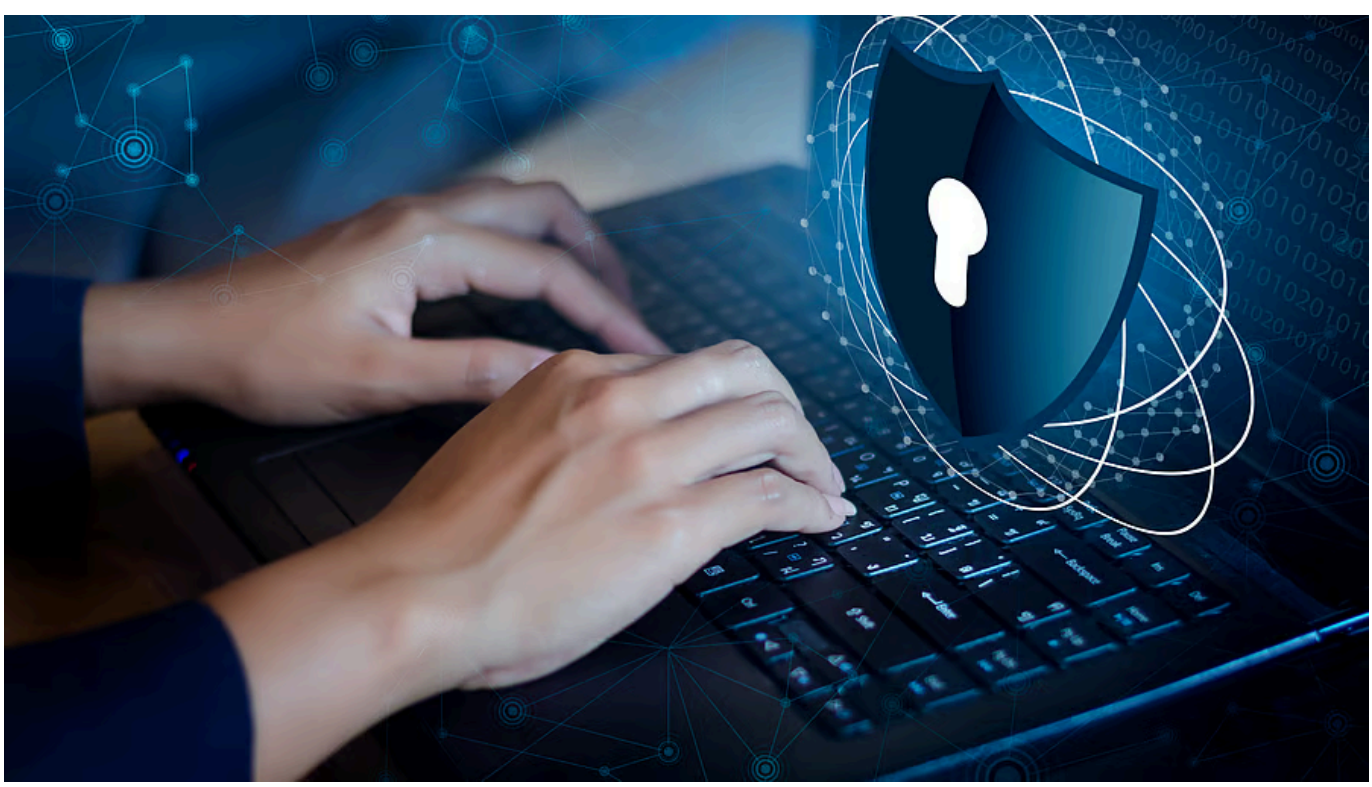
DECCAN HERALD

Bank of Baroda breach: Real-time monitoring key to stopping email-driven attacks, say experts

According to Govind Rammurthy, chief executive officer and managing director of security solutions provider eScan, the weak password was the mistake.

Uma Kannan

Last Updated : 29 July 2026, 05:50 IST



Cyber resilience extends beyond safeguarding critical systems as a risk mitigation strategy. Credit: iStock Photo

Bengaluru: The Bank of Baroda (BoB) incident reveals that modern-day cyberattacks can expose sensitive banking data with a single compromised employee mailbox, without even impacting the core banking systems. On Monday, the state-owned Bank of Baroda reported an incident that involved the compromise of an employee's email account, resulting in unauthorised access to certain data.

"The matter was promptly identified, and immediate containment measures were implemented," the bank said. However, the incident raises several questions, including the safety of customers' data. Dipesh Kaura, country director, India and SAARC, Securonix, said financial data in banks is a very high-value target for cyber criminals, and any data breach is certainly a major concern for banking organisations.

"Organisations handling huge volumes of sensitive financial data at scale require AI-powered, cloud-native, and outcome-driven SIEM platforms to detect, prioritise, and mitigate email-driven threats. These platforms help reduce dwell time, enabling security teams to accelerate incident response before single isolated events escalate to major breaches," Kaura said.

Also Read: Bank of Baroda data breach: Beware of 'Digital Arrest' scam; here's how to safeguard your account

Also Read: Bank of Baroda data breach: Beware of 'Digital Arrest' scam; here's how to safeguard your account

Cyber resilience extends beyond safeguarding critical systems as a risk mitigation strategy. It requires continuous monitoring of identities, financial data, privileged access, and user behaviour across the organisation to detect threats early and strengthen overall security, the expert said.

'Fairly predictable'

According to Govind Rammurthy, chief executive officer and managing director of security solutions provider eScan, the weak password was the mistake. "Bank of Baroda's breach isn't surprising — it's fairly predictable," he said. TripleX, a new hacking group, is believed to be behind the attack.

Rammurthy said, "TripleX didn't use zero-days or nation-state exploits. They walked through a weak password on an internet-facing system. Then they waited. For 2.5 months, they collected data quietly, without any fanfare, without alerts, without disruption, as no individual or internal system monitored what data and how much data actually moved. This is where organisations fail. They build firewalls, run scans, deploy intrusion detection, all the while assuming that attackers will use obvious techniques."

TripleX exploited basic security gaps that strong endpoint monitoring would have caught immediately, he added.

Bank of Baroda said a comprehensive forensic investigation has been initiated, and the bank is working closely with the relevant authorities.

"By leveraging the latest advances in Machine Learning, security teams can detect and respond to potential compromises across the IT environment in real time while attacks are contained before they escalate into major security incidents," Kaura added.