SOPHOS

THE STATE OF RANSOMWARE IN SINGAPORE 2025

Findings from an independent, vendor-agnostic survey of 90 organizations in Singapore 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 90 from Singapore.

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

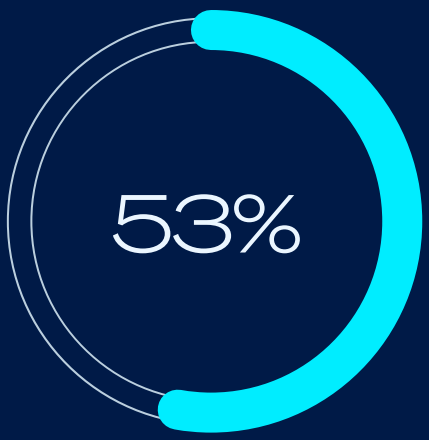
All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

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

Survey of

90

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



Percentage of attacks that resulted in data being encypted.

The most common technical root cause of attacks.

Average cost to recover from a ransomware attack.

Why Singaporean organizations fall victim to ransomware

- **Phishing was the most common technical root cause of attack,** cited by 36% of Singaporean respondents. This is followed by malicious emails which were the start of 29% of attacks. 17% said that compromised credentials were the root cause of the attack.
- **A lack of protection was the most common operational root cause,** cited by 47% of Singaporean respondents. This was followed by a lack of people / capacity cited by 43% of organizations. 39% reported that the inability of their cybersecurity products and services to prevent the attack contributed to their organization falling victim to ransomware.

What happens to the data

- **53% of attacks resulted in data being encrypted.** This is above the global average of 50% and the 50% reported by Singaporean respondents in 2024.
- **Data was also stolen in 10% of attacks where data was encrypted,** below the 25% reported last year.
- **All Singaporean organizations that had data encrypted were able to get it back.**
- **50% of Singaporean organizations paid the ransom and got data back,** a decrease from the 63% reported last year.
- **46% of Singaporean organizations used backups to recover encrypted data,** a drop from the 58% reported last year.

Ransoms: Demands and payments

- **The median Singaporean ransom demand in the last year was $365,565** – a substantial decrease from the $760,000 reported in our 2024 survey.

Median Singaporean ransom demand in the last year.

- **58% of ransom demands were between $10,000 and $499,999.**
- 24 respondents from Singapore whose organization paid the ransom shared the amount, revealing a **median ransom payment of $365,565.**
- **Singaporean organizations typically paid 94% of the ransom demand,** above the global average of 85%.
  - 39% **paid LESS THAN the initial ransom** demand (global average: 53%).
  - 35% **paid THE SAME as the initial ransom** demand (global average: 29%).
  - 26% **paid MORE THAN the initial ransom** demand (global average: 18%).

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) bill incurred by Singaporean organizations to recover from a ransomware attack in the last year came in at just $1.54 million**, a notable decrease from the $2.20 million reported by Singaporean respondents in 2024. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **Singaporean organizations are getting slower at recovering from a ransomware attack,** with 53% fully recovered in up to a week, a decrease from the 77% reported last year. 22% took between one and six months to recover, an increase from last year's 14%.

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

52% reported **increased pressure** from senior leaders.

46% reported a **change of team priorities / focus.**

46% reported an **ongoing increase in workload.**

42% report **increased anxiety or stress** about future attacks.

25% report **feelings of guilt** that the attack was not stopped.

Recommendations

Ransomware remains a major threat to Singaporean 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 SG-WP (DD)