

## Hey! What's New? 2025-89

### Shadow AI Emerges As Significant Cybersecurity Threat

Steph Brown writes in *FM Financial Management* that “use of unmonitored artificial intelligence (AI), better known as shadow AI, is a growing issue for companies in more ways than one. According to IBM’s [Cost of a Data Breach Report 2025](#), the global average breach cost dropped for the first time in five years (from \$4.88 million in 2024 to \$4.44 million), but incidents involving shadow AI systems proved more expensive to resolve. Companies with high levels of shadow AI added \$670,000 to the average breach cost, compared with those that had low levels of shadow AI or none.”

That, she notes, “is a cause for concern because breaches involving shadow AI are quite common. Security incidents involving shadow AI accounted for 20% of data breaches globally, seven percentage points higher than security incidents involving sanctioned AI. Breaches across shadow AI systems also resulted in more of customers’ personal identifiable information being comprised, compared with breaches of sanctioned AI.”

Brown explains that “one reason shadow AI is becoming an expensive problem for companies is because those systems can go undetected by organizations, giving attackers more time to exploit vulnerabilities when employees use it. This problem is intensified by inadequate AI governance procedures.”

IBM found that most organizations lacked governance to both manage and detect shadow AI. “Ninety-seven per cent of organizations that experienced an AI-related breach said they lacked proper AI access controls,” the report said. The majority of breached organizations (63%) also said they don’t have an AI governance policy or are still developing one.

According to the research, “security teams continue to improve their mean time to identify and mean time to contain a data breach with the help of AI and automation. The mean time organizations took to identify and contain a breach fell to 241 days, reaching a nine-year low and continuing a downward trend that started after a 287-day peak in 2021, IBM found. This year, researchers found these teams and tools detected 50% of breaches, a vast leap over last year’s tally of 42%, which was itself was a jump from 33% in 2023.” Breaches identified by internal security teams also cost companies less, the report added.

As more cybersecurity risks emerge from shadow AI, security teams and AI tools are proving effective in mitigating those risks. So far, those teams have been more effective in identifying shadow AI incidents (57%) than overall breach discoveries (50%), the report stated.

Brown points out that, “as cybersecurity personnel move smarter and faster, so do attackers, who are beginning to utilize AI to improve their rate of success. Overall, 16% of data breaches involved attackers using AI, most often for AI-generated phishing (37%) and deepfake impersonation attacks (35%).”

Alarming, IBM found that generative AI has cut the time needed for attackers to craft a convincing phishing email from 16 hours to five minutes.

Phishing replaced stolen credentials this year as the most common initial vector (16%), and supply chain compromise surged to become the second-most prevalent attack vector (15%). Approximately one-third of organizations (31%) that experienced a security incident involving authorized AI suffered operational disruption.

The IBM report makes recommendations that include:

- **Secure AI data:** “Securing AI data is essential not just for privacy and compliance, but also to protect data integrity, maintain organizational trust, and avoid data compromise.”
- **Utilize AI security tools:** “Security teams can use AI to reduce the volume of alerts; identify at-risk data; spot security gaps and threats earlier; detect in-progress breaches; and enable faster, more precise attack responses.”
- **Integrate security and governance:** “When organizations keep security for AI and governance for AI in silos, they increase risks, complexities, and costs. “Investing in integrated security and governance software and processes ... can help organizations automatically discover and govern shadow AI.”
- **Improve resilience:** “Organizations should include regular testing of incident response plans and restoration of backups, ensuring clear roles and responsibilities during crisis response, even for nontechnical leaders.”

Read the article at [Shadow AI emerges as significant cybersecurity threat](#); download the report at [Cost of a Data Breach Report 2025](#).