SOPHOS

THE STATE OF RANSOMWARE IN MEXICO 2025

Findings from an independent, vendor-agnostic survey of 111 organizations in Mexico that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JUNE 2025

About the report

This report is based on the findings of an independent, vendor-agnostic survey of 3,400 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 111 from Mexico.

The survey was commissioned by Sophos and conducted by a third-party specialist between January and March 2025.

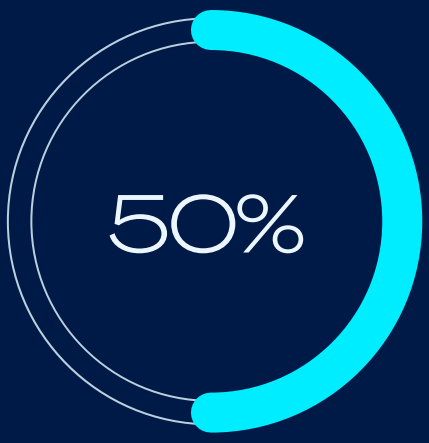
All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

The report includes comparisons with the findings from our 2024 survey. All financial data points are in U.S. dollars.

Survey of

111

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 encypted.

The most common technical root cause of attacks.

Average cost to recover from a ransomware attack.

Why Mexican organizations fall victim to ransomware

- **Exploited vulnerabilities were the most common technical root cause of attack,** used in 45% of attacks. They are followed by compromised credentials, which were the start of 28% of attacks. Malicious emails were used in 13% of attacks.
- **A known security gap was the most common operational root cause,** cited by 47% of Mexican respondents. This was followed by an unknown security gap as reported by 43% of organizations. 40% said that not having the skills or knowledge available to detect and stop the attack in time played a factor in their organization falling victim to ransomware.

What happens to the data

- **50% of attacks resulted in data being encrypted -** this is in line with the global average.
- **Data was also stolen in 52% of attacks where data was encrypted.**
- **All Mexican organizations that had data encrypted were able to get it back,** above the global average.
- **23% of Mexican organizations paid the ransom and got data back,** well below the 49% global average.
- **68% of Mexican organizations used backups to recover encrypted data**.

Ransoms: Demands and payments

- **The median Mexican ransom demand in the last year was $2 million**, well above the $1.32 million global average.

Median Mexican ransom demand in the last year.

- **Close to three quarters (70%) of ransom demands were for $1 million or more**
- 13 respondents from Mexico whose organization paid the ransom shared the amount, revealing a **median ransom payment of $1 million.**
- **Mexican organizations typically pay ALL of the ransom demand,** notably above the global average of 85%.
  - 46% **paid LESS THAN the initial ransom** demand (global average: 53%).
  - 23% **paid THE SAME as the initial ransom** demand (global average: 29%).
  - 31% **paid MORE THAN the initial ransom** demand (global average: 18%).

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) bill incurred by Mexican organizations to recover from a ransomware attack in the last year came in at $1.35 million**, notably below the $1.53 million global average. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **Mexican organizations recover swiftly from ransomware attacks,** with 64% fully recovered in up to a week (well above the 53% global average) and just 10% taking between one and six months to recover.

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

39% say the team's **workload has increased** since the attack.

32% report **increased anxiety or stress** about future attacks.

32% reported **increased pressure** from senior leaders.

30% report **feelings of guilt** that the attack was not stopped.

21% have experienced a **team member absence due to stress/ mental health issues.**

Recommendations

Ransomware remains a major threat to Mexican organizations. As adversaries continue to iterate and evolve their attacks, it's essential that defenders and their cyber defenses keep pace. The learnings from this report indicate key areas for focus in 2025 and beyond.

- **Prevention.** The best ransomware attack is the one that didn't happen because adversaries couldn't get into your organization. Look to reduce both the technical root causes of attack and the operational ones highlighted in this report.
- **Protection.** Strong foundational security is a must. Endpoints (including servers) are the primary destination for ransomware actors, so ensure that they are well defended, including dedicated anti-ransomware protection to stop and roll back malicious encryption.
- **Detection and response.** The sooner you stop an attack, the better your outcomes. Around-the-clock threat detection and response is now an essential layer of defense. If you lack the resources or skills to deliver this in house, look to work with a trusted managed detection and response (MDR) provider.
- **Planning and preparation.** Having an incident response plan that you are well versed in deploying will greatly improve your outcomes if the worst happens and you experience a major attack. Be sure to take good backups and regularly practice recovering from them.

SOPHOS

To explore how Sophos can help you optimize your ransomware defenses, speak to an adviser or visit **sophos.com/ransomware2025**

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.

2025-06-19 MX-WP (DD)