SOPHOS

THE STATE OF RANSOMWARE IN SOUTH AFRICA 2025

Findings from an independent, vendor-agnostic survey of 154 organizations in South Africa 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 154 from South Africa.

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

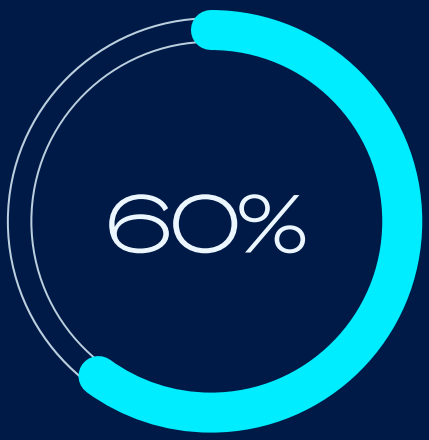
All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

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

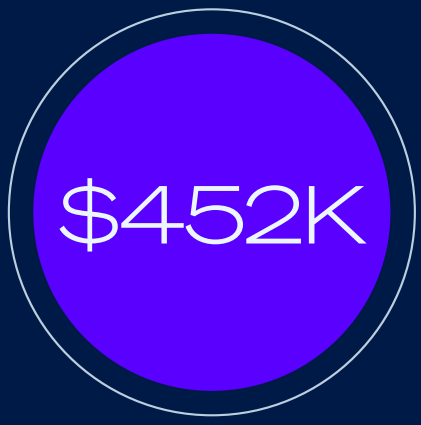
Survey of

154

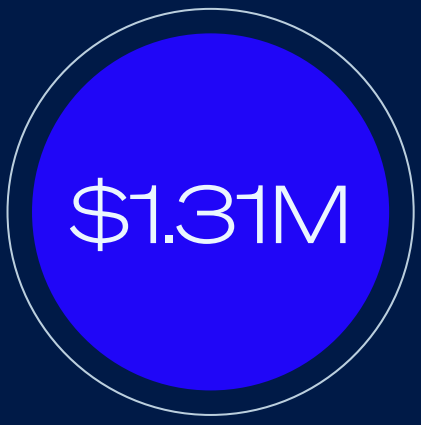
IT/cybersecurity leaders in South Africa working in organizations that were hit by ransomware in the last year



Percentage of attacks that resulted in data being encypted.



Median South African ransom payment in the last year.



Average cost to recover from a ransomware attack.

Why South African organizations fall victim to ransomware

- **Compromised credentials were the most common technical root cause of attack,** used in 34% of attacks. They are followed by exploited vulnerabilities which were the start of 28% of attacks. Malicious emails were used in 22% of attacks.
- **A lack of expertise was the most common operational root cause,** cited by 58% of South African respondents. This was followed by a lack of protection cited by 55% of organizations. 53% said that a weakness in their defenses that they were not aware of played a factor in their organization falling victim to ransomware.

What happens to the data

- **60% of attacks resulted in data being encrypted.** This is above the global average of 50% but a significant drop from the 76% reported by South African respondents in 2024.
- **Data was also stolen in 39% of attacks where data was encrypted,** just above the 35% reported last year.
- **90% of South African organizations that had data encrypted were able to get it back,** below the global average.
- **71% of South African organizations paid the ransom and got data back,** a considerable increase from the 43% reported last year.
- **35% of South African organizations used backups to recover encrypted data,** a significant drop from the 72% reported last year.

Ransoms: Demands and payments

- **The median South African ransom demand in the last year was $1 million** – a considerable increase over the $165,000 reported in our 2024 survey.

Median South African ransom demand in the last year.

- **49% of ransom demands were for $1 million or more.**
- **The median South African ransom payment in the last year was $451,818** – nearly triple the $152,000 reported last year.
- **South African organizations typically paid 64% of the ransom demand,** well below the global average of 85%.
  - 60% **paid LESS THAN the initial ransom** demand (global average: 53%).
  - 35% **paid THE SAME as the initial ransom** demand (global average: 29%).
  - 4% **paid MORE THAN the initial ransom** demand (global average: 18%).

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) bill incurred by South African organizations to recover from a ransomware attack in the last year came in at $1.31 million**, a small increase from the $1.04 million reported by South African respondents in 2024. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **South African organizations are getting faster at recovering from a ransomware attack,** with 47% fully recovered in up to a week, an increase from the 41% reported last year. 19% took between one and six months to recover, a drop from last year's 26%.

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

76% reported **increased pressure** from senior leaders.

47% report **increased anxiety or stress** about future attacks.

42% reported an **ongoing increase in workload.**

37% reported a **change of team priorities / focus.**

29% report **feelings of guilt** that the attack was not stopped.

Recommendations

Ransomware remains a major threat to South African 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 ZA-WP (DD)