SOPHOS

THE STATE OF RANSOMWARE IN CHILE 2026

Findings from an independent, vendor-agnostic survey of 48 organizations in Chile 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 48 from Chile.

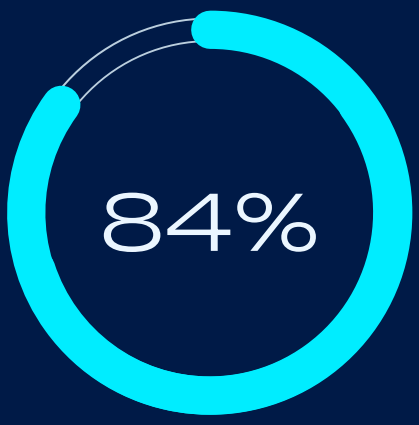
The survey was conducted between January and March 2026. All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months. All financial data points are in U.S. dollars. Outlier ransoms of $40 million or more were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

Survey of

48

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

The most common technical root cause of attacks.



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 Chilean organizations fall victim to ransomware

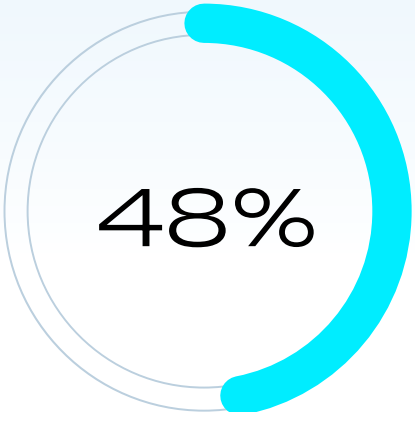
- **Exploited vulnerabilities were the most common technical root cause of attack,** used in 33% of attacks. They were followed by malicious email, which was the start of 31% of attacks. Compromised credentials were used in 21% of attacks. Exploited vulnerabilities dropped sharply, falling to 33% from 46% in the 2025 report.
- **A lack of expertise (52%) was the most common operational root cause,** followed by an unknown security gap (48%) and a lack of people/capacity (48%).
- **(NEW) User devices were the most common attack entry point (52%)** for exploited vulnerabilities, compromised credentials, and brute force attack root causes. Exposed applications and systems (32%) and Firewalls (13%) were the second and third-most common.
- **(NEW) 84% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.** Although not all the attacks resulted in data encryption, this finding establishes identity compromise as a dominant ransomware delivery mechanism.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) recovery cost for Chilean organizations was $1.04 million**, a slight decrease from the $1.2 million mean in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **44% of Chilean organizations recovered from a ransomware attack in up to a week,** a significant reduction from the 65% reported in the 2025 report. 21% took between one and six months to recover, a considerable increase from the 8% in the 2025 report.

What happens to the data

- **48% of attacks resulted in data being encrypted**. This is below the global average of 56% and a drop from the 52% reported by Chilean respondents in the 2025 report.



of attacks resulted in data being encrypted.

Recommendations

Strengthen identity security as a ransomware defense. The vast majority of Chilean 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 one-third of ransomware root causes in Chile, 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 CL-WP (TA) CRE-6013