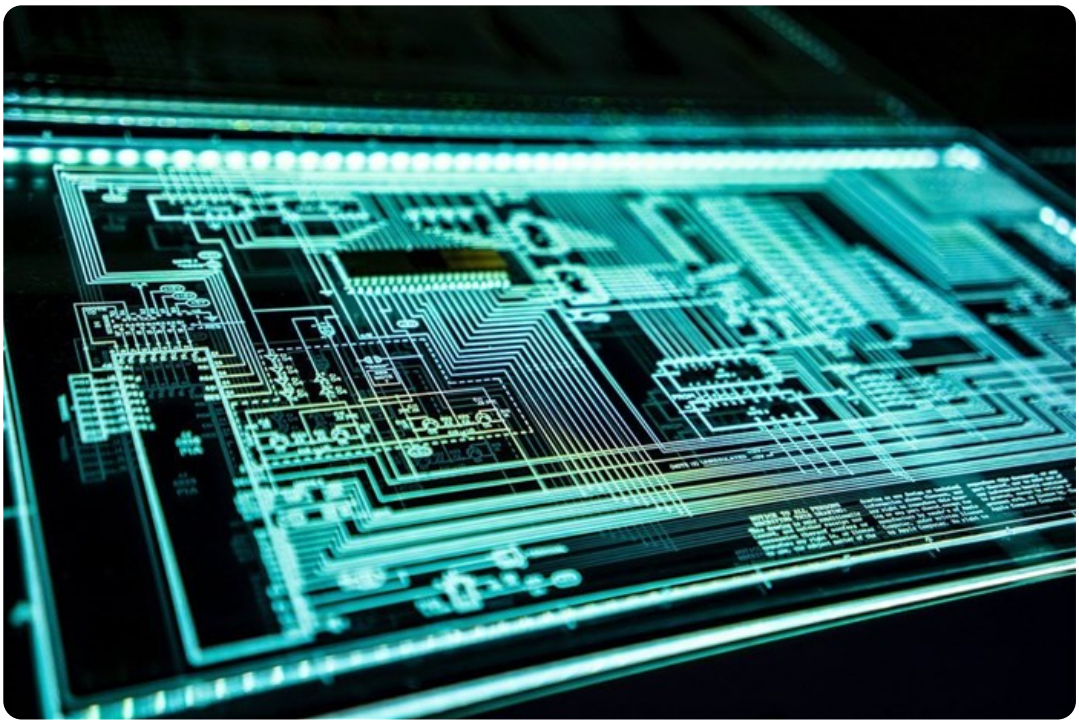
SA's cybercrime hotspot status intensifies need for cybersecurity in logistics

With South Africa now among the world's biggest cybercrime hotspots, logistics firms are scrambling to guard against new and highly sophisticated attacks.



Source: Supplied

The ransomware breach of Transnet in 2021 exposed just how damaging cybercrime can be to local supply chains and th export/import market, with Transnet having to resort to manual processing, causing congestion outside the country's major ports.

If anything, the situation has only intensified since then.

Internet service provider Seacom found that in 2023, South Africa was the most targeted country in Africa when it came t ransomware and attacks on company e-mail services.

But, as Morne Visser, head of IT operations and infrastructure at Bidvest International Logistics (BIL), explains, spending millions of rand on external cyber protection measures won't make a bit of difference unless companies' end-users are trained in what to look out for. "We receive about three million e-mails a month. That's three million opportunities for a hacker. That means there must be extensive end-user training and awareness," he says.

Choosing the right cybersecurity partner

So frequent have attacks become that companies now have to alert staff to new threats and update cyber security tools ev quarter, where it used to be only once a year.

Visser adds that logistics companies deal with a variety of industries across the world, and each of these needs to safegu against phishing and other attacks. In other words, it is a war on numerous fronts.

According to BIL's information technology Director Lesiba Sebola, an excellent track record is key in this process.

"Logistics uses the IoT (Internet of Things), and the security aspects need to be looked at. You want to look for a company that has experience in this field," Sebola says. "In logistics, you are required to give a client visibility on where they are in the supply chain process, and there needs to be integration across the different areas. What you want is a cyber security company that has expertise in integration."

Visser adds that these experts also need to have a firm grasp of the latest cybersecurity toolsets and be proactive in everything they do. Certifications and awards from tech industry giants like Microsoft are good indications of their quality and standing within the sector.

He stresses that older tools need to be discarded in favour of the latest technology. Every day, hackers find new ways to breach companies' defences, and the firm needs to possess safeguards that can counter such attacks.

What is vitally important for companies to understand, Visser says, is that an **effective cybersecurity response plan is non-negotiable**.

Too often is the case that "people run around like headless chickens" when a system has been breached. In their panicked state, they call for servers to be shut down when this would immediately remove the ability to investigate the attack properly so a solution can be found.

A well-drilled team that understands the latest cybercrime trends will prevent such scenarios from playing out.

Sebola says the best company will be the one that is 100% committed to ensuring protections are maintained. "We talk about technology, people and processes. For technology, we ask whether we have the right tech in place. For people, it's all about training. And for processes, it's about whether people are following them. Yet even with all this in place, if you are not maintaining your cybersecurity system, you might as well not even bother."