SOPHOS

THE STATE OF RANSOMWARE IN FRANCE 2026

Findings from an independent, vendor-agnostic survey of 129 organizations in France that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

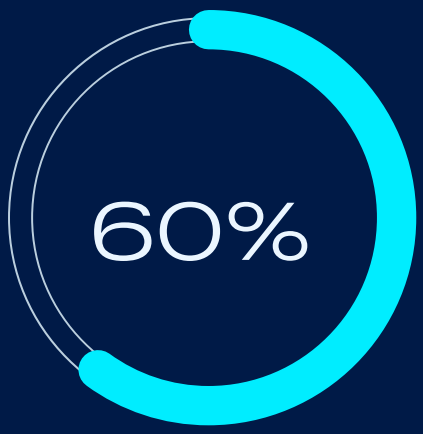
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 129 from France.

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.

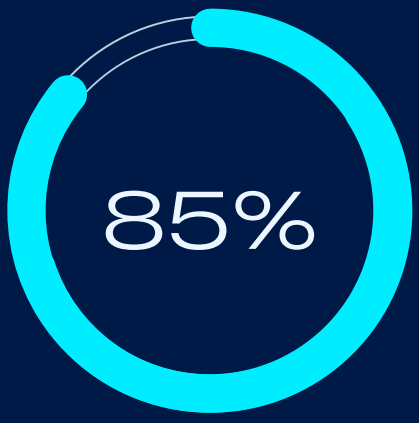
Survey of

129

IT/cybersecurity leaders in France 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 French organizations fall victim to ransomware

- **Compromised credentials were the most common technical root cause of attack,** used in 30% of attacks, followed by phishing (27%) and malicious email (20%). Exploited vulnerabilities dropped sharply, falling to 13% from 30% in the 2025 report.
- **(NEW) 85% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.** This was significantly higher than the global average of 67%.
- **(NEW) Exposed applications and systems were the most common attack entry point (46%)** for non-email, non-phishing root causes, followed by user devices (22%) and VPNs (15%). France had the highest percentage of VPN-based attack entries of any country surveyed.
- **A lack of people/capacity (40%) was the most common operational root cause,** followed by a lack of protection (38%) and a lack of expertise (33%).

What happens to the data

- **60% of attacks resulted in data being encrypted.** This is above the global average of 56% and an increase from the 58% reported by French respondents in the 2025 report.
- **Data was also stolen in 18% of attacks where data was encrypted,** a considerable drop from the 44% reported in 2025.
- **100% of French organizations that had data encrypted were able to get it back,** in line with the global average.
- **36% of French organizations paid the ransom and got data back,** a slight increase from the 33% reported in last year's report.
- **76% of French organizations used backups to recover encrypted data,** a considerable increase from the 60% reported in the 2025 report.

Ransom demands

- **The median French ransom demand was $500,000,** a 22% drop from the $643,125 reported in the 2025 report.
- **39% of ransom demands were for $1 million or more,** down from the 49% reported in the 2025 report.

Median French ransom demand.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) cost incurred by French organizations to recover from a ransomware attack in this year's report came in at $2.02 million,** a significant increase from the $1.22 million mean reported in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **64% of French organizations recovered from a ransomware attack in up to a week,** a considerable increase from the 53% reported in the 2025 report. 10% took between one and six months to recover, a notable drop from the 18% in the 2025 report.

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

42% report increased pressure from senior leaders.

37% report increased recognition from senior leaders. Up from 18% in 2025.

33% report an ongoing increase in workload since the attack.

31% report feelings of guilt that the attack was not stopped.

17% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. The vast majority of French 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 France, 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.

2026-08-03 FR-WP (TA) CRE-6006