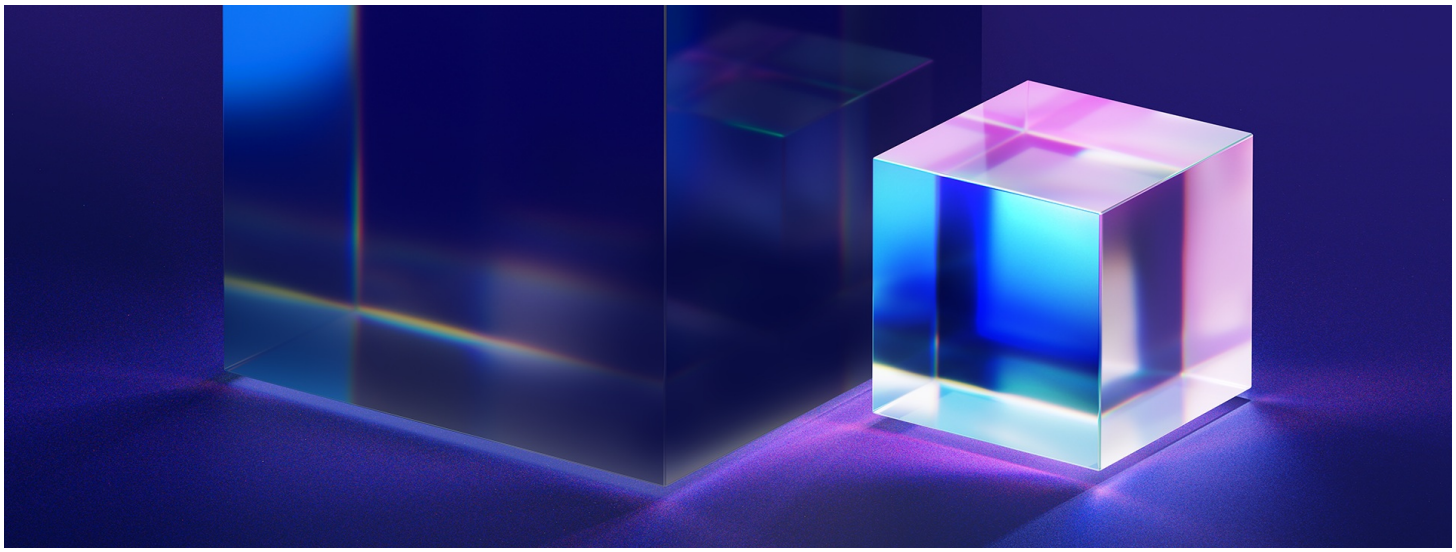
IBM Newsroom

IBM Report: 13% Of Organizations Reported Breaches Of AI Models Or Applications, 97% Of Which Reported Lacking Proper AI Access Controls

