SOPHOS

THE STATE OF RANSOMWARE IN COLOMBIA 2025

Findings from an independent, vendor-agnostic survey of 122 organizations in Colombia 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 122 from Colombia.

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

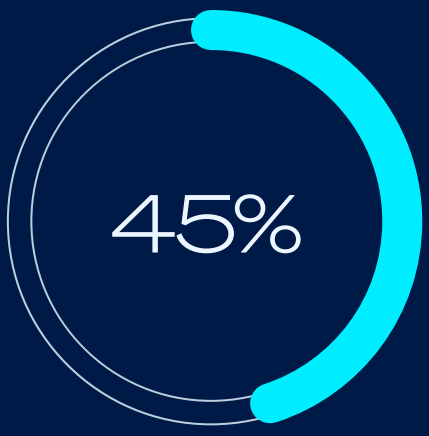
All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

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

Survey of

122

IT/cybersecurity leaders in Colombia 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 Colombian organizations fall victim to ransomware

- **Exploited vulnerabilities were the most common technical root cause of attack,** used in 30% of attacks. They are followed by compromised credentials, which were the start of 27% of attacks. Malicious emails were used in 24% of attacks.
- **Known security gaps** and a **lack of expertise are the two most common operational root causes,** both cited by 43% of Colombian respondents. 41% said that not having the necessary cybersecurity products and services in place played a factor in their organization falling victim to ransomware.

What happens to the data

- **45% of attacks resulted in data being encrypted.** This is slightly below the global average of 50%.
- **Data was also stolen in 18% of attacks where data was encrypted.**
- **98% of Colombian organizations that had data encrypted were able to get it back.**
- **18% of Colombian organizations paid the ransom and got data back,** significantly below the 49% global average.
- **56% of Colombian organizations used backups to recover encrypted data.**

Ransoms: Demands and payments

- 24 respondents from Colombia who had their data encrypted shared the initial ransom demand they received from attackers, revealing a **median ransom demand of $60,000** over the past year.

Median Colombian ransom demand in the last year.

- **63% of ransom demands were for amounts up to $99,999.**
- 10 respondents from Colombia whose organization paid the ransom shared the amount, revealing a **median ransom payment of $40,000.**
- **Colombian organizations typically paid 78% of the ransom demand,** below the global average of 85%.
  - 70% **paid LESS THAN the initial ransom** demand (global average: 53%).
  - 20% **paid THE SAME as the initial ransom** demand (global average: 29%).
  - 10% **paid MORE THAN the initial ransom** demand (global average: 18%).

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) bill incurred by Colombian organizations to recover from a ransomware attack in the last year came in at $0.87 million,** well below the $1.53 million global average. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **Colombian organizations recover from ransomware attacks swiftly,** with 50% fully recovered in up to a week – just below the 53% global average. 25% took between one and six months to recover.

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

45% have experienced a **team member absence** due to stress/ mental health issues.

44% report **feelings of guilt** that the attack was not stopped.

33% say the team's **workload has increased** since the attack.

29% report **increased anxiety or stress** about future attacks.

24% reported **increased pressure** from senior leaders.

Recommendations

Ransomware remains a major threat to Colombian 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 CO-WP (DD)