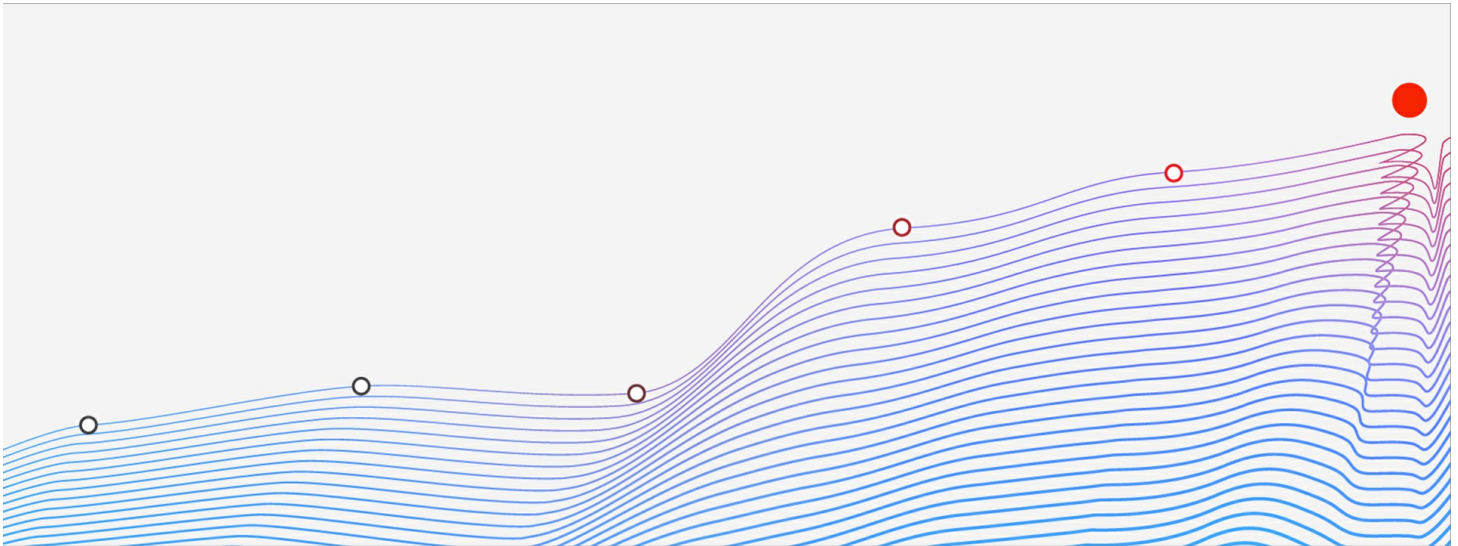# IBM Report: Average cost of a data breach in India touched INR 179 million in 2023

**In the country, organizations with extensive use of security AI and automation helped cut data breach costs by INR 95 million and reduce breach lifecycles by 153 days**



**INDIA, Bengaluru, July 25, 2023** -- IBM (NYSE: IBM) Security today released its annual Cost of a Data Breach Report,[1] showing the average cost of a data breach in India reached INR 179 million in 2023 – an all-time high for the report and almost a 28% increase since 2020. Detection and escalation costs jumped 45% over this same time frame, representing the highest portion of breach costs, and indicating a shift towards more complex breach investigations.

At nearly 22%, the most common attack type in India was phishing, followed by stolen or compromised credentials (16%). Social engineering was the costliest root cause of breaches at INR 191 million, followed by malicious insider threats, which amounted to approximately INR 188 million.

According to the 2023 IBM report, globally businesses are divided in how they plan to handle the increasing cost and frequency of data breaches. The report found that while 95% of organizations studied globally have experienced more than one breach, these breached organizations were more likely to pass incident costs onto consumers (57%) than to increase security investments (51%).

"With cyberattacks growing in pace and cost in India, businesses must invest in modern security strategies and solutions to stay resilient. The report shows that security AI and automation had the biggest impact on keeping breach costs down and cutting time off the investigation - and yet a majority of organizations in India still haven't deployed these technologies. It's clear that there is still considerable opportunity for businesses to boost detection and response speeds and help stop the ongoing trend of growing breach costs," said Viswanath Ramaswamy, Vice President, Technology, IBM India & South Asia.

**Breaching data across environments**
In India, 28% of data breaches studied resulted in the loss of data spanning multiple types of environments (i.e., public cloud, private cloud, on-prem) – indicating that attackers were able to compromise multiple environments while avoiding detection. When breached data was stored across multiple environments, it also had the highest

associated breach costs (INR 188 million) and took the longest to identify and contain (327 days).

**Need for AI and automation to pick up speed in India**
AI and automation had the biggest impact on the speed of breach identification and containment for studied organizations. In India, companies with extensive use of AI and automation experienced a data breach lifecycle that was 153 days shorter compared to studied organizations that have not deployed these technologies (225 days versus 378 days). In fact, studied organizations that deployed security AI and automation extensively saw nearly INR 95 million lower data breach costs than organizations that didn't deploy these technologies – the biggest cost saver identified in the report. In this context, it is important to note that 80% of studied organizations in India have limited (37%) or no use (43%) of AI and automation.

**Additional Sources**

- To download a copy of the 2023 Cost of a Data Breach Report, please visit: https://www.ibm.com/security/data-breach.
- Read more about the report's top findings in this IBM Security Intelligence blog.
- Sign up for the 2023 IBM Security Cost of a Data Breach webinar on Tuesday, August 1, 2023, at 11:00 a.m. ET here.
- Connect with the IBM Security X-Force team for a personalized review of the findings: https://ibm.biz/book-a-consult.
- For a closer look at the report recommendations visit: Cost of a Data breach Action Guide.

**About IBM Security**
IBM Security helps secure the world's largest enterprises and governments with an integrated portfolio of security products and services, infused with dynamic AI and automation capabilities. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to predict threats, protect data as it moves, and respond with speed and precision without holding back business innovation. IBM is trusted by thousands of organizations as their partner to assess, strategize, implement, and manage security transformations. IBM operates one of the world's broadest security research, development, and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide.

[1] The 2023 Cost of a Data Breach Report, conducted by Ponemon Institute, is sponsored and analyzed by IBM Security.

**Media contact:**

Lakshmi Visakha K B
lakshmi.visakha@ibm.com