SOPHOS

THE STATE OF RANSOMWARE IN THE U.S. 2025

Findings from an independent, vendor-agnostic survey of 546 organizations in the United States of America that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JUNE 2025

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 546 from the U.S.

The survey was commissioned by Sophos and conducted by a third-party specialist between January and March 2025.

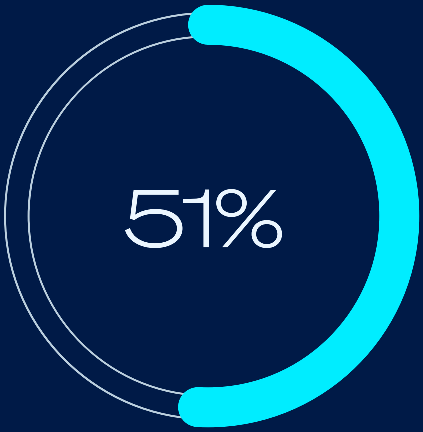
All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

The report includes comparisons with the findings from our 2024 survey. All financial data points are in U.S. dollars.

Survey of

546

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 encypted.

$1.50M

Median U.S. ransom payment in the last year.

$1.91M

Average cost to recover from a ransomware attack.

Why U.S. organizations fall victim to ransomware

- Exploited vulnerabilities were the most common **technical root cause of attack,** used in 27% of attacks. They are closely followed by phishing emails, which were the start of 26% of attacks. Compromised credentials were used in 23% of attacks.
- An unknown security gap and a lack of protection are the two most common **operational root causes,** both cited by 39% of U.S. respondents. 38% said that a lack of people/capacity monitoring their systems at the time of the attack was a factor in their organization falling victim to ransomware.

What happens to the data

- **51% of attacks resulted in data being encrypted.** This is in line with the global average of 50% and a drop from the 58% reported by U.S. respondents in 2024.
- **Data was also stolen in 29% of attacks where data was encrypted,** a notable drop from the 39% reported last year.
- **97% of U.S. organizations that had data encrypted were able to get it back,** in line with the global average.
- **53% of U.S. organizations paid the ransom and got data back,** down from 62% last year.
- **43% of U.S. organizations used backups to recover encrypted data,** a considerable drop from the 61% reported last year.

Ransoms: Demands and payments

- The **median U.S. ransom demand** in the last year was $2 million, which is a drop of one third from the $3 million reported in our 2024 survey.

$2.0M

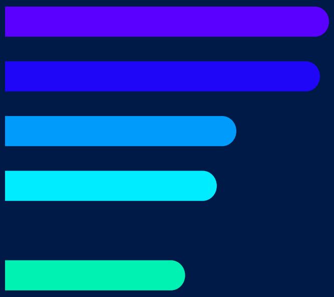
Median U.S. ransom demand in the last year.

- 65% of **ransom demands were for $1 million or more,** down from 81% in 2024.
- The **median U.S. ransom payment** in the last year was $1.5 million, a 50% drop from the $3 million reported last year.
- **U.S. organizations typically paid** 87% of the ransom demand, slightly above the global average of 85%.
  - 53% **paid LESS THAN the initial ransom** demand (global average: 53%).
  - 23% **paid THE SAME as the initial ransom** demand (global average: 29%).
  - 24% **paid MORE THAN the initial ransom** demand (global average: 18%).

Business impact of ransomware

- Excluding any ransom payments, the **average (mean) bill incurred by U.S. organizations to recover from a ransomware attack in the last year came in at $1.91 million**, a drop of one million dollars from the $2.91 million reported by U.S. respondents in 2024. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **U.S. organizations are getting faster at recovering from a ransomware attack**, with 51% fully recovered in up to a week, an increase from the 36% reported last year. 20% took between one and six months to recover, a notable drop from last year's 35%.

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



45% say the team's **workload has increased** since the attack.

44% report **increased anxiety or stress** about future attacks.

32% report **feelings of guilt** that the attack was not stopped.

29% have experienced a **team member absence** due to stress/mental health issues.

25% report that the team's **leadership has been replaced**.

Recommendations

Ransomware remains a major threat to U.S. 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.

2025-06-19 US-WP (DD)