V092525

IBM's October 2025 report on the state of AI risk—formally part of its *Cost of a Data Breach Report*—reveals a stark and widening gap between AI adoption and AI governance.

Here are the key findings: 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

---

🧠 AI Risk Landscape: Key Insights from IBM's 2025 Report

🚨 Breach Statistics

- **13%** of organizations reported breaches involving AI models or applications.
- **97%** of those breached lacked proper AI access controls.
- **60%** of AI-related incidents led to data compromise; **31%** caused operational disruption.

🕵️ Shadow AI: The Hidden Threat

- **1 in 5** breaches were caused by "shadow AI"—unsanctioned AI tools used without organizational oversight.
- Breaches involving shadow AI cost **$670K more** on average than standard incidents.
- Only **37%** of organizations have policies to detect or manage shadow AI.

🧩 Governance Gaps

- **63%** of breached organizations had no AI governance policy or were still developing one.
- Of those with policies, only **34%** conducted regular audits for unauthorized AI use.
- Just **17%** of companies had technical controls to prevent employees from uploading sensitive data to public AI tools.

💸 Financial Impact

- Global average breach cost: **$4.44M** (down for the first time in 5 years).
- U.S. average breach cost: **$10.22M**—a record high.
- Organizations using AI and automation extensively in security saved **$1.9M** and reduced breach lifecycles by **80 days**.

This report underscores a critical paradox: while AI accelerates breach detection and operational efficiency, it simultaneously introduces new vulnerabilities that most organizations are unprepared to manage.

Here's a concise briefing on IBM's *State of AI Risk* findings from October 2025:

🧠 IBM 2025 AI Risk Brief

- **AI-related breaches** affected 13% of organizations, with most lacking proper access controls.

- **Shadow AI**—unauthorized tools—was responsible for 1 in 5 breaches, costing $670K more per incident.

- **Governance gaps** persist: 63% of breached firms had no formal AI policy; only 17% had controls to prevent sensitive data uploads to public AI.

- **Security automation** helped reduce breach costs by $1.9M and shortened breach lifecycles by 80 days.

- **U.S. breach costs** hit a record $10.22M, while global averages fell slightly to $4.44M.