SOPHOS

THE STATE OF RANSOMWARE IN MEXICO 2026

Findings from an independent, vendor-agnostic survey of 84 organizations in Mexico that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

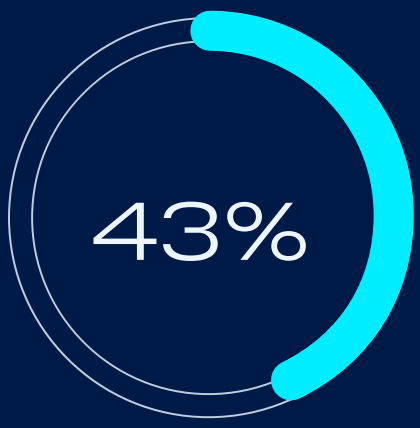
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 84 from Mexico.

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

84

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



Percentage of attacks that resulted in data being encrypted.

Confirmed that this past year's ransomware incident was the same event as their most significant identity attack.

Average cost to recover from a ransomware attack.

Why Mexican organizations fall victim to ransomware

- **Compromised credentials were the most common technical root cause,** used in 39% of attacks — the highest share of any country surveyed — followed by malicious email (24%) and exploited vulnerabilities (18%). Exploited vulnerabilities fell to 18% from 45% in the 2025 report.
- **An unknown security gap (43%) was the most common operational root cause,** followed by a known security gap (38%) and poor quality protection (35%).
- **(NEW) Exposed applications and systems were the most common attack entry point (48%)** for non-email, non-phishing root causes, followed by user devices (26%) and firewalls (14%).
- **(NEW) 67% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.**

What happens to the data

- **43% of attacks resulted in data being encrypted.** This is below the global average of 56% and a drop from the 50% reported by Mexican respondents in the 2025 report.
- **58% of Mexican organizations used backups to recover encrypted data,** a notable drop from the 68% reported in the 2025 report.
- **Data was also stolen in 33% of attacks where data was encrypted,** a considerable drop from the 52% in the 2025 report.
- **100% of Mexican organizations that had data encrypted were able to get it back,** in line with the global average.
- **47% of Mexican organizations paid the ransom and got data back,** a big jump from the 23% in the 2025 report.

Ransom demands

- **The median Mexican ransom demand was $540,000,** a 73% drop from the $2 million in the 2025 report.
- **31% of ransom demands were for $1 million or more,** a considerable drop from the 70% in the 2025 report.

Median Mexican ransom demand.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) recovery cost for Mexican organizations after their ransomware attack was $752,000,** a significant drop from the $1.35 million mean in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **64% of Mexican organizations recovered from a ransomware attack in up to a week,** unchanged from the 64% in the 2025 report. 12% took between one and six months to recover, a slight increase from the 10% in the 2025 report.

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

47% report increased pressure from senior leaders. Up from 32% in 2025.

44% report feelings of guilt that the attack was not stopped. Up from 30% in 2025.

42% report increased anxiety or stress about future attacks. Up from 32% in 2025

39% report an ongoing increase in workload since the attack.

8% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. Nearly two-thirds of Mexican 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 one-third of ransomware root causes in Mexico, 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.

2026-08-03 MX-WP (TA) CRE-6012