SOPHOS

THE STATE OF RANSOMWARE IN AUSTRALIA 2026

Findings from an independent, vendor-agnostic survey of 119 organizations in Australia that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

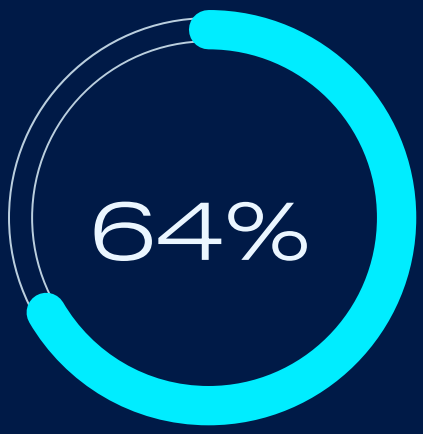
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 119 from Australia.

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

119

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



Percentage of attacks that resulted in data being encrypted.

Median Australian ransom payment.

Average cost to recover from a ransomware attack.

Why Australian organizations fall victim to ransomware

- **Phishing was the most common technical root cause of attack,** used in 24.4% of attacks, followed by malicious email (23.5%) and exploited vulnerabilities (also 23.5%). Exploited vulnerabilities dropped to 24% from 28% in the 2025 report.
- **A lack of people/capacity (45%) was the most common operational root cause,** followed by a known security gap (39%) and human error (35%).
- **(NEW) Exposed applications and systems were the most common attack entry point (43%)** for non-email, non-phishing root causes, followed by firewalls (28%) and User devices (24%).
- **(NEW) 77% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.**

What happens to the data

- **64% of attacks resulted in data being encrypted.** This is above the global average of 56% and an increase from the 33% reported by Australian respondents in the 2025 report.
- **Data was also stolen in 25% of attacks where data was encrypted,** a drop from the 35% in 2025.
- **99% of Australian organizations that had data encrypted were able to get it back,** in line with the global average.
- **57% of Australian organizations paid the ransom and got data back,** up from the 41% in last year's report.
- **57% of Australian organizations also used backups to recover encrypted data,** a drop from the 67% reported in the 2025 report.

Ransoms: Demands and payments

- **The median Australian ransom demand was $1.34 million,** a substantial increase from the $217,000 reported in the 2025 report.

Median Australian ransom demand.

- **49% of ransom demands were for $1 million or more,** up from the 37% reported in the 2025 report.
- **The median Australian ransom payment was $855,000,** a major increase from the $186,000 reported in the 2025 report.
- **Australians paid 73% of the ransom demand (median),** compared to the 88% reported in the 2025 report.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) recovery cost for Australian organizations from their ransomware attack was $1.66 million**, a significant increase from the $0.65 million mean in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **50% of Australian organizations recovered from a ransomware attack in up to a week,** a slight increase from the 47% reported in the 2025 report. 16% took between one and six months to recover, a slight increase from the 13% in the 2025 report.

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

38% report increased anxiety or stress about future attacks. Down from 48% in 2025.

38% report increased pressure from senior leaders. Also down from 48% in 2025.

36% have experienced staff absence due to stress/mental health issues.

33% report increased recognition from senior leaders.

22% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. More than three-quarters of Australian 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 Australia, 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.

2026-07-24 AU-WP (NP)