SOPHOS

THE STATE OF RANSOMWARE IN BRAZIL 2026

Findings from an independent, vendor-agnostic survey of 71 organizations in Brazil that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

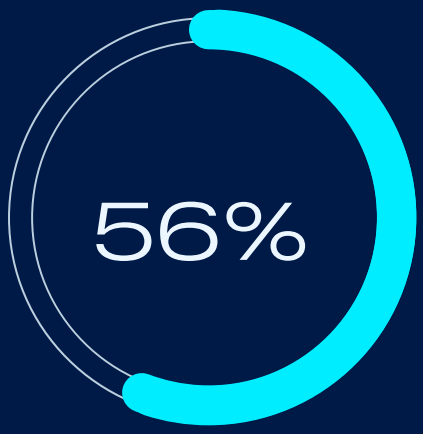
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 71 from Brazil.

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

71

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



Percentage of attacks that resulted in data being encrypted.

Median Brazilian ransom demand.

Average cost to recover from a ransomware attack.

Why Brazilian organizations fall victim to ransomware

- **Malicious emails were the most common technical root cause of attack used in 37% of attacks. This was the highest percentage of malicious email root causes of any country in the study.** They were followed by exploited vulnerabilities (24%) and phishing (18%). Exploited vulnerabilities fell to 24% from 44% in the 2025 report.
- **An unknown security gap (42%) was the most common operational root cause,** followed by a known security gap (39%) and a lack of people/capacity (37%).
- **(NEW) 74% 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.

What happens to the data

- **56% of attacks resulted in data being encrypted.** This is in line with the global average of 56% and an increase from the 54% reported by Brazilian respondents in the 2025 report.
- **Data was also stolen in 38% of attacks where data was encrypted,** up from the 22% in 2025.
- **98% of Brazilian organizations that had data encrypted were able to get it back,** in line with the global average.
- **45% of Brazilian organizations paid the ransom and got data back,** a big drop from the 66% in last year's report.
- **85% of Brazilian organizations used backups to recover encrypted data,** a considerable increase from the 73% reported in the 2025 report.

Ransom demands

- **The median Brazilian ransom demand was $640,000,** a 63% jump from the $392,500 reported in the 2025 report.
- **35% of ransom demands were for $1 million or more,** down from the 41% reported in the 2025 report.

Median Brazilian ransom demand.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) recovery cost for Brazilian organizations after their ransomware attack was $1.05 million,** a slight decrease from the $1.19 million mean in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **58% of Brazilian organizations recovered from a ransomware attack in up to a week,** a slight increase from the 55% reported in the 2025 report. 18% took between one and six months to recover, a small drop from the 20% in the 2025 report.

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

48% report increased anxiety or stress about future attacks. Up from 31% in 2025

43% report increased recognition from senior leaders. Also up from 31% in 2025

43% experienced changes to team/organizational structure.

43% report a change of team priorities/focus.

28% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. Three-quarters of Brazilian 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 over half of ransomware root causes in Brazil, 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.

2026-07-24 BR-WP (TA) CRE-6010