

RISK CONTROL • CYBER RESILIENCE

Cyber Resilience Is Not a Firewall. It Is What Happens After One Fails.

Defence and aerospace supply chains run on the same assumption every modern organisation runs on: that the systems behind the systems will keep working. Most of the time they do. Cyber resilience is about the times they don't.



The Real Exposure

Interpol's African Cyberthreat Assessment has repeatedly placed South Africa among the countries most targeted by cybercrime on the continent, a pattern driven in part by its concentration of ports, energy infrastructure and defence manufacturing capacity. None of that is going away, and none of it makes the threat someone else's problem.

01

Cyber resilience is about the times they don't. —

Resilience means keeping operations, communications and decisions moving while an incident is underway, and recovering on your own timeline rather than the attacker's. A delayed shipment or a grounded aircraft carries consequences that go well past cost, and that is precisely where most organisations discover their plan was theoretical.

2021

In July 2021, a ransomware attack shut down container operations at every major South African port for several days. Trucks queued outside Durban and Cape Town with nowhere to unload. The attacker never touched a crane or a ship. **One compromised system in a back office was enough to stop freight moving across the country.**

02

The four phases every resilience engagement is built around.

01

PREPARE

02

DETECT

03

RESPOND

04

RECOVER

Why It Matters at AAD

Defence and aerospace organisations sit at the intersection of national interest and commercial pressure. That combination attracts a different class of adversary, and it means a resilience failure is rarely just an internal problem. We help organisations in this sector build a defensible position before they need one, not after.

03

What we do

DISystems works with organisations across South Africa, the SADC region and internationally on the practical side of cyber resilience, not just the paperwork behind it.



Cyber resilience assessments benchmarked against ISO 27001, NIST and King IV, built around our G-RISE methodology rather than a generic checklist.



Incident readiness and response planning, including tabletop exercises run with your actual leadership team, not a scenario borrowed from a template.



Third-party and supply chain risk reviews, aimed at the vendors and subcontractors who carry as much risk as your own network.



Governance, risk and compliance advisory aligned with POPIA and international standards, documented in a form your auditors and regulators can actually use.

DISYSTEMS

Most organisations discover the gap between their plan and their reality during an actual incident. We would rather find it with you beforehand, on an ordinary Tuesday, with time left to fix it.

DISystems – cybersecurity and GRC advisory across South Africa, the SADC region and internationally, in partnership with **Cyberantix™**

CONTACT US AT:
tsepang@disystems.co.za
to setup a time for more details.

