SOPHOS

# THE STATE OF RANSOMWARE IN ITALY 2026

Findings from an independent, vendor-agnostic survey of 171 organizations in Italy that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

# About the report

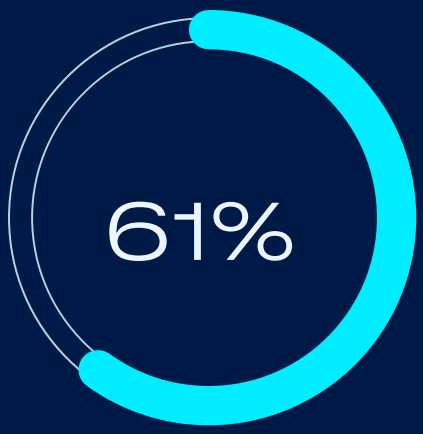
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 171 from Italy.

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.

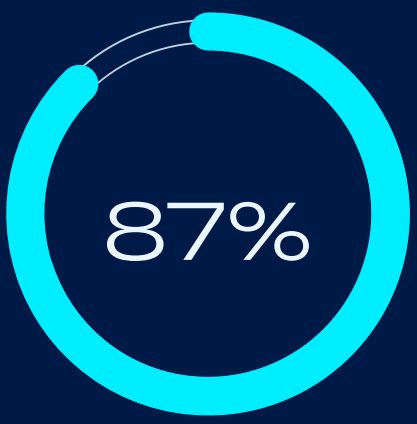
Survey of

**171**

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




Percentage of attacks that resulted in data being encrypted.




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 Italian organizations fall victim to ransomware

- **Exploited vulnerabilities were the most common technical root cause of attack,** used in 27.5% of attacks, followed by malicious email (26.9%) and phishing (22%). Exploited vulnerabilities dropped to 27.5% from 35% in the 2025 report.
- **An unknown security gap (37.4%) was the most common operational root cause,** followed by a lack of expertise (36.8%) and human error (36%).
- **(NEW) User devices were the most common attack entry point (44%)** for non-email, non-phishing root causes, followed by exposed applications and systems (29%) and VPNs (12%).
- **(NEW) 87% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.** Much higher than the global average of 67%, and the highest overlap of any country.

## What happens to the data

- **61% of attacks resulted in data being encrypted.** This is above the global average of 56% and an increase from the 55% reported by Italian respondents in the 2025 report.
- **47% of Italian organizations paid the ransom and got data back,** a considerable increase from the 27% reported in last year's report.
- **98% of Italian organizations that had data encrypted were able to get it back,** in line with the global average.
- **Data was also stolen in 23% of attacks where data was encrypted,** up from the 11% reported in 2025.
- **65% of Italian organizations used backups to recover encrypted data,** a notable increase from the 58% reported in the 2025 report.

## Ransoms: Demands and payments

- **The median Italian ransom demand was $1 million,** a 76% drop from the $4.12 million reported in the 2025 report.


Median Italian ransom payment.

- **48% of ransom demands were for $1 million or more,** a considerable drop from the 68% reported in the 2025 report.
- **The median Italian ransom payment was $1.14 million,** a 51% drop from the $2.32 million reported in the 2025 report.
- **Italian organizations typically pay 97% of the ransom demand (median),** compared to the 97% reported in the 2025 report.

## Business impact of ransomware

- Excluding any ransom payments, **the average (mean) cost incurred by Italian organizations to recover from a ransomware attack in this year's report came in at $2.07 million,** a significant drop from the $3.55 million mean reported in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **64% of Italian organizations recovered from a ransomware attack in up to a week,** a considerable increase from the 46% reported in the 2025 report. 17% took between one and six months to recover, a notable drop from the 26% in the 2025 report.

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

**39% report increased pressure from senior leaders.**

**36% report increased recognition from senior leaders.**

**36% report a change of team priorities/focus.**

**30% experienced changes to team/organizational structure.** Down from 39% in 2025.

**20% report that the team's leadership has been replaced.**

## Recommendations

**Strengthen identity security as a ransomware defense.** The vast majority of Italian 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 nearly half of ransomware root causes in Italy, 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.



2026-08-05 IT-WP (TA) CRE-6009