SOPHOS

THE STATE OF RANSOMWARE IN JAPAN 2025

Findings from an independent, vendor-agnostic survey of 207 organizations in Japan 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 207 from Japan.

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

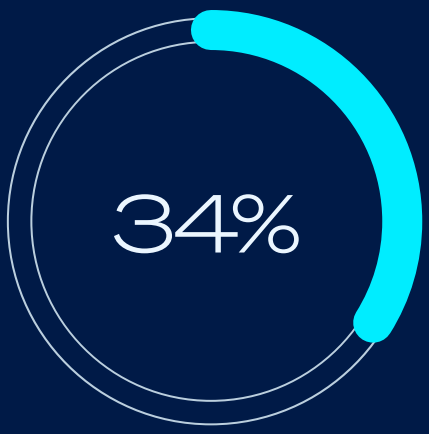
All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

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

Survey of

207

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



Percentage of attacks that resulted in data being encypted.

Median Japanese ransom payment in the last year.

Average cost to recover from a ransomware attack.

Why Japanese organizations fall victim to ransomware

- **Exploited vulnerabilities and compromised credentials were the most common technical root causes of attack,** both cited by 26% of Japanese respondents. They are followed by phishing which was the start of 22% of attacks.
- **A lack of expertise was the most common operational root cause,** cited by 50% of Japanese respondents. This was followed by poor quality protection cited by 45% of organizations. 44% said that a lack of protection played a factor in their organization falling victim to ransomware.

What happens to the data

- **34% of attacks resulted in data being encrypted.** This is well below both the global average of 50% and the 76% reported by Japanese respondents in 2024.
- **Data was also stolen in 21% of attacks where data was encrypted,** below the 26% reported last year.
- **97% of Japanese organizations that had data encrypted were able to get it back,** in line with the global average.
- **70% of Japanese organizations paid the ransom and got data back,** an increase from the 60% reported last year.
- **59% of Japanese organizations used backups to recover encrypted data,** a drop from the 68% reported last year.

Ransoms: Demands and payments

- **The median Japanese ransom demand in the last year was $1 million** – a substantial increase from the $85,200 reported in our 2024 survey.

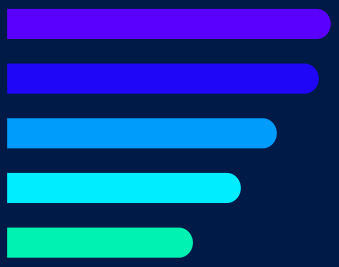
Median Japanese ransom demand in the last year.

- **53% of ransom demands were for $1 million or more.**
- **The median Japanese ransom payment in the last year was $500,000** – a considerable increase from $99,400 reported last year.
- **Japanese organizations typically paid 68% of the ransom demand,** below the global average of 85%.
  - 67% **paid LESS THAN the initial ransom** demand (global average: 53%).
  - 25% **paid THE SAME as the initial ransom** demand (global average: 29%).
  - 8% **paid MORE THAN the initial ransom** demand (global average: 18%).

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) bill incurred by Japanese organizations to recover from a ransomware attack in the last year came in at just $0.67 million,** a substantial decrease from the $2.93 million reported by Japanese respondents in 2024. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **Japanese organizations are getting faster at recovering from a ransomware attack,** with 50% fully recovered in up to a week, an increase from the 27% reported last year. Just 16% took between one and six months to recover, a drop from last year's 36%.

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



54% report **feelings of guilt** that the attack was not stopped.

52% reported a **change of team priorities/focus.**

45% reported **increased pressure** from senior leaders.

39% report **increased anxiety or stress** about future attacks.

31% reported an **ongoing increase in workload.**

Recommendations

Ransomware remains a major threat to Japanese 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 JA-WP (DD)