SA corporates over budget on security, but cyber risks mount - report

According to the newly released *State of Cybersecurity in South Africa* report, nearly three-quarters of South Africa's top 100 corporates are investing more in cybersecurity than the industry average, but an almost equal proportion don't feel fully protected by their current cybersecurity strategy.

Source: Pexels

The new study, conducted by World Wide Worx on behalf of Intel and Dell Technologies South Africa, reveals that half of South African large businesses are over budget on cybersecurity spend, and just over half feel there are now more threats introduced by remote work culture.

Budgeting for breaches

“Corporations being over-budget on cybersecurity spend may look like a positive sign, but it also raises the likelihood that the budgets were too low to begin,” says World Wide Worx CEO Arthur Goldstuck, principal analyst on the research project.

Source: Supplied

click to enlarge

“In the game of cybercrime cat and mouse, one could argue there is no such thing as being over-resourced. However, under-resourcing not only exposes companies to risk, but also poses an existential threat. A major breach can bring down a company. Budgets must catch up to the significance of the threat.”

Challenges range from these macro threats all the way down to individual losses. With the pandemic and lockdowns having sent corporate employees home, 55% of IT decision-makers are concerned about their staff losing their devices. And it’s not only about the physical loss and immediate cost of replacement.

Khairy Ammar, services sales director for emerging Africa and South Africa at Dell Technologies, says: “As new threats and vulnerabilities appear at break-neck speed, new technology also creates opportunities to innovate. As we navigate the changing landscape of work, it is imperative to deliver solutions that keep the organisations and their employees safe. With breaches now happening both above and below the OS,

organisations need to keep endpoints secure from anywhere.

“You need intelligent solutions that prevent, detect and respond to threats wherever they occur. A procedural measure like taking on a certified cybersecurity partner to manage these services is often the best protection for corporates.”

A finding that will provide the business world with greater confidence is that three-quarters of large corporations (77%) report their devices are upgraded frequently, and support both Secure Boot and Trusted Protection Modules – which helps mitigate physical access vulnerabilities.

Many cyber hygiene factors are implemented by corporates, with the majority using VPN access control, and cloud platform-managed security. These factors being implemented show that corporates are aware of advanced methods of protecting themselves.

Disaster management essential

The vast majority (99%) of corporates are aware that disaster management is essential. This figure must, however, be seen in the context of only 40% of large businesses using multiple solutions to protect, backup, and replicate their data in the event of disaster. That said, most respondents (99%) had not experienced cyber attacks that led to financial loss.

The 1% that experienced loss after a data leak provide a useful case study of security stances after an attack: these businesses had their systems compromised before the onset of remote working, indicating that no matter how a corporate geographically locates its employees, it remains vulnerable.

Cryptocurrency scams are on the rise in SA: How crypto cons work and how to protect yourself

ESET 22 Apr 2022

Compromises and vulnerabilities are revealed through the weakest link in the IT system, which is often an organisation’s own employees, and this may allow in ransomware programs or phishing attempts. More than half of businesses report that ransomware and phishing attempts have increased in the past year, or that they simply can’t keep up with the numbers of attempts.

Bryan Turner, World Wide Worx senior data analyst, says awareness and action are key: “Training employees to work safely but spotting out-of-character emails and communications can save a company from all the phishing headaches involved with cybersecurity incidents.”