WERKSMANS
ATTORNEYS

COMPETITION

Who let the dogs in?

17 July 2025 *3 min read*

Cyber epidemic, ever present in South Africa, and it would seem that the Government is realising this.

by Ahmore Burger-Smidt, Director and Head of Regulatory

Cyber infiltration allows for a ransomware demand. The one is dependent on the other.

Reading *'The State of Ransomware in South Africa Report 2025*[1]*'*, published by cybersecurity firm Sopas, leaves one somewhat numb. One thing that cannot be disputed is that cyberattacks and ransomware demands are prevalent in South Africa, and together with the prevalence comes the growing ransom demand.

It has been determined that the median ransom demanded, which was R2.9 million in 2024, shot up to a staggering R17 Million in 2025.

On 16 July 2025, the Minister in the Presidency, Khumbudzo Ntshavheni, announced that the Government is finalising a new Cybersecurity Bill aimed at strengthening defences against online threats. The need to enhance digital safety, raise public awareness, and protect critical infrastructure, is a priority and therefore a national cybersecurity strategy is being crafted. The Cybersecurity Bill is expected to shed light on and outline the Government's response, among others, to cyberattacks and data breaches. This is all in an attempt to create a "cyber-secure nation".

The question is however a simple one. If it was found by Sophos that the most common reasons for cyber infiltration and security breaches are compromised credentials, contributing to 34% of all successful attacks and additionally, the risk of phishing resulted in 22% of attacks, do we need to wait for a strategy to aim for a "cyber-secure nation"?

A data breach i.e. cyber-attack for ransom, that exposes personal information, immediately results in a obligation to notify the Information Regulator. Also, to notify affected individuals if there's a risk to their rights, identity, finances, etc and notification of partners or service providers (especially if data was shared).

Media coverage and public perception can quickly turn negative post a security breach. Social media backlash can amplify the issue rapidly and this could very well open the doors for competitors to capitalise on a perceived weakness. Internationally it has been noted that publicly traded companies often experience a drop in stock price following a breach and increased scrutiny from shareholders and regulators.

News of non-compliance or data privacy violations can linger in the public record.

Therefore, while the country awaits the Cybersecurity Bill, focus should be placed on the low-hanging fruit, amongst others, a well-crafted Incident Response Plan, focusing on access controls, undertaking an Impact Assessment and training of employees.

South Africa has been identified as '*the most targeted African country for cybercrime, accounting for 40% of ransomware attacks and nearly 35% of infostealer incidents on the continent*'[1] according to Newzroom Africa.

No country is entirely immune to cyber threats.

But, no country should become a cybersecurity risk statistic.

Read more about our Regulatory practice area.

---

[1] Newzroom Africa

Ahmore Burger-Smidt

Head of Regulatory

View Profile