SOPHOS

THE STATE OF RANSOMWARE IN SPAIN 2025

Findings from an independent, vendor-agnostic survey of 237 organizations in Spain 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 237 from Spain.

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

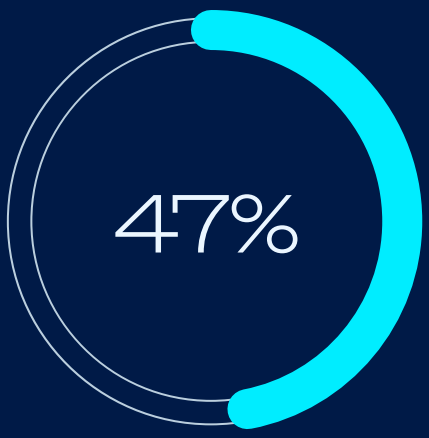
All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

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

Survey of

237

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



Percentage of attacks that resulted in data being encypted.

Median Spanish ransom payment in the last year.

Average cost to recover from a ransomware attack.

Why Spanish 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 21% of attacks. Malicious emails were used in 17% of attacks.
- **A known security gap was the most common operational root cause,** cited by 42% of Spanish respondents. This was followed by a lack of people / capacity cited by 41% of organizations. 39% said that a lack of expertise and an unknown security gap played a factor in their organization falling victim to ransomware.

What happens to the data

- **47% of attacks resulted in data being encrypted.** This is below the global average of 50% but a significant drop from the 89% reported by Spanish respondents in 2024.
- **Data was also stolen in 36% of attacks where data was encrypted,** just above the 34% reported last year.
- **All Spanish organizations that had data encrypted were able to get it back.**
- **36% of Spanish organizations paid the ransom and got data back,** a significant drop from the 56% reported last year.
- **70% of Spanish organizations used backups to recover encrypted data,** a drop from the 73% reported last year.

Ransoms: Demands and payments

- **The median Spanish ransom demand in the last year was $911,600** – less than a quarter of the $4.24 million reported in our 2024 survey.

Median Spanish ransom demand in the last year.

- **50% of ransom demands were for $1 million or more,** down from 73% in 2024.
- **The median Spanish ransom payment in the last year was $322,500** – considerably less than the $4.4 million reported last year.
- **Spanish organizations typically paid 80% of the ransom demand**, below the global average of 85%.
  - 72% **paid LESS THAN the initial ransom** demand (global average: 53%).
  - 28% **paid THE SAME as the initial ransom** demand (global average: 29%).
  - 0% **paid MORE THAN the initial ransom** demand (global average: 18%).

Business impact of ransomware

- Excluding any ransom payments, the **average (mean) bill incurred by Spanish organizations to recover from a ransomware attack in the last year came in at $1.15 million,** a substantial drop from the $3.43 million reported by Spanish respondents in 2024. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **Spanish organizations are getting faster at recovering from a ransomware attack,** with 49% fully recovered in up to a week, an increase from the 27% reported last year. 24% took between one and six months to recover, a notable drop from last year's 45%.

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

36% reported an **ongoing increase in workload.**

33% report **increased anxiety or stress about future attacks.**

28% report **increased pressure** from senior leaders.

27% report **feelings of guilt** that the attack was not stopped.

25% reported staff **absences due to stress/mental health issues.**

Recommendations

Ransomware remains a major threat to Spanish 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 ES-WP (DD)