Average cost of a data breach in the **financial industry**

USD 5.56M

2nd highest cost
of 17 industries studied

25% higher than
the USD 4.44M global average

9% lower
compared to 2024

Global highlights

Top three initial attack vectors

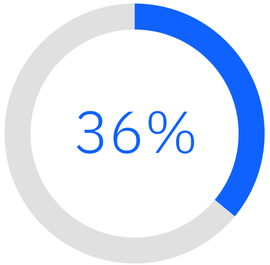
1 in 6

Number of breaches involving AI-driven attacks

USD 5.14M

Average cost of a ransomware-related breach

Key statistics

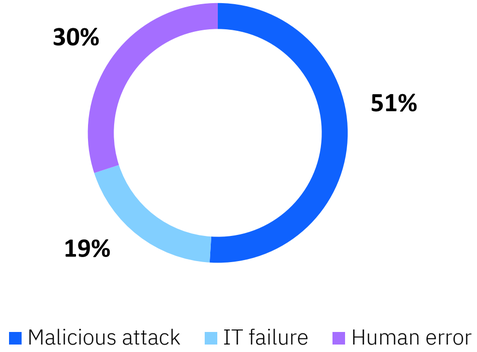


Percentage of financial organizations with extensive use of security AI and automation

USD 1.9M

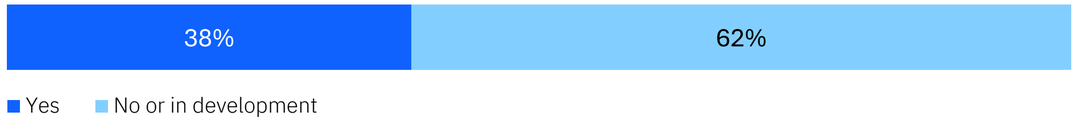
Global cost savings of extensive use of security AI and automation versus no security AI and automation

Root causes of a data breach

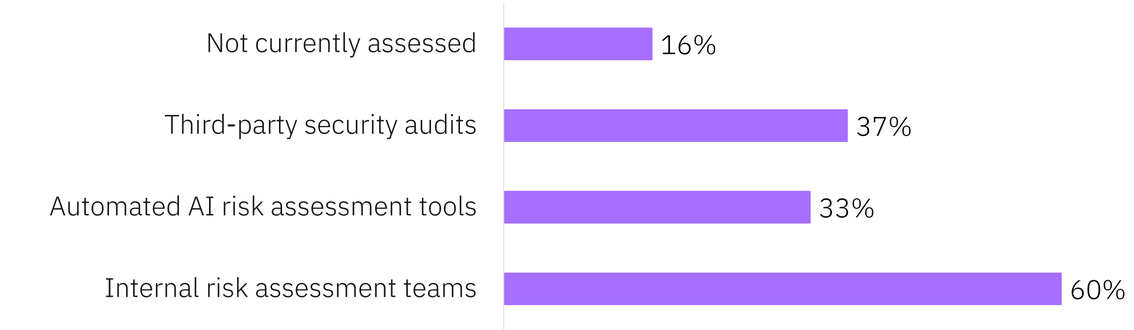


Time to identify and contain

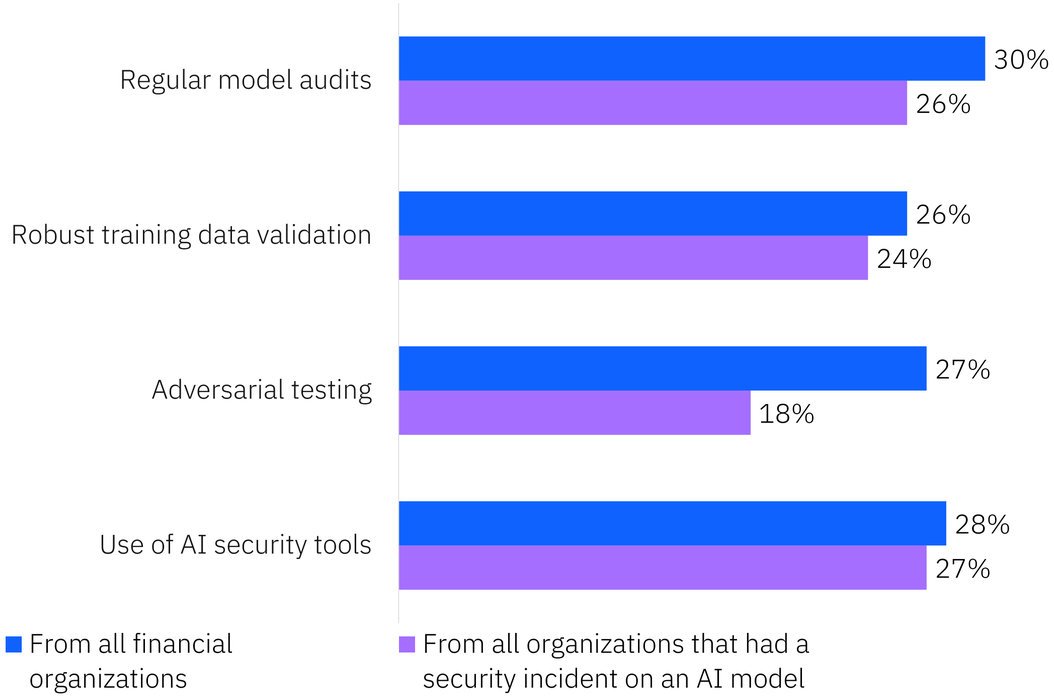
Prevalence of governance policies to manage the use of AI and prevent shadow AI



Assessing the risk of AI model evasion attacks*



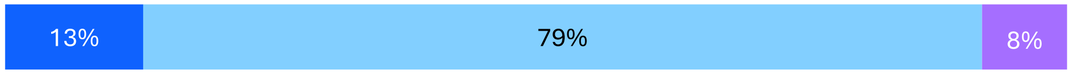
Top ways organizations mitigate risk to AI models*



Global findings

Has your organization experienced a security incident involving shadow AI?

Has your organization experienced a security incident on an AI model or application?



Yes No Unsure

USD 4.63M

Average cost of a breach involving shadow AI

97%

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

* More than one response permitted

Recommendations

- Adopt a **risk management** approach where data encryption strategies consider the types of data, its use and where it resides to lower the impact in case of a breach. Unmanaged data sources and unencrypted data, including data in AI workloads, further exacerbate the risk.
- Apply **data security posture management** (DSPM) and other solutions, such as identity and access management (IAM) and attack surface management (ASM), across all **hybrid environments** for consistent and comprehensive protection. 40% of data breaches involved data stored across multiple environments.
- Implement risk-based **IAM** lifecycle policies that support your hybrid cloud environment and user experience.
- Apply **AI and automation** to enhance your security prevention strategies, including areas of red-teaming and posture management. This enhancement can often be addressed by managed security services.
- Adopt a framework for securing **generative AI (gen AI) data**, models and usage, along with establishing **AI governance** controls. Only 24% of gen AI initiatives are secured. Use data discovery and classification to detect sensitive data used in training or fine-tuning.
- Offer **security training** to nonsecurity practitioners, including data scientists and data engineers who work in machine learning and AI teams.
- Invest in post-breach response preparedness, including **cyber range crisis simulation exercises**. Document, communicate and practice a company-wide incident response plan (IRP) to include security, IT, ops, legal, HR, PR, C-suite and third parties, including retained IR vendors.
- Apply and potentially integrate IT security principles into your **operational technology (OT) and Internet of Things (IoT)** environments.

Download full report →