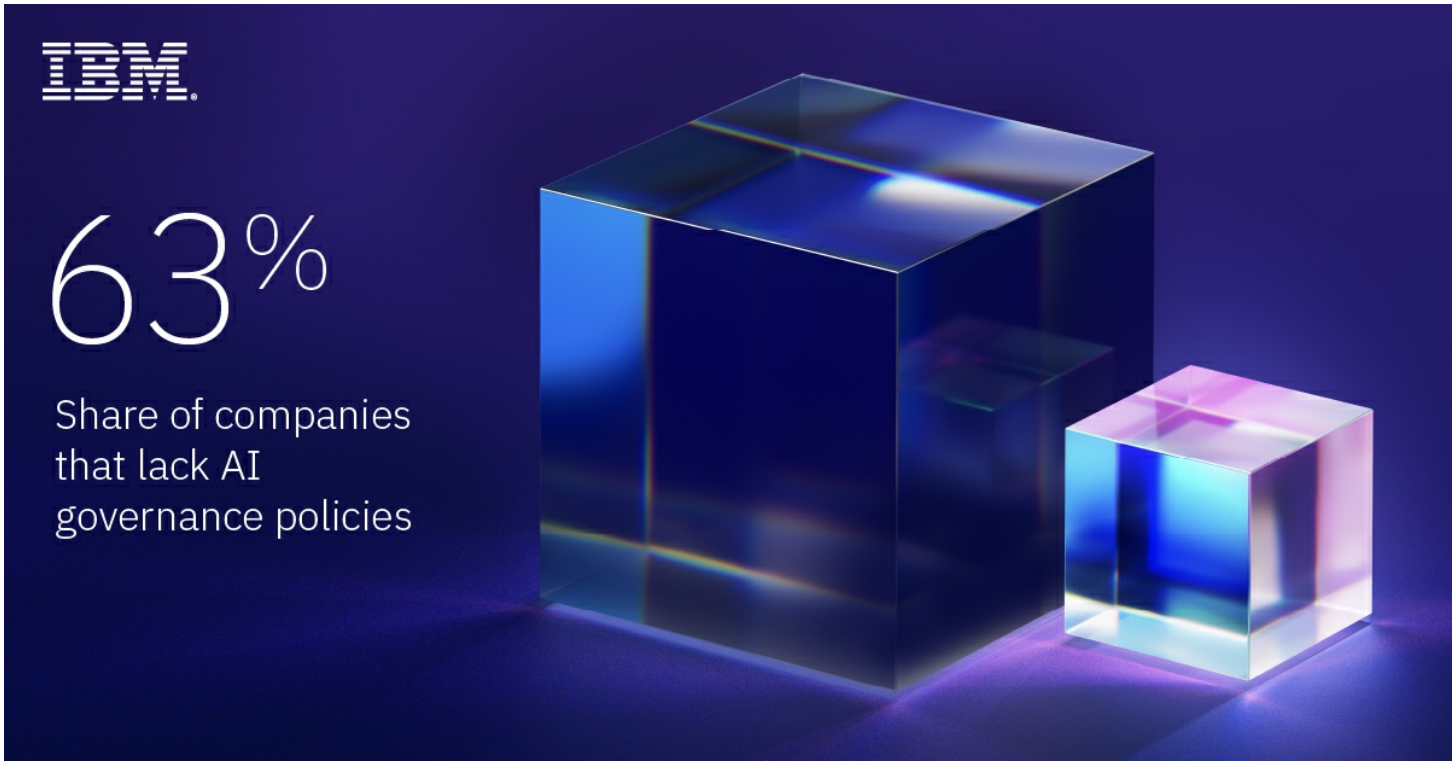
U.S. breach costs rise to $10.22 million, despite the global average cost of a breach decreasing to $4.44 million; Only 49% of breached organizations plan to invest in security



ARMONK, N.Y., July 30, 2025 /PRNewswire/ -- IBM (NYSE:IBM) today released its Cost of a Data Breach Report, which revealed AI adoption is greatly outpacing AI security and governance. While the overall number of organizations experiencing an AI-related breach is a small representation of the researched population, this is the first time security, governance and access controls for AI have been studied in this report, which suggests AI is already an easy, high value target.

- 13% of organizations reported breaches of AI models or applications, while 8% of organizations reported not knowing if they had been compromised in this way.
- Of those compromised, 97% report not having AI access controls in place.
- As a result, 60% of the AI-related security incidents led to compromised data and 31% led to operational disruption.

This year's results show that organizations are bypassing security and governance for AI in favor of do-it-now AI adoption. Ungoverned systems are more likely to be breached—and more costly when they are.



"The data shows that a gap between AI adoption and oversight already exists, and threat actors are starting to exploit it," said **Suja Viswesan, Vice President, Security and Runtime Products, IBM** "The report revealed a lack of basic access controls for AI systems, leaving highly sensitive data exposed, and models vulnerable to manipulation. As AI becomes more deeply embedded across business operations, AI security must be treated as foundational. The cost of inaction isn't just financial, it's the loss of trust, transparency and control."

However, the report did reveal that organizations using AI and automation extensively throughout their security operations saved an average $1.9 million in breach costs and reduced the breach lifecycle by an average of 80 days.

The 2025 report, conducted by Ponemon Institute, sponsored and analyzed by IBM, is based on data breaches experienced by 600 organizations globally from March 2024 through February 2025. Key findings from the report around AI security and breaches, the financial cost of a breach, and operational disruption are as follows:

Breaches and the AI era

- **AI Governance Policies.** 63% of breached organizations either don't have an AI governance policy or are still developing a policy. Of the organizations that have AI governance policies in place, only 34% perform regular audits for unsanctioned AI.
- **The Cost of Shadow AI.** One in five organizations reported a breach due to shadow AI, and only 37% have policies to manage AI or detect shadow AI. Organizations that used high levels of shadow AI observed an average of $670,000 in higher breach costs than those with a low level or no shadow AI. Security incidents involving shadow AI led to more personally identifiable information (65%) and intellectual property (40%) being compromised compared to the global average (53% and 33% respectively).
- **Smarter Attacks with AI**. 16% of breaches studied involved attackers using AI tools, most often for phishing or deepfake impersonation attacks.

