SOPHOS

THE STATE OF RANSOMWARE IN INDIA 2026

Findings from an independent, vendor-agnostic survey of 240 organizations in India that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

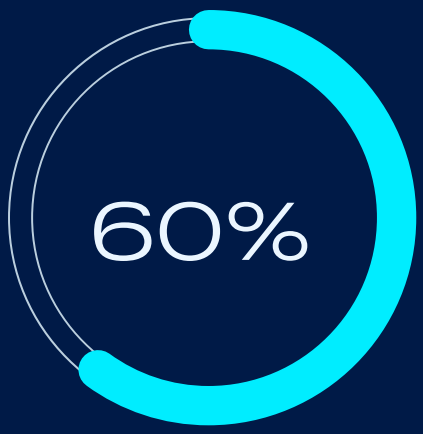
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 240 from India.

The survey was conducted between January and March 2026. All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months. All financial data points are in U.S. dollars. Outlier ransoms of $40 million or more were removed from this data.

Survey of

240

IT/cybersecurity leaders in India working in organizations that were hit by ransomware in the last year.



Percentage of attacks that resulted in data being encrypted.

Median Indian ransom payment.

Average cost to recover from a ransomware attack.

Why Indian organizations fall victim to ransomware

- **Malicious email was the most common technical root cause of attack,** used in 28% of attacks, followed by phishing (26%) and compromised credentials (19%). Exploited vulnerabilities dropped sharply, falling to 11% from 29% in the 2025 report.
- **A lack of protection (43%) was the most common operational root cause,** followed by an unknown security gap (40%) and poor-quality protection (38%).
- **(NEW) Exposed applications and systems were the most common attack entry point (47%)** for non-email, non-phishing root causes, followed by firewalls (27%) and user devices (20%).
- **(NEW) 79% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.**

What happens to the data

- **60% of attacks resulted in data being encrypted.** This is above the global average of 56% and an increase from the 42% reported by Indian respondents in the 2025 report.
- **Data was also stolen in 26% of attacks where data was encrypted**, a drop from the 31% reported in 2025.
- **98% of Indian organizations that had data encrypted were able to get it back,** in line with the global average.
- **56% of Indian organizations paid the ransom and got data back,** a slight increase from the 53% reported in last year's report.
- **67% of Indian organizations used backups to recover encrypted data,** a considerable increase from the 51% reported in the 2025 report.

Ransoms: Demands and payments

- **The median Indian ransom demand was $88,000,** the lowest recorded of any country, and a 91% drop from the $961,289 reported in the 2025 report.

Median Indian ransom demand.

- **25% of ransom demands were for $1 million or more,** the lowest of any country, and a considerable drop from the 49% reported in the 2025 report.
- **The median Indian ransom payment was $22,000**, the second-lowest recorded of any country, and a 96% drop from the $510,591 reported in the 2025 report.
- **Indian organizations typically pay 85% of the ransom demand (median)**, compared to the 88% reported in the 2025 report.

Business impact of ransomware

- **Excluding any ransom payments, the average (mean) cost incurred by Indian organizations to recover from a ransomware attack in this year's report came in at $1.11 million**, a slight increase from the $1.01 million mean reported in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **58% of Indian organizations recovered from a ransomware attack in up to a week,** a notable increase from the 48% reported in the 2025 report. 10% took between one and six months to recover, a considerable drop from the 23% in the 2025 report.

Human impact of ransomware on IT/cybersecurity teams in organizations where data was encrypted

45% report increased anxiety or stress about future attacks.

42% report increased recognition from senior leaders.

39% report increased pressure from senior leaders.

39% experienced changes to team/organizational structure.

22% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. More than three-quarters of Indian ransomware victims confirmed their ransomware incident was the same event as their most significant identity attack. Organizations should prioritize identity threat detection and response (ITDR), enforce multi-factor authentication across all access points, and regularly audit both human and non-human identity credentials.

Strengthen endpoint protection for AI frontier models. Frontier AI is accelerating vulnerability discovery and exploitability. Having strong endpoint defenses that automatically block exploit-based attacks is essential.

Prioritize email security. With phishing and malicious email accounting for over half of ransomware root causes in India, organizations should deploy advanced email filtering, implement DMARC/DKIM/SPF protocols, and invest in regular phishing awareness training.

Invest in backup and recovery infrastructure. Organizations that maintained robust backup systems recovered encrypted data at nearly record rates in the past year. Backups should be tested regularly, stored offline or in immutable formats, and integrated into a documented incident response plan that can be executed under pressure.

SOPHOS

To explore how Sophos can help you optimize your ransomware defenses, speak to an advisor or visit **sophos.com/ransomware2026**

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2026-07-28 IN-WP (TA) CRE-6008