

<https://www.engineeringnews.co.za/article/what-the-transnet-and-jaguar-land-rover-cyber-attacks-mean-for-south-african-trade-2025-10-07>

What the Transnet and Jaguar Land Rover cyber attacks mean for South African trade

7TH OCTOBER 2025

The recent cyber-attack on UK's Jaguar Land Rover (first detected at the end of August 2025) is not just an IT problem for a single OEM: it is a live demonstration of how digital contagion cascades through modern supply chains and into national economies. The immediate consequence – prolonged factory shutdowns, blocked ordering and registration systems and disrupted supplier payments – rapidly translates into lost production, cashflow stress for tier-1 and smaller suppliers, and delayed deliveries to dealers and fleet customers.

And this is not an isolated risk. South Africa learned a similar lesson in 2021 when Transnet, operator of the country's ports and rail network, suffered a ransomware attack that forced it to declare force majeure at several container terminals, including Durban, Cape Town and Port Elizabeth. Durban, which handles nearly 60% of South Africa's container traffic, was paralysed, with refrigerated exports like citrus at risk of spoilage as reefer plugs ran short. The incident took about a week to stabilise, costing exporters millions of rand per day

and exposing how vulnerable South Africa's trade arteries are to digital disruption.

Countries like South Africa, which both import finished vehicles and form part of global supplier networks, the effects are tangible: slower deliveries to local dealers, difficulty obtaining specific components or spare parts and knock-on impacts for businesses that rely on vehicle availability – such as logistics firms, service workshops and rental fleets.

For South Africa, the lessons are sobering. Local exporters in sectors like citrus, automotive parts, and mining rely on digital platforms to connect with international buyers and move goods efficiently through ports. A major breach could leave exports stranded, buyers frustrated, and hard-earned market credibility at risk.

Many companies still prefer to downplay or remain silent about cyber incidents because of reputational risk: fear that customers, investors and partners will lose trust. Yet past cases show that secrecy often compounds the harm. British Airways' 2018 data breach, followed by a high-profile investigation and a large regulatory fine, eroded public confidence and invited prolonged media and regulatory scrutiny. The lesson is clear: opacity can turn a technical incident into a long-running crisis.

Transparency is therefore not merely ethical, it is strategic. Prompt, factual disclosure allows supply-chain partners to take protective steps (segmentation of networks, suspension of risky integrations, alternative sourcing), preserves customer trust through honest communication, and reduces the likelihood of speculation that damages brand value. It also

helps governments and industry bodies coordinate targeted support, which is especially important where small suppliers or local economies are exposed. In the JLR case the UK government's engagement to protect the wider supply chain underlines that collective response matters.

In South Africa, the lessons are sobering. Local exporters in sectors like citrus, automotive parts, and mining rely on digital platforms to connect with international buyers and move goods efficiently through ports. A major breach could leave exports stranded, buyers frustrated, and hard-earned market credibility at risk.

For South African stakeholders the immediate priorities are clear: dealers and fleet operators should check contractual provisions, confirm schedules with OEM partners, and review spare-parts inventories; suppliers should verify payment terms and seek confirmation of continued support; and all parties must accelerate cyber-hygiene and incident-response planning. Above all, the episode should trigger a pragmatic shift: treat cyber resilience as a supply-chain priority, not an IT footnote.

Cyber resilience is now as critical as physical infrastructure. If South Africa wants to position itself as a trusted regional logistics hub for BRICS and African trade, it must show trading partners that its digital infrastructure is secure and reliable. Conversely, if the country is seen as fragile or unprepared for cyber threats, global shippers may divert cargo flows elsewhere.

Building resilience therefore requires more than firewalls. It means diversifying supply routes, segmenting IT and

operational systems, investing in real-time monitoring, and training people to respond quickly to incidents. 🇿🇦

Phone: +27 (0)11 622 3744

Email: newsdesk@engineeringnews.co.za

Website: www.engineeringnews.co.za

To subscribe email
subscriptions@creamermmedia.co.za or [click here](#)

To advertise email
advertising@creamermmedia.co.za or [click here](#)

