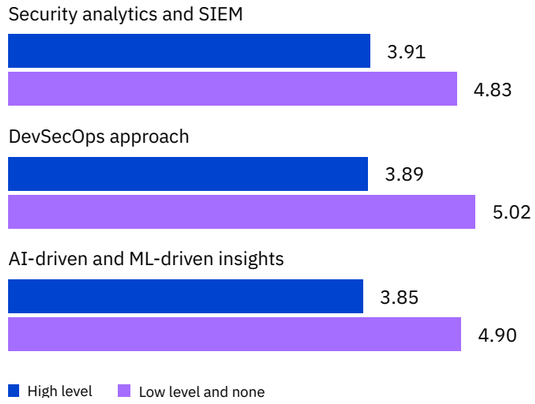
High levels of shadow AI drove up costs
When organizations used a high level of shadow AI, their average breach costs were USD 4.74 million, which is USD 670,000 higher than organizations that had a low level or no shadow AI (USD 4.07 million). Similar disparities were seen with the other two key cost amplifying factors. See Figure 40.

Figure 40.
Measured in USD millions



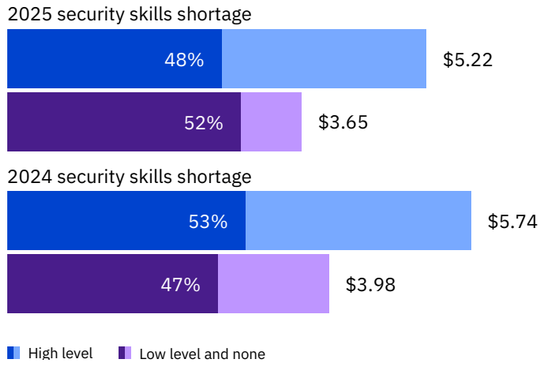
High versus low levels of key cost mitigating factors
When organizations used AI or machine-learning insights in their security, their average breach costs were USD 3.85 million, compared to USD 4.9 million for organizations that used these technologies at a low level or not at all. For the other two cost mitigating factors, DevSecOps created a similar difference, while SIEM created slightly less of a difference, at USD 3.91 million versus USD 4.83 million. See Figure 41.

Figure 41.
Measured in USD millions



Security skills shortages remain costly
The cybersecurity skills shortage has challenged the industry for years. This year's report found 48% of organizations had a high level of security skills shortage, down from 53% last year. However, those high skills shortages continue to exert pressure, equating to USD 5.22 million in average breach costs compared to USD 3.65 million for organizations that had a low level or no skills shortage. See Figure 42.

Figure 42.
Measured in USD millions

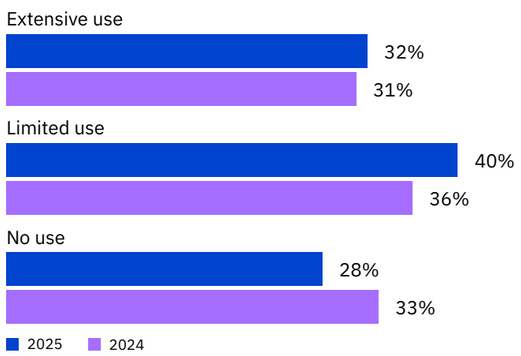


Security AI and automation

AI and automation play an increasingly crucial role in security, providing defenders with speed and scale. Both are necessary for securing organizations and detecting and responding to AI-driven threats from attackers. Since AI tools act as a skills multiplier, security teams can oversee more systems and react quickly to possible threats. While this year's report found these technologies accelerated the work of identifying and containing breaches and reducing costs, adoption rates appear to be uneven.

Extensive AI and automation use remained constant
The share of organizations that used security AI and automation extensively ticked up slightly to 32% in this year's report compared to 31% last year. Organizations that used these tools in a limited way rose to 40% from 36%. Although that increase is just a four-percentage-point difference, it represents an 11% increase in use. Correspondingly, those claiming no use dropped to 28% in this year's report from 33% last year. See Figure 43.

Figure 43.
Percentage of organizations per usage level



More AI and automation equaled lower breach costs

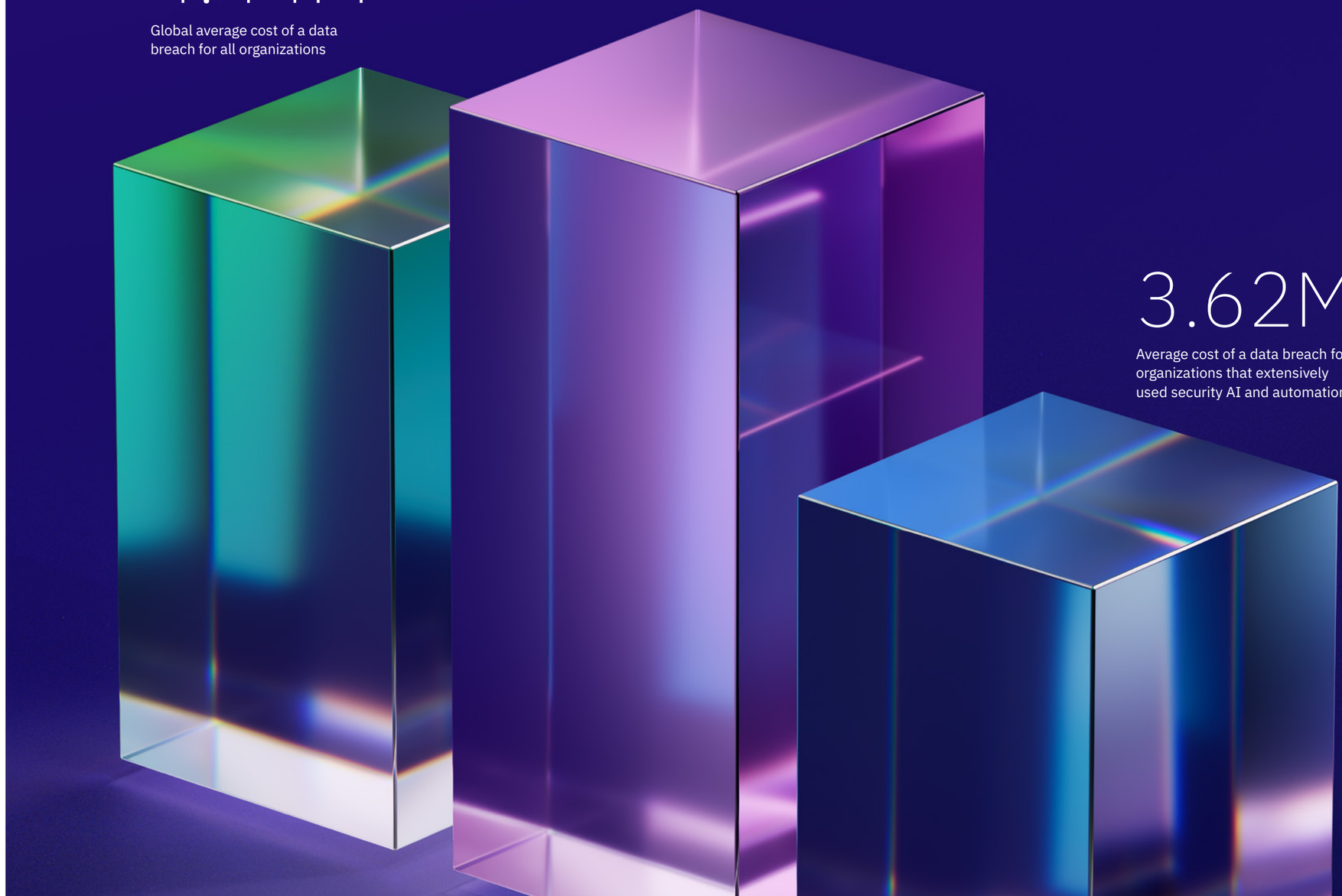
Security AI and automation continue to drive down breach costs. This correlation was noted last year and gained momentum this year. Organizations that didn't use AI or automation had an average breach cost of USD 5.52 million, while those that used these technologies extensively had an average breach cost of USD 3.62 million. These figures represent a USD 200,000 improvement over last year, and a savings of USD 1.9 million. See Figure 44.

Figure 44.
Measured in USD

4.44M
Global average cost of a data breach for all organizations

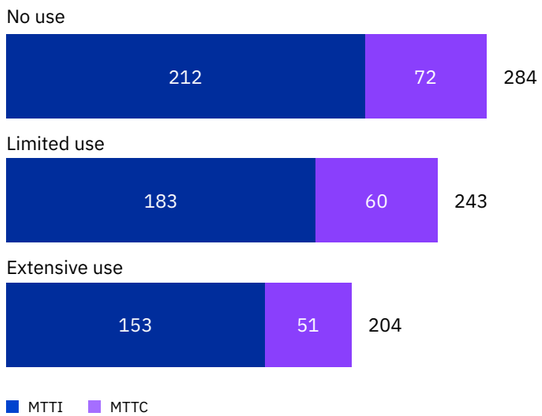
5.52M
Average cost of a data breach for organizations that didn't use security AI and automation

3.62M
Average cost of a data breach for organizations that extensively used security AI and automation



More AI and automation meant faster identification and containment
By extensively using AI and automation, organizations drove down the time it took to identify and contain a breach by an average of 80 days compared to those that didn't use AI and automation. Those quicker speeds directly equated to cost savings. See Figure 45.

Figure 45.
Time to identify and contain a breach with and without AI and automation; measured in days



Security teams used AI and automation evenly across workflows
Among organizations that said they used AI and automation extensively, nearly one-third did so across the full cybersecurity lifecycle: prevention, detection, investigation and response. Meanwhile, organizations that used these technologies in a limited way reported the same level of dispersion across the security lifecycle, but at slightly over 40%. See Figure 46.

Figure 46.
Percentage of organizations per usage level

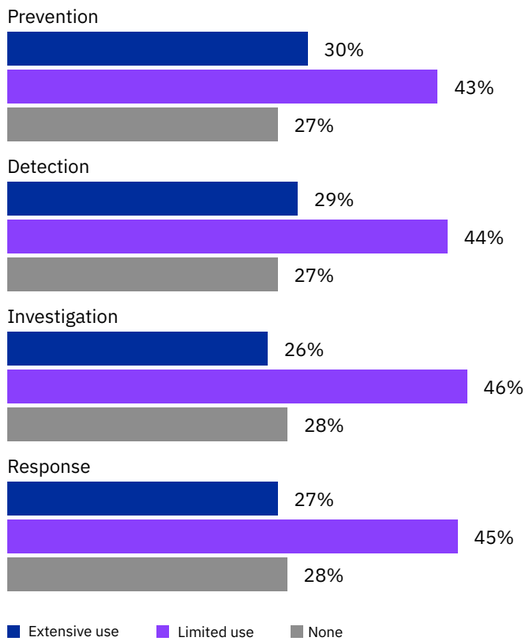
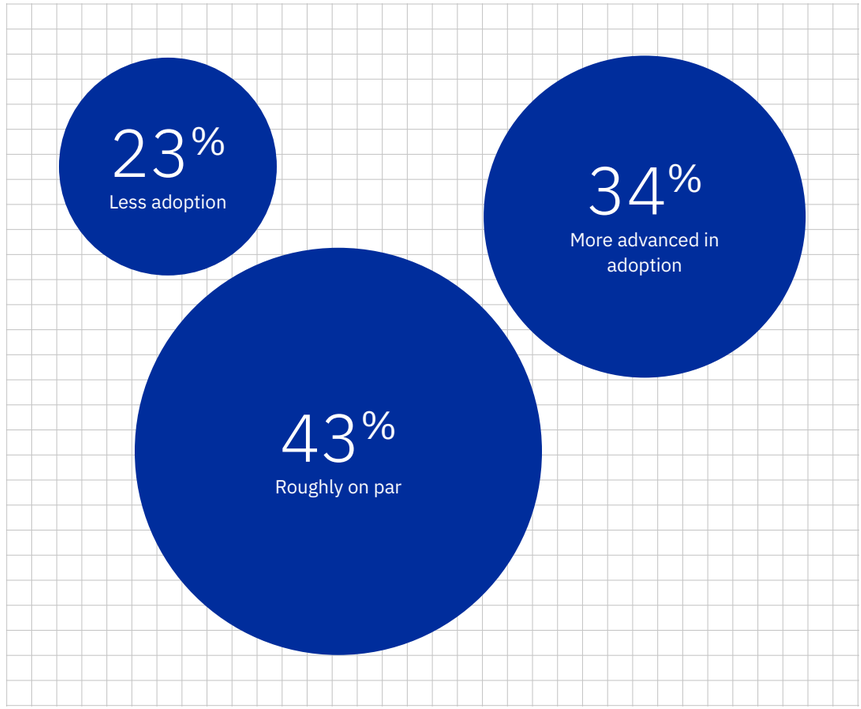


Figure 47.
Percentage of all organizations



Security teams adopted AI at the same rate as other business functions
This year's report aimed to discover if security teams were adopting AI at the same pace as other business units and functions in the wider organization. They are. A combined 77% were either adopting these technologies on par with (43%) or more advanced than (34%) their wider organization.
See Figure 47.

Security investments

Following a breach, security and IT leaders often turn their attention to fortifying their security defenses. Each year, organizations are asked if they plan to invest in new security measures and if so, where. Organizations in this study were allowed to choose more than one area of investment.

Post-breach investment declined
Less than half of organizations (49%) said they would increase security investments following a breach, a 22% drop over last year. While we saw more expected security investments post-breach last year, this year's anticipated slowdown might be attributed to organizations taking a more disciplined approach to evaluating which security initiatives deliver impact. For those organizations that do plan to increase security spending, the top three areas of investments were: threat detection (43%), data security and protection tools (37%), and IR planning and testing (35%). See Figures 48 and 49.

Figure 48.
Following the data breach, will your organization increase its security investment?

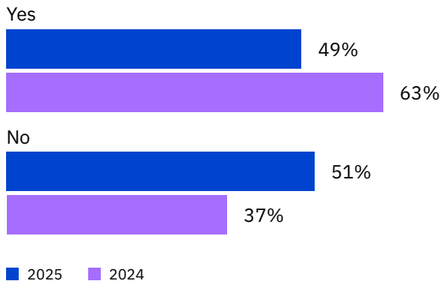
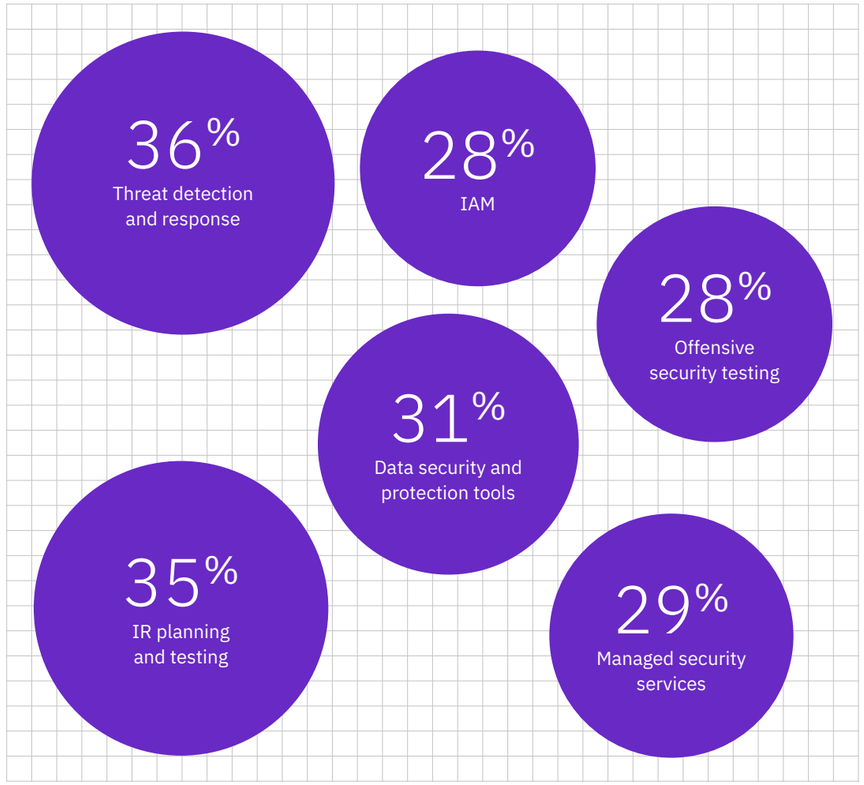


Figure 49.
Categories among organizations that will increase security investment; more than one response permitted

Figure 50.
Categories among post-breach organizations that plan to invest in AI-driven solutions, by percentage; more than one response permitted



AI-driven security solution investments remain strong
For organizations that plan to invest in security after a breach, 45% said they would choose AI-driven solutions. They also said they would do so fairly evenly across threat detection and response (36%), IR planning and testing (35%) and data security and protection tools (31%). See Figure 50.

Recommendations

To help prevent, mitigate and reduce the costs of a data breach, as well as secure and govern AI models, applications and usage, IBM experts suggest these five successful approaches.

Fortify identities—human and machine