The Financial Cost of a Breach

- **Data Breach Costs**. The global average cost of a data breach fell to$4.44 million, the first decline in five years, while the average U.S. cost of a breach reached a record $10.22 million.
- **Global Breach Lifecycles Hit Record Low**. The global average breach lifecycle (the mean time to identify and contain a breach, including restore services) dropped to 241 days, a 17-day reduction from the year prior, as more studied organizations detected the breach internally. Those organizations who detected the breach internally also observed a $900,000 savings on breach costs compared to those disclosed by an attacker.
- **Healthcare Breaches Remain the Costliest**. Averaging $7.42 million, healthcare breaches remained the most expensive across all studied industries, even as this sector saw a $2.35 million reduction in costs compared to 2024. Breaches across this sector take the longest to identify and contain at 279 days, that's more than 5 weeks longer than the global average of 241 days.
- **Ransom Payment Fatigue**. Last year, organizations pushed back against ransom demands, with more opting not to pay (63%) compared to the year prior (59%). As more organizations refuse to pay ransoms, the average cost of an extortion or ransomware incident remains high, particularly when disclosed by an attacker ($5.08 million).
- **Security Investments Stall Amid Rising AI Risks**. There was a significant reduction in the number of organizations that said they plan to invest in security following a breach, 49% in 2025 compared to 63% in 2024. Less than half of those that plan to invest in security post-breach will focus on AI-driven security solutions or services.

The Long Tail of a Breach: Operational Disruption

According to the 2025 IBM report, nearly all organizations studied suffered operational disruption following a data breach. This level of disruption is taking a toll on recovery timelines. Among organizations that reported recovery, most took more than 100 days on average to do so.

However, the consequences of a breach continue to extend beyond containment. While down compared to the year prior, nearly half of all organizations reported that they planned to raise the price of goods or services because of the breach, and nearly one-third reported price increases of 15% or more.

About the Cost of a Data Breach Report

The Cost of a Data Breach Report has investigated nearly 6,500 data breaches over the past 20 years. Since the inaugural report in 2005, the nature of breaches has evolved dramatically. Back then, risk was largely physical. Today, the threat landscape is overwhelmingly digital and increasingly targeted, with breaches now driven by a spectrum of malicious activity.

With the pace of enterprise AI adoption proliferating, for the first time, the Cost of a Data Breach research studied the state of security and governance for AI, the type of data targeted in security incidents involving AI, breach costs associated with AI-driven attacks, and the prevalence and risk profile of shadow AI (unregulated, unauthorized use of AI). Historical findings from past reports include the following:

- **2005:** nearly half (45%) of all data breaches were caused by lost or stolen computing devices, such as a laptop or thumb drive, and only 10% of breaches were due to hacked electronic systems.
- **2015:** breaches due to cloud misconfiguration weren't even a categorized threat, today they are a leading target.
- **2020:** ransomware began to surge, and by 2021 it accounted for an average of$4.62 million in breach costs, and this year

that number reached an average of $5.08 million (when the incident was disclosed by an attacker).

- **2025:** AI, which was included for the first time in the research this year, is quickly emerging as a high value target.

Additional sources:

- Download a copy of the 2025 Cost of a Data Breach Report to learn more.
- Sign up for the 2025 IBM Cost of a Data Breach webinar onWednesday, August 13, 2025, at 11:00 a.m. ET.
- Read more about the report's top findings in this IBM blog.

About IBM
IBM is a leading provider of global hybrid cloud and AI, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs, and gain a competitive edge in their industries. Thousands of governments and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently, and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's long-standing commitment to trust, transparency, responsibility, inclusivity, and service. Visit www.ibm.com for more information.

Media contact:

IBM
Michele Brancati
mbrancati@ibm.com

SOURCE IBM

Additional assets available online: Photos

https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls