Journey to Green

Partnering to secure your networks and online business

CyberAntix™ is an implementation-led cybersecurity partner. Founded in 2020 and supported by a 35+ person Security Operations Centre. We combine rigorous governance, modern security engineering, and pragmