



THE STATE OF RANSOMWARE IN CHILE 2025

Findings from an independent, vendor-agnostic survey of 122 organizations in Chile that were hit by ransomware in the last year.

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 Chile.

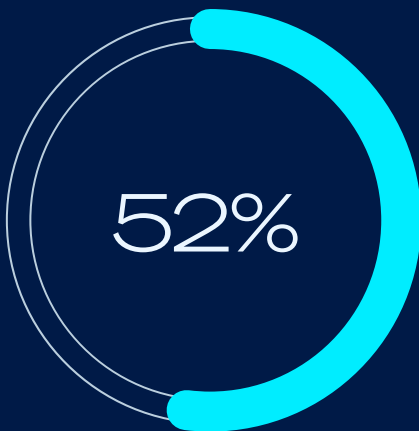
The survey was commissioned by Sophos and conducted by a third-party specialist between January and March 2025.

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 Chile working in organizations that were hit by ransomware in the last year



Percentage of attacks that resulted in data being encrypted.



Median Chilean ransom payment in the last year.



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 46% of attacks. They are followed by compromised credentials, which were the start of 22% of attacks. Malicious emails were used in 20% of attacks.
- ▶ **A known security gap was the most common operational root cause**, cited by 55% of Chilean respondents. This was followed by a lack of expertise reported by 46% of organizations. 44% said that a lack of people/capacity to monitor their systems at the time of the attack played a factor in their organization falling victim to ransomware.

What happens to the data

- ▶ **52% of attacks resulted in data being encrypted.**
- ▶ **Data was also stolen in 17% of attacks where data was encrypted**, significantly below the 28% global average.
- ▶ **97% of Chilean organizations that had data encrypted were able to get it back.**
- ▶ **56% of Chilean organizations paid the ransom and got data back.**
- ▶ **49% of Chilean organizations used backups to recover encrypted data.**

Ransoms: Demands and payments

- ▶ **The median Chilean ransom demand in the last year was \$1 million**, slightly lower than the \$1.32 million global average.
- ▶ **53% of ransom demands were for \$1 million or more.**
- ▶ **The median Chilean ransom payment in the last year was \$675,000**, well below the \$1 million global average.
- ▶ **Chilean organizations typically paid 80% of the ransom demand**, below the global average of 85%.
 - 67% **paid LESS THAN the initial ransom demand** (global average: 53%).
 - 19% **paid THE SAME as the initial ransom demand** (global average: 29%).
 - 14% **paid MORE THAN the initial ransom demand** (global average: 18%).

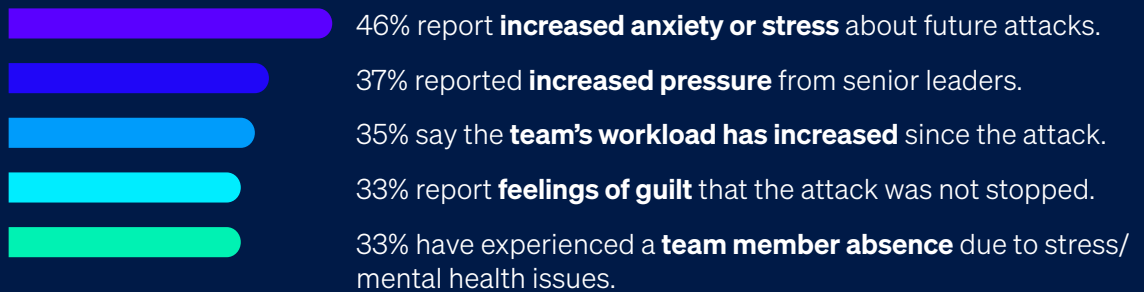


Median Chilean ransom demand in the last year.

Business impact of ransomware

- ▶ Excluding any ransom payments, **the average (mean) bill incurred by Chilean organizations to recover from a ransomware attack in the last year came in at \$1.2 million**, below the \$1.53 million global average. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- ▶ **Chilean organizations recover swiftly from ransomware attacks**, with 65% fully recovered in up to a week, well above the 53% global average. Just 8% took between one and six months to recover, significantly below the 18% global average.

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



Recommendations

Ransomware remains a major threat to Chilean 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.



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.