Attacks are a case of ‘if’ not ‘when’ – why cyber resilience has become critical to SA businesses

As cyber threats continue to escalate globally, businesses are becoming increasingly aware of the need for not only cybersecurity, but also cyber resilience. Datacentrix, the leading hybrid ICT systems integrator and managed services provider emphasises that resilience – defined as the ability of an entity to continue operating despite cyberattacks – has become a crucial component of a modern IT strategy.

Cyber resilience goes beyond traditional cybersecurity, explains Brett Skinner, Security Business Unit Manager at Datacentrix, acknowledging that, in today's interconnected world, attacks are inevitable – it's no longer a case of 'if' but 'when' they will take place.

“The key question is: how quickly can an organisation bounce back and minimise disruption when an attack occurs?” he asked.

> “Cyber resilience isn't just about stopping an attack, it's about the ability to keep going when an attack happens. We need to get to a place where recovery times are measured in minutes or hours – not weeks or months. Unfortunately, some businesses have taken as long as two and a half months to return to normal operations after a breach.

Kyle Pillay, Security As A Service Centre Manager at Datacentrix

Kyle Pillay, Security As A Service Centre Manager at Datacentrix, underlines the importance of this distinction. "Cyber resilience isn't just about stopping an attack, it's about the ability to keep going when an attack happens. We need to get to a place where recovery times are measured in minutes or hours – not weeks or months. Unfortunately, some businesses have taken as long as two and a half months to return to normal operations after a breach," he stated.

Indeed, a 2024 report by PwC on global digital trust highlights that, while South Africa experiences a slightly lower than average rate of cyberattacks compared to the global norm, the threat is still significant. For example, email compromise is reported at a higher rate than the global average, with 38 percent of local businesses impacted versus 29 percent worldwide. This shows the necessity for cyber resilience measures that address both attack prevention as well as recovery.

> The first step is to build a roadmap and plan against it, checking whether you're prepared for disaster recovery. Next, because it can be difficult to journey alone within the security space, you must ensure that you have a level of trust with a specialist partner. Together, you can then gain a better understanding of your attack surface exposure and subsequently plan, deploy and test.

The impact of AI-powered cyberattacks
Looking ahead, the European Union Agency for Cybersecurity (ENISA) predicts that by 2030, cyber threats will evolve even further, driven by new technologies. ENISA's top ten predicted threats include disinformation campaigns, privacy loss through digital surveillance, smart device data manipulation and advanced hybrid threats.

“As AI-generated synthetic media, such as deepfakes, become more prevalent, discerning truth from deceit could become a challenge for businesses,” says Pillay, pointing to the rise of AI-powered cyberattacks, such as password spraying and brute-force attacks, as a growing local threat.

"These attacks leverage AI's capability to analyse patterns and vulnerabilities on a massive scale," he continues. "Password spraying involves criminals trying to access a large volume of accounts with a few commonly used passwords, one password at a time. On the other hand, brute force attacks see attackers attempting to gain unauthorised access to a single account by guessing the password using large lists of potential passwords.

“AI is a double-edged sword – it's useful for security, but it also magnifies the capabilities of cybercriminals. And AI isn't the only emerging technology that brings with it additional cybersecurity risk; quantum computing and the internet of things (IoT) too are widening the attack landscape.”

The role of cyber resilience in the modern enterprise
Skinner offers a pragmatic approach for businesses aiming to implement effective cyber resilience strategies. "The tendency, frequently, is to rush into execution mode when there's a threat, but that can be dangerous, especially if you don't have a clear plan or roadmap in place. Resist knee-jerk reactions.

“The first step is to build a roadmap and plan against it, checking whether you're prepared for disaster recovery. Next, because it can be difficult to journey alone within the security space, you must ensure that you have a level of trust with a specialist partner. Together, you can then gain a better understanding of your attack surface exposure and subsequently plan, deploy and test.”

He also calls attention to the importance of user education as a fundamental element of cyber resilience. "People are still the weakest link in any cyber resilience strategy. Educating your workforce on security hygiene and emerging threats can significantly reduce your vulnerability.”

As cyberattacks grow in scale and complexity, the discussion is shifting from merely preventing breaches to ensuring fast recovery when they occur, meaning that businesses must focus on resilience as a critical defence mechanism.

For South African organisations, the message from Datacentrix's 2024 Showcase is clear: No industry is immune to digital extortion. As Pillay aptly noted, "It's not about how hard you get hit; it's about how fast you get back up."

Brett Skinner Security Business Unit Manager at Datacentrix

For more information contact Elzette du Preez on edupreez@datacentrix.co.za