SOPHOS

THE STATE OF RANSOMWARE IN JAPAN 2026

Findings from an independent, vendor-agnostic survey of 152 organizations in Japan that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

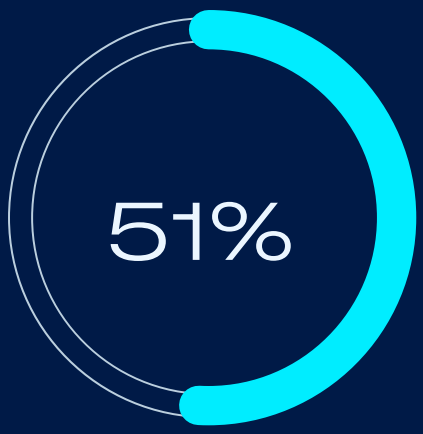
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 152 from Japan.

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

152

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 encrypted.

Median Japanese ransom payment.

Average cost to recover from a ransomware attack.

Why Japanese organizations fall victim to ransomware

- **Phishing was the most common technical root cause of attack,** used in 26.3% of attacks, followed by malicious email (25.7%) and compromised credentials (25%). Exploited vulnerabilities dropped sharply to 14% from 26% in the 2025 report.
- **A lack of expertise (39%) was the most common operational root cause,** followed by an unknown security gap and a known security gap, tied at 37% each.
- **(NEW) Exposed applications and systems were the most common attack entry point (38%)** for non-email, non-phishing root causes, followed by firewalls (25%) and user devices (16%).
- **(NEW) 74% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.**

What happens to the data

- **51% of attacks resulted in data being encrypted.** This is below the global average of 56% and an increase from the 34% reported by Japanese respondents in the 2025 report.
- **Data was also stolen in 36% of attacks where data was encrypted,** up from the 21% in the 2025 report.
- **96% of Japanese organizations that had data encrypted were able to get it back,** in line with the global average.
- **51% of Japanese organizations paid the ransom and got data back**, a considerable drop from the 70% in the 2025 report.
- **58% of Japanese organizations used backups to recover encrypted data,** a slight drop from the 59% in the 2025 report.

Ransoms: Demands and payments

- **The median Japanese ransom demand was $1.75 million,** a 75% jump from the $1 million reported in the 2025 report.

Median Japanese ransom demand.

- **61% of ransom demands were for $1 million or more,** up from the 53% in the 2025 report.
- **The median Japanese ransom payment was $3 million,** a substantial increase from the $525,000 reported in the 2025 report.
- **Japanese organizations typically pay 100% of the ransom demand (median),** compared to the 68% in the 2025 report.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) recovery cost for Japanese organizations after their ransomware attack was $1.88 million,** a substantial increase from the $0.67 million mean in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **52% of Japanese organizations recovered from a ransomware attack in up to a week,** a slight increase from the 50% in the 2025 report. 23% took between one and six months to recover, a notable increase from the 16% in the 2025 report.

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

42% report an ongoing increase in workload since the attack. Up from 31% in 2025.

41% report increased anxiety or stress about future attacks.

38% have experienced staff absence due to stress/mental health issues.

32% report increased pressure from senior leaders.

23% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. More than three-quarters of Japanese 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 Japan, 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.

2026-07-28 JP-WP (TA) CRE-6011