SOPHOS

THE STATE OF RANSOMWARE IN SOUTH AFRICA 2026

Findings from an independent, vendor-agnostic survey of 135 organizations in South Africa that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

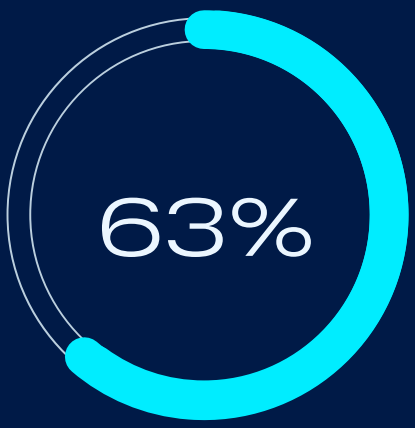
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 135 from South Africa.

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.

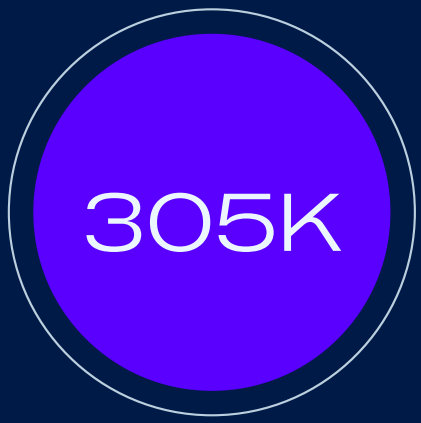
Survey of

135

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 encrypted.



Median South African ransom payment.

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 27% of attacks, followed by exploited vulnerabilities (25%, down from 28% in the 2025 report) and malicious email (22%).
- **A lack of protection (47%) was the most common operational root cause,** the highest of any country surveyed, followed by a lack of people/capacity (43%) and a known security gap (42%).
- **(NEW) User devices were the most common attack entry point (43%)** for non-email, non-phishing root causes, followed by exposed applications and systems (38%) and firewalls (13%).
- **(NEW) 85% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.** This was significantly higher than the global average of 67%.

What happens to the data

- **63% of attacks resulted in data being encrypted.** This is above the global average of 56% and an increase from the 60% reported by South African respondents in the 2025 report.
- **58% of South African organizations paid the ransom and got data back,** a considerable drop from the 71% in the 2025 report.
- **99% of South African organizations that had data encrypted were able to get it back,** in line with the global average.
- **Data was also stolen in 27% of attacks where data was encrypted,** a drop from the 39% in the 2025 report.
- **54% of South African organizations used backups to recover encrypted data,** a considerable increase from the 35% in the 2025 report.

Ransoms: Demands and payments

- **The median South African ransom demand was $427,000,** a 57% drop from the $1 million reported in the 2025 report.

Median South African ransom demand.

- **33% of ransom demands were for $1 million or more** a considerable drop from the 49% in the 2025 report.
- **The median South African ransom payment was $305,000,** a 28% drop from the $425,241 reported in the 2025 report.
- **South African organizations typically pay 71% of the ransom demand (median),** the lowest of any country surveyed, compared to the 64% in the 2025 report.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) recovery cost for South African organizations after their ransomware attack was $1.08 million,** a drop from the $1.31 million mean in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **40% of South African organizations recovered from a ransomware attack in up to a week,** the lowest of any country surveyed and a notable drop from the 47% in the 2025 report. 13% took between one and six months to recover, a sizeable drop from the 19% in the 2025 report.

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

52% report increased pressure from senior leaders.

42% report increased recognition from senior leaders.

39% experienced changes to team/organizational structure.

36% report increased anxiety or stress about future attacks.

24% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. The vast majority of South African 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 over one-third of ransomware root causes in South Africa, 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.

2026-08-04 ZA-WP (TA) CRE-6081