NEWS BRIEF

U.S. AVERAGE BREACH COST HITS RECORD HIGH OF $10.22 MILLION

The average cost of a data breach in the U.S. soared to an all-time high of $10.22 million, even as the global average cost dropped 9% to $4.44 million, according to IBM's **Cost of a Data Breach Report 2025.**

The firm attributed the 9% rise in U.S. breach costs to regulatory fines and "higher detection and escalation costs."

Outside the U.S., the decrease in the average breach cost stemmed from quicker identification and containment of breaches via AI and automation, making for shorter breach investigations and an estimated cost savings of $1.9 million. The global average for time to detect and contain a breach dropped 17 days to 241 days last year.

However, IBM also found that nearly all organizations that faced a data breach experienced operational disruption, with most taking more than 100 days on average to recover fully. Additionally, about 65% of breached businesses say they haven't fully recovered from their cyber events.

The report also revealed that artificial intelligence-related cyber breaches remain uncommon, but of those that have occurred, nearly 97% were due to a lack of proper AI access controls.

"The data shows that a gap between AI adoption and oversight already exists, and threat actors are starting to exploit it," said Suja Viswesan, vice president of security and runtime products at IBM. "The report revealed a lack of basic access controls for AI systems, leaving highly sensitive data exposed and models vulnerable to manipulation. As AI becomes more deeply embedded across business operations, AI security must be treated as foundational."

Viswesan added, "The cost of inaction isn't just financial, it's the loss of trust, transparency and control."

About 13% of organizations responding to IBM's survey reported having a breach involving their AI models or applications, with incidents most often occurring via a company's supply chain, compromised apps, APIs or plug-ins.

"These incidents had a ripple effect: they led to broad data compromise (60%) and operational disruption (31%). The findings suggest AI is emerging as a high-value target," said IBM in the report.

IBM also found that "shadow AI" – the use of AI without approval or oversight by employers – added about $670,000 to the global average cost of a data breach.

"These incidents also resulted in more personal identifiable information (65%) and intellectual property (40%) data being compromised. And that data was most often stored across multiple environments, revealing that just one unmonitored AI system can lead to widespread exposure," said the firm.

CONCLUSION

In today's evolving digital risk landscape, it's vital for organizations to take cybersecurity seriously and utilize effective measures to decrease their exposures. By leveraging proper cybersecurity controls, organizations can help safeguard their operations from a wide range of losses and reduce the likelihood of related insurance claims.

For more risk management and cyber secruity guidance, **contact us today.**