SOPHOS

THE STATE OF RANSOMWARE IN THE U.S. 2026

Findings from an independent, vendor-agnostic survey of 377 organizations in the United States of America that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

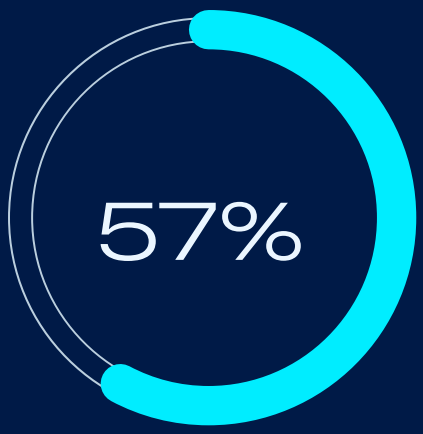
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 377 from the U.S.

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

377

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



Percentage of attacks that resulted in data being encrypted.

Median U.S. ransom payment.

Average cost to recover from a ransomware attack.

Why U.S. organizations fall victim to ransomware

- **Phishing was the most common technical root cause of attack**, used in 27% of incidents, followed by malicious email (26%), and compromised credentials (22%). Exploited vulnerabilities fell to 16% from 27% in the 2025 report.
- **Human error (40%) was the most common operational root cause**, followed by a lack of protection (38%) and known security gap (37%).
- **(NEW) Exposed applications and systems were the most common attack entry point (36%)** for non-email, non-phishing root causes, followed by user devices (34%) and firewalls (23%).
- **(NEW) 69% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.**

What happens to the data

- **57% of attacks resulted in data being encrypted.** This is slightly above the global average of 56% and an increase from the 51% reported by U.S. respondents in the 2025 report.
- **Data was also stolen in 28% of attacks where data was encrypted,** in line with the 29% reported in 2025.
- **98% of U.S. organizations that had data encrypted were able to get it back,** in line with the global average.
- **56% of U.S. organizations paid the ransom and got data back,** up from 53% in last year's report.
- **60% of U.S. organizations used backups to recover encrypted data,** up significantly from the 43% reported in 2025.

Ransoms: Demands and payments

- **The median U.S. ransom demand was $1 million,** a 50% drop from the $2 million reported in the 2025 report.

Median U.S. ransom demand.

- **55% of ransom demands were for $1 million or more**, down from the 65% reported in last year's report.
- **The median U.S. ransom payment was $1 million,** a 26% drop from the $1.35 million reported in the 2025 report.
- **33% of U.S. organizations paid less than the ransom demand** while 20% paid more.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) cost incurred by U.S. organizations to recover from a ransomware attack is now $2.51 million** up from $1.91 million reported in 2025. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **U.S. organizations show a bimodal recovery pattern**, with 53% fully recovered in up to a week (up slightly from 51% in the 2025 report). However, 24% took between one and six months to recover, up from 20% in the 2025 report — indicating a widening gap between organizations with strong recovery capabilities and those that struggle.

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

52% report increased anxiety or stress about future attacks. Up from 44% in the last report.

39% report increased pressure from senior leaders.

36% experienced changes to team/organizational structure.

35% report feelings of guilt that the attack was not stopped.

18% report that the team's leadership has been replaced. Down from 25% in 2025.

Recommendations

Strengthen identity security as a ransomware defense. Nearly two-thirds of U.S. 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 the U.S., 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.

2026-07-22 US-WP (NP)