datacentrix

Why cyber resilience matters now more than ever

By Brett Skinner, Business Unit Manager: Cyber Resilience at Datacentrix

South Africa is facing a particularly high prevalence of cyberattacks, emphasising the importance of prioritising cybersecurity in the region. The increasing sophistication of these incidents, and the emergence of new threats, require continuous vigilance and adaptation to ensure effective protection.

In fact, shocking local statistics show that local businesses are 75 percent more likely to suffer from a ransomware attack, as compared to 60 percent globally, and 65 percent more likely to experience a phishing attack, 10 percent higher than international figures. Furthermore, 55 percent of South African businesses will be targeted with data breaches, as opposed to 45 percent globally, and 45 percent will suffer through distributed denial of service (DDoS) attacks, which again is 10 percent higher than global levels.

These figures emphasise the fact that, in South Africa, cyber resilience is no longer an option; it is an absolute necessity.

Cyber resilience can be defined as an organisation's ability to maintain its core purpose and integrity in the face of a cyberattack. The real challenge lies in whether it can recover swiftly and continue to deliver services in its aftermath.

Cyber resilience is not about making money; it is about protecting the revenue that businesses generate. It is a fundamental layer of defence that allows organisations to continue operations

“Cyber resilience can be defined as an organisation's ability to maintain its core purpose and integrity in the face of a cyberattack. The real challenge lies in whether it can recover swiftly and continue to deliver services in its aftermath. Cyber resilience is not about making money; it is about protecting the revenue that businesses generate.

Brett Skinner
Business Unit Manager: Cyber Resilience at Datacentrix

despite security breaches. The reality is that cyberattacks are no longer a question of *if* but *when* they will happen, and *how often*. The real differentiator is how quickly and efficiently a business can recover.

The rise of AI-driven cyberthreats

The rise of AI-powered cyberattacks means that threats are evolving faster than ever. Attackers are leveraging automation to accelerate brute-force attacks, bypass security protocols and deploy highly targeted phishing campaigns.

Emerging threats include:

- **Ransomware surge:** AI-driven cyberattacks can be a precursor to more devastating ransomware incidents, in which threat actors use machine learning (ML) to identify and target vulnerable systems, deploy malware and extort victims.
- **Synthetic media manipulation:** Deepfakes and AI-generated holograms pose a growing threat, as they can be used to spread misinformation, impersonate trusted individuals and conduct social engineering attacks that are increasingly difficult to detect.
- **Open source tool exploitation:** Threat actors can make use of freely available open source tools and scripts, combined with AI capabilities, to automate and scale up their attacks, putting organisations and individuals at greater risk.
- **Undetectable cyberthreats:** AI-powered malware continuously adapts to evade detection, rendering traditional security tools ineffective and requiring more advanced, AI-driven defences.

By 2030, software supply chain vulnerabilities will become a primary cybersecurity risk, with third-party libraries and frameworks introducing inherited weaknesses into enterprise environments. In addition, weak points within legacy systems, which have often not been addressed due to cost and complexity combined with human error, are becoming extremely vulnerable. The rise of IoT devices is also providing cybercriminals with new attack vectors and valuable data to enhance targeted attacks.

“

At Datacentrix, our mission is to help customers navigate cybersecurity complexities, defend against threats and ensure uninterrupted business operations. In the end, resilience is not just about prevention; it is about ensuring that when a cyber event occurs, businesses can recover swiftly and efficiently – because, in today's digital world, downtime is not an option.

This makes real-time detection, proactive threat mitigation and AI-driven security tools essential components of any cyber resilience strategy.

Resilience is the future

Cyberattack prevention alone is insufficient – businesses must prioritise recovery and continuity to minimise downtime. As businesses continue to navigate the complexities of cybersecurity, the shift toward resilience-driven strategies will be crucial.

At Datacentrix, our mission is to help customers navigate cybersecurity complexities, defend against threats and ensure uninterrupted business operations.

In the end, resilience is not just about prevention; it is about ensuring that when a cyber event occurs, businesses can recover swiftly and efficiently – because, in today's digital world, downtime is not an option.

Have you, or your business, fallen prey to cyber criminals? Report incidents to Datacentrix's cybercrime line, by emailing cybercrimeline@datacentrix.co.za or calling (012) 657 5100.