SOPHOS

The State of Ransomware in South Africa 2024

Findings from an independent, vendor-agnostic, survey of 330 IT professionals in mid-sized organizations in South Africa.

A Sophos Whitepaper. April 2024

About the survey

Sophos commissioned an independent, vendor-agnostic survey of 5,000 IT/cybersecurity leaders in mid-sized organizations (100-5,000 employees) across 14 countries, including 330 respondents in South Africa. The survey was conducted between January and February 2024, and respondents were asked to respond based on their experiences in the previous 12 months. All financial data points are in U.S. dollars.

Key findings

- **69% of South African organizations were hit by ransomware in the last year**. This is a decrease on the 78% reported in our 2023 survey but a substantial increase on the 51% reported in 2022. By comparison, globally, 59% of respondents said their organization had experienced a ransomware attack in the last twelve months.
- **46% of computers were impacted, on average, in the attack**, below the global average of 49%.
- **Malicious email was the most common root cause of attack** for South African organizations, used in 32% of incidents. Compromised credentials were the second most frequent attack vector, used in 26% of attacks.
- **76% of attacks resulted in data being encrypted**. This is above the global average of 70%, but below the 89% reported by South African respondents in last year's survey.
- **Data was also stolen in 35% of attacks where data was encrypted**, above the global average of 32% but in line with the 35% reported by South African respondents in our 2023 study.
- **In 97% of South African ransomware attacks, cybercriminals tried to compromise the organization's backups**, slightly above the global average of 94%.
- **44% of backup compromise attempts were successful**, below the global average of 57%.
- **All South African organizations whose data was encrypted got data back**, above the global average of 98% but in line with last year's figure.
- **Backups remain the most common method used for restoring data**, with 72% of South African respondents whose data was encrypted using this approach. This is a decrease from the 76% that used backups in our 2023 survey.
- **43% of those that had data encrypted in South Africa paid the ransom**, a decrease from both last year's rate of 45% and the 2024 global average of 56%.
- **45% of South African organizations that had data encrypted used multiple recovery methods to get data back**, slightly below the global average of 47%.
- 160 respondents from South Africa whose organization had data encrypted shared the initial ransom demand:
  - **Mean South African ransom demand: $975,675**; global average $4,321,880
  - Median South African ransom demand: $165,000; global average $2 million
  - 29% of demands were for $250,000 or more
- 66 respondents from South Africa whose organization paid the ransom shared the amount:
  - **Mean South African ransom payment: $958,110**; global average $3,960,917
  - Median South African ransom payment: $152,000; global average $2 million
- **The eventual ransom paid by South African organizations, was on average, 93% of the initial demand**. In comparison, globally, organizations paid 94% of the initial demand.

- **87% of South African ransom payments are funded from multiple sources**, above the global average of 82%.
- **Cyber insurance providers contributed to the ransom in 87% of incidents**, but never paid the full ransom.
- Excluding any ransom payments, **the average (mean) bill incurred by South African organizations to recover from a ransomware attack was reported at $1.04 million**. This is an increase on the $0.75 million reported in 2023. This includes costs of downtime, people time, device cost, network cost, lost opportunity, et cetera.
- **South African organizations are getting slower at recovering from attacks** with 41% fully recovered in up to a week, down from 53% in 2023. 26% took between one and six months, an increase from 19% last year.
- **99% of South African ransomware victims reported the attack** to law enforcement and/or an official government body.
  - 64% received advice on dealing with the attack
  - 68% got help investigating the attack
  - 47% received assistance in recovering data encrypted in the attack
- **61% of those that reported the attack found it easy to engage with law enforcement and/or official bodies**. 35% found it somewhat difficult while 4% said it was very difficult to engage.

Recommendations

Ransomware remains a major threat to South African organizations of all sizes around the globe. While the overall attack rate has dropped over the last year, the impact of an attack on those that fall victim has increased. As adversaries continue to iterate and evolve their attacks, it's essential that defenders and their cyber defenses keep pace.

Prevention. The best ransomware attack is the one that didn't happen because the adversaries couldn't get into your organization.

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. Detecting and neutralizing an adversary inside your environment before they can compromise your backups or encrypt your data will considerably improve your outcomes.

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.

To explore how Sophos can help you optimize your ransomware defenses, speak to an adviser or visit www.sophos.com

Learn more about ransomware and how Sophos can help you defend your organization.

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.

2024-04-24 (WP-MP)

SOPHOS