# SOPHOS

# THE STATE OF RANSOMWARE IN BRAZIL 2025

Findings from an independent, vendor-agnostic survey of 110 organizations in Brazil 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 110 from Brazil.

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
# 110

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

**54%**
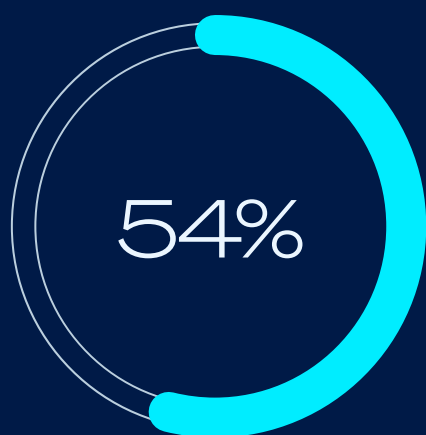
Percentage of attacks that resulted in data being encypted.

**$400K**

Median Brazilian ransom payment in the last year.

**$1.19M**

Average cost to recover from a ransomware attack.

## Why Brazilian organizations fall victim to ransomware

▶ **Exploited vulnerabilities were the most common technical root cause of attack,** used in 44% of attacks. They are followed by compromised credentials, which were the start of 20% of attacks. Malicious emails were used in 18% of attacks.

▶ **A known security gap was the most common operational root cause,** cited by 47% of Brazilian respondents. This was followed by a lack of people/capacity as reported by 39% of organizations. 35% said that a mistake/failure to follow processes properly by their teams played a factor in their organization falling victim to ransomware.

## What happens to the data

▶ **54% of attacks resulted in data being encrypted.** This is above the global average of 50% but a significant drop from the 77% reported by Brazilian respondents in 2024.

▶ **Data was also stolen in 22% of attacks where data was encrypted,** a drop from the 26% reported last year.

▶ **All Brazilian organizations that had data encrypted were able to get it back,** above the global average.

▶ **66% of Brazilian organizations paid the ransom and got data back,** a slight decrease from the 67% reported last year.

▶ **73% of Brazilian organizations used backups to recover encrypted data,** a notable drop from the 81% reported last year.

## Ransoms: Demands and payments

▶ The **median Brazilian ransom demand** in the last year was $392,500, which is a 53% drop from the $840,000 reported in our 2024 survey.

$393K

Median Brazilian ransom demand in the last year.

▶ 40% of **ransom demands were for $1 million or more,** over double the 16% recorded in 2024.

▶ The **median Brazilian ransom payment** in the last year was $400,000, a 52% drop from the $840,000 reported last year.

▶ **Brazilian organizations typically paid** 86% of the ransom demand, in line with the global average of 85%.

   ▪ 55% **paid LESS THAN the initial ransom** demand (global average: 53%).

   ▪ 11% **paid THE SAME as the initial ransom** demand (global average: 29%).

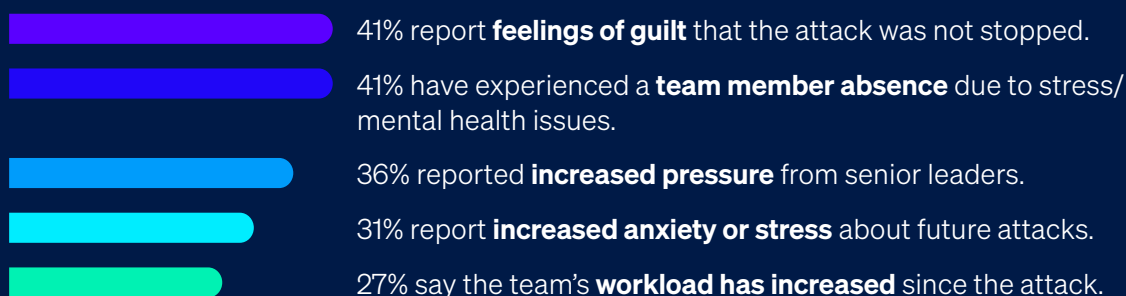   ▪ 34% **paid MORE THAN the initial ransom** demand (global average: 18%).

## Business impact of ransomware

▶ Excluding any ransom payments, the **average (mean) bill incurred by Brazilian organizations to recover from a ransomware attack in the last year came in at $1.19 million,** a drop from the $2.73 million reported by Brazilian respondents in 2024. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.

▶ **Brazilian organizations are getting faster at recovering from a ransomware attack,** with 55% fully recovered in up to a week, a significant increase from the 28% reported last year. 20% took between one and six months to recover, a notable drop from last year's 38%.

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

41% report **feelings of guilt** that the attack was not stopped.

41% have experienced a **team member absence** due to stress/mental health issues.

36% reported **increased pressure** from senior leaders.

31% report **increased anxiety or stress** about future attacks.

27% say the team's **workload has increased** since the attack.

## Recommendations

Ransomware remains a major threat to Brazilian 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.