Kiteworks

TOP 5

FOR CISOS AND COMPLIANCE LEADERS

What the 2026 IBM Cost of a Data Breach Report Revealed About Data Security and Compliance Risk

The Five Findings That Matter Most for Security and Compliance Leaders Right Now.

1 Governance Gaps Drive the Cost, Not AI Itself

92% of organizations hit by an AI-related security incident had no AI access controls in place when it happened. AI-driven attacks are up 56% year over year, yet only 32% of breached organizations have an AI policy today, down from 37% last year, and just 19% coordinate between AI governance and security teams. The share with no policy at all fell from 41% to 35%, but the share stuck "in development" jumped from 22% to 33% — governance is stalling in draft form while the global average breach cost climbed 12% to a record $4.99 million.

2 Shadow AI Use Doubled in a Single Year

Incidents involving unsanctioned AI tools more than doubled, from 20% to 43% of cases studied, as AI-driven attacks broadly grew 56% year over year. Nearly half of shadow AI incidents, 49%, resulted in data loss or compromise, 42% caused operational disruption, and 21% led to a regulatory fine. Shadow AI has become shadow IT with higher stakes.

3 AI-Related Breaches Cost More and Draw Fines

AI-related breaches averaged $5.33 million versus $4.70 million for other incidents. Specific techniques ran higher still: model inversion attacks averaged $6.07 million, 18% above the global average, and prompt injection came in at $5.89 million. Breaches involving an organization's own AI models drew regulatory fines in about 1 of 5 cases. Financial services and energy together accounted for 62% of all AI-driven breaches studied, while healthcare remained the costliest industry overall at $6.64 million per breach.

4 Security Automation Pays Off, but Adoption Lags

Organizations that used security AI and automation extensively cut their average breach cost to $4.00 million, versus $5.93 million for organizations with no use at all, and contained breaches 65 days faster. Adoption is still shallow and uneven: only 36% use these tools extensively, 56% apply them to threat hunting and 54% to automated response, but just 18% extend them to vulnerability scanning and management.

5 Machine Identity Is the Overlooked Risk

Only 46% of organizations secure the machine identities their AI workflows depend on. UC Berkeley researchers project that within two years, AI will favor attackers over defenders by 31.7% — a gap that widens fastest wherever machine and agent identities go ungoverned alongside human ones.

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.