Many organizations operate with lax access controls, over-permissioned accounts and low visibility into who has access to critical systems. In many cases, different departments and tools are used for identity and access management (IAM). All these factors create openings attackers are actively exploiting, so it's essential to limit such openings. Meanwhile, AI models and infrastructure are rapidly growing, offering attackers a new, high-value attack surface.

Fortifying identity security with the help of AI and automation can improve IAM without overburdening chronically understaffed security teams. And as AI agents begin to play a larger role in organizational operations, the same rigor must be applied to protecting agent identities as to protecting human identities. Just like human users, AI agents increasingly rely on credentials to access systems and perform tasks. So, it's essential to implement strong operational controls, or services that can help you do so, and maintain visibility into all non-human identity (NHI) activity. Organizations must be able to distinguish between NHIs using managed (vaulted) credentials and those using unmanaged credentials.

Once credentials are brought under management, it's crucial to protect and enforce proper lifecycle management and governance. It includes provisioning, rotation, auditing, protection and decommissioning of credentials, as well as monitoring the behavior of NHIs to ensure they operate within expected parameters. By doing so, organizations can reduce the risk of credential misuse and maintain a secure and compliant environment.

Today, many attackers are logging in rather than hacking in. To combat this issue, it's critical to prevent attackers from obtaining those credentials in the first place. One of the most effective ways to do so is by ensuring all human users adopt modern, phishing-resistant authentication methods, such as passkeys. These technologies are designed to eliminate the vulnerabilities of traditional passwords and one-time codes, making it significantly harder for attackers to intercept or misuse login credentials.

Elevate AI data security practices

Organizations have now moved beyond the experimentation phase with gen AI and AI agents into real-world innovation, weaving the technology deep into the fabric of their businesses. But the speed of adoption is outpacing security. This year's report found 97% of organizations that experienced an AI-related incident lacked proper access controls on AI systems. And because data is the fuel for AI, it's a prime target for attackers.

Securing AI data is essential not just for privacy and compliance, but also to protect data integrity, maintain organizational trust and avoid data compromise. This approach means going beyond surface-level controls and implementing strong data security fundamentals: data discovery and classification, as well as data protections, such as access control, encryption and key management. It can also include the use of data and AI security services. These measures aren't unique to securing AI, but the rise of AI as both a threat vector and security helper means they're more important than ever before.

Connect security for AI and governance for AI

Security for AI and governance for AI are complementary disciplines. When organizations keep them in silos, they increase risk, complexity and cost. Unfortunately, AI adoption is outpacing security and governance adoption: 41% of organizations in this year's report said they didn't have such policies in place, and 22% are still developing them.

Organizations must ensure chief information security officers (CISOs), chief revenue officers (CROs) and chief compliances officers (CCOs)—and their teams—collaborate regularly. Investing in integrated security and governance software and processes to bring these cross-functional stakeholders together can help organizations automatically discover and govern shadow AI. Such investments can also help them:

- Gain visibility into all AI deployments.
- Identify and mitigate vulnerabilities.
- Protect the prompts and data generated from unintended use.
- Use observability tools to improve compliance and detect anomalies.

Use AI security tools and automation to move faster

AI is already helping attackers move faster—for example, making deepfakes easy to create with just a few prompts, or cutting the time needed to produce a realistic phishing message from hours to minutes. As attackers turn to AI to produce and distribute more adaptive attacks, security teams should also embrace AI technologies. Security teams can use AI to reduce or prevent attacks and their business impacts, proactively employing measures that improve the accuracy of detection (threat hunting) and reduce the time to respond.

Security tools and managed security services, including those powered by AI and automation, can augment already overburdened security teams. They can significantly reduce the volume of alerts; identify at-risk data; spot security gaps and threats earlier; detect in-progress breaches; and enable faster, more precise attack responses.

Improve resilience

On a long enough timeline, data breaches are inevitable. They happen despite strong preventative measures. While it's important to try to block threats, it can't be an organization's only focus. They must also focus on, and plan for, minimizing damage once an attack gets through and a breach occurs.

Building resilience means being able to detect issues quickly, contain them before they cause significant impact and recover operations quickly with minimal disruption. A plan for building resilience should include regularly testing IR plans and restoration of backups, ensuring clear roles and responsibilities during crisis response—even for nontechnical leaders—and limiting high-level access to reduce the scope of a potential problem. In-person or virtual training can be essential in helping security teams understand their roles and execute in a crisis. To enhance their ability to handle attacks, organizations can also participate in cyber range crisis simulation exercises.

Organization demographics

This year's study examined 600 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 2025 study was conducted across 16 countries and geographic regions. For the second year the study included Benelux, the economic union of Belgium, the Netherlands and Luxembourg.

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.

Distribution by sample or region

ASEAN	4%	Australia	5%
US	11%	Benelux	5%
India	9%	Canada	5%
Brazil	8%	LATAM	5%
UK	8%	South Korea	5%
Germany	7%	ASEAN	4%
Japan	7%	Italy	4%
Middle East	7%	South Africa	4%
France	6%		

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 600 organizations studied.

Industry

Financial	14%	Consumer	4%
Industrial	12%	Hospitality	4%
Services	11%	Media	3%
Technology	10%	Pharma	3%
Energy	8%	Education	3%
Public	7%	Research	2%
Communications	6%	Healthcare	2%
Transportation	5%	Entertainment	1%
Retail	5%		

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
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

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 2025 report ranged in size between 2,960 and 113,620 compromised records.

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 2,960 and 113,620 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 3,470 separate interviews with individuals at 600 organizations that suffered a data breach between March 2024 and February 2025. 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 600 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.

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 6,485 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 1 March 2025.

About

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 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