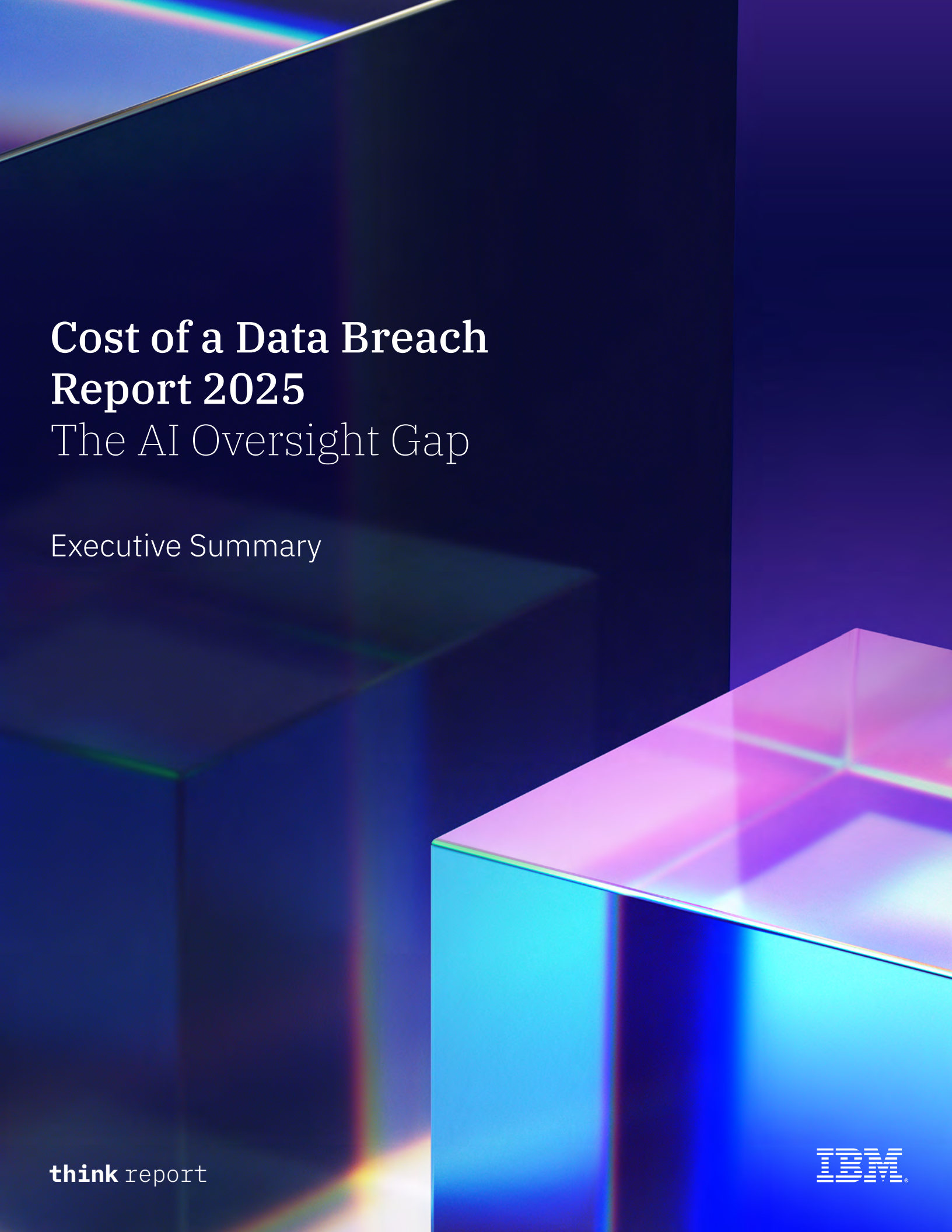
Cost of a Data Breach Report 2025

The AI Oversight Gap

Executive Summary



think report

IBM

Executive summary

Welcome to IBM's annual Cost of a Data Breach Report. With this edition, we celebrate 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.

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, 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.

13%

Share of AI-related security incidents

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 200K

Added cost of a breach involving shadow AI

Among the organizations studied this year, 20% said they suffered a breach due to security incidents involving shadow AI. Those breaches added USD 200,321 to the average breach price tag. 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 62% lack proper access controls on AI systems. 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%).

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 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 62% of organizations lack 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 don'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.

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