PUBLICATION

Ten Key Insights from IBM's Cost of a Data Breach Report 2025

Authors: Matthew George White, Alexander Frank Koskey, III
August 22, 2025

IBM and the Ponemon Institute have released the 2025 Cost of a Data Breach Report. The report, which has become an annual late-summer tradition, highlights the evolving risks and costs associated with data breaches. This year's report underscores two critical items: (1) breach costs for U.S. organizations reached an all-time high, and (2) Artificial intelligence (AI) is reshaping both sides of the cyber landscape. While organizations are deploying AI-driven security, attackers are exploiting AI to fuel phishing, deepfakes, and other sophisticated attacks, raising the stakes (and costs) for organizations across the country.

Below are ten key insights from this year's report, along with some recommendations for your organization to mitigate AI and other related breach risks.

Key Insights

1. **Global Costs Ease While U.S. Costs Surge**: The global average cost of a data breach dropped to $4.44 million, the first decline in five years. However, average costs in the U.S. surged to a record $10.22 million per incident, driven by increased regulatory fines and detection costs.

2. **AI-Related Breaches Are Rising**: One in six organizations experienced breaches involving AI-driven attacks. The most common tactics involving AI were phishing (37 percent) and deepfake impersonations (35 precent).

3. **AI Governance Is Lacking**: AI models used by organizations emerged as an attractive attack surface with 13 percent of organizations reporting an incident on an AI model that resulted in a breach. 97 percent of those organizations reported that they lacked proper AI access controls. Furthermore, 63 percent of organizations stated that they do not have an AI governance policy and, for those that do, only one in three said they perform regular audits for unsanctioned AI.

4. **Shadow AI Remains a Hidden Risk**: Incidents involving shadow AI accounted for 20 percent of data breaches – seven percent higher than AI models sanctioned by organizations. Furthermore, 11 percent of organizations were unsure if they experienced a shadow AI incident. Of those organizations that did experience a shadow AI incident, 62 percent reported that the compromised data was most often stored across multiple environments and a public cloud.

5. **Regulators Take Action**: One of the primary reasons U.S. breach costs have risen is due to the more active role taken by regulators. Of the 600 breaches surveyed by IBM, 32 percent paid a regulatory fine. Forty-eight percent of those fines were more than $100,000, and signal a trend that regulatory enforcement is likely on the rise when it comes to data breaches.

6. **Phishing is the Most Common Initial Attack Vector**: Phishing attacks replaced stolen credentials as the most common initial attack vector (16 percent of attacks). Supply chain compromise and compromised credentials rounded out the top three and highlight the emergence of threat actors leveraging AI tools and/or targeting AI platforms for attacks.

7. **Health care and Financial Services Remain Primary (and Expensive) Targets**: To no surprise, health care continues to be the industry with the highest average breach costs at $7.42 million. Financial services remained second at $5.56 million. However, these average costs are down from 2024.

8. **Recovery Time Remains Extensive**: Although organizations are identifying and containing breaches at a faster rate than in previous years, the time for full recovery remains extensive. Seventy-six percent of organizations reported that recovery took longer than 100 days, and just two percent said they were able to recover in less than 50 days.

9. **Costs from Insider Threats are on the Rise**: Insider attacks resulted in the highest average breach costs among initial threat vectors ($4.92 million). This is the second year in a row these attacks have been the costliest initial threat vector and a great reminder to organizations that protecting against threats internally is just as critical as protecting against threats externally.

10. **More Organizations Refuse to Pay a Ransom**: Sixty-three percent of organizations in this year's report opted not to pay a ransom. This is up from 2024 (59 percent) and reinforces a growing trend within the U.S. Interestingly, fewer organizations contacted law enforcement following a ransomware attack, with just 40 percent of organizations reporting that they did, down from 52 percent in the previous year.

Recommendations for Clients

The following are some recommendations for your organization to mitigate AI and other related risks identified in this year's report:

1. **Implement AI Governance Frameworks**: An AI governance framework must be a priority for your organization. This includes establishing clear policies for the use of AI tools across your organization, minimizing shadow AI risks, and regularly auditing AI models and tools to minimize risk and ensure compliance with applicable regulations.

2. **Adopt AI-Powered Security Tools**: Use automation for threat detection, investigation, and response. Furthermore, leverage tools to detect shadow AI and monitor AI deployments. These tools reduce breach costs and accelerate containment.

3. **Elevate Data Security for AI**: Implement encryption, access controls, and key management along with mapping and classifying AI-related data assets.

4. **Incorporate AI Into Tabletop Exercises**: In light of the proliferation of AI-related attacks and expanded attack surface due to the deployment of AI tools, your organization must incorporate AI-related scenarios into your tabletop exercises. This is not just a technical issue; it is a management and enterprise-wide issue.

5. **Bolster Insider Threat and Training Programs**: Deploy monitoring and access controls to detect suspicious behavior by employees. Also, combine this technology with HR-led awareness campaigns to reduce malicious insider risks.

If you have questions about your data strategy or how to protect against unauthorized data access, reach out to our authors, Alexander F. Koskey, CIPP/US, CIPP/E, PCIP and Matthew G. White, AIGP, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, or any member of our Data Protection, Privacy and Cybersecurity Team.