OVERVIEW

Cyber Intelligence Overview

Understanding Digital and Insider Threats for South African Organisations

Cyber intelligence is the practice of understanding the threats facing your organisation, digital and human, so you can prevent, detect and respond before a loss compounds. In South Africa the risk is not only the outside attacker; it is increasingly the insider who is recruited or placed to open the door.

The threat landscape

- **External.** Phishing and business email compromise, ransomware, credential theft, and fraud that targets payments and payroll.
- **Insider.** Employees or contractors who leak information, disable controls, or facilitate theft, sometimes recruited by organised networks.
- **Blended.** The most damaging schemes combine an inside facilitator with an outside actor, which is exactly what a single control assuming a lone outsider will miss.

What cyber intelligence adds

Tools record what happens; intelligence explains what it means and who is behind it. It combines technical monitoring with human insight to surface the pattern early, when it is still cheapest to stop.

Protective strategies

- **People.** Screening on appointment, security awareness, and clear separation of duties.
- **Process.** Least-privilege access, change control, supplier and payment verification, and an incident plan.
- **Technology.** Multi-factor authentication, logging and monitoring, backups, and timely patching.

POPIA note. Personal information must be processed lawfully and kept secure. A data breach involving personal information must be reported to the Information Regulator and to affected data subjects; administrative fines reach up to R10 million.

If an incident occurs

1. Contain and preserve evidence; do not tip off a suspected insider.
2. Assess scope and impact, including any personal information affected.
3. Notify as POPIA and your policies require.
4. Investigate lawfully, remediate the root cause, and recover.

Joining the dots

Cyber threats rarely sit apart from physical and corporate risk. Reading them together, the digital signal and the human one, is what turns scattered alerts into a picture you can act on.

Talk to Trio Data

Trio Data Special Services provides corporate intelligence, undercover audits, and forensic and fraud investigations across South Africa. For a confidential, no-obligation discussion, contact +27 21 949 4440 or office@triodatacape.co.za.