

THE STATE OF RANSOMWARE IN AUSTRALIA 2025

Findings from an independent, vendor-agnostic survey of 191 organizations in Australia that were hit by ransomware in the last year.

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 191 from Australia.

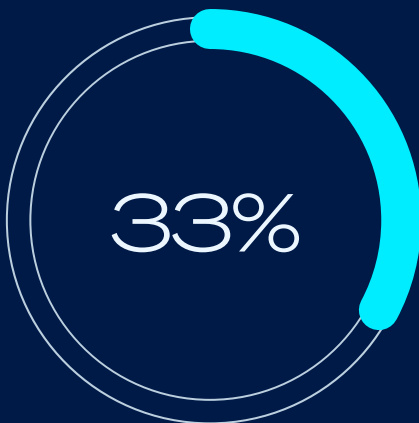
The survey was commissioned by Sophos and conducted by a third-party specialist between January and March 2025.

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
191

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 in the last year.



Average cost to recover from a ransomware attack.

Why Australian organizations fall victim to ransomware

- ▶ **Exploited vulnerabilities were the most common technical root cause of attack**, used in 28% of attacks. They are followed by phishing which was the start of 24% of attacks. Compromised credentials were used in 21% of attacks.
- ▶ **A lack of protection was the most common operational root cause**, cited by 45% of Australian respondents. This was followed by a lack of people/capacity cited by 44% of organizations. 41% said that both known and unknown security gaps played a factor in their organization falling victim to ransomware.

What happens to the data

- ▶ **33% of attacks resulted in data being encrypted**. This is well below both the global average of 50% and the 49% reported by Australian respondents in 2024.
- ▶ **Data was also stolen in 35% of attacks where data was encrypted**, above the 20% reported last year.
- ▶ **98% of Australian organizations that had data encrypted were able to get it back**, above the global average.
- ▶ **41% of Australian organizations paid the ransom and got data back**, a considerable decrease from the 66% reported last year.
- ▶ **67% of Australian organizations used backups to recover encrypted data**, a drop from the 72% reported last year.

Ransoms: Demands and payments

- ▶ **The median Australian ransom demand in the last year was \$217,000** – a substantial drop from the \$4.42 million reported in our 2024 survey.
- ▶ **47% of ransom demands were for \$250,000 or more.**
- ▶ 26 respondents from Australia whose organization paid the ransom shared the amount, revealing a **median ransom payment of \$350,000.**
- ▶ **Australian organizations typically paid 88% of the ransom demand**, just above the global average of 85%.
 - 52% **paid LESS THAN** the initial ransom demand (global average: 53%).
 - 24% **paid THE SAME** as the initial ransom demand (global average: 29%).
 - 24% **paid MORE THAN** the initial ransom demand (global average: 18%).



Median Australian ransom demand in the last year.

Business impact of ransomware

- ▶ Excluding any ransom payments, **the average (mean) bill incurred by Australian organizations to recover from a ransomware attack in the last year came in at just \$0.65 million**, a substantial decrease from the \$2.37 million reported by Australian respondents in 2024. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- ▶ **Australian organizations are getting faster at recovering from a ransomware attack**, with 47% fully recovered in up to a week, an increase from the 36% reported last year. Just 13% took between one and six months to recover, a drop from last year's 33%.

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



Recommendations

Ransomware remains a major threat to Australian 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.



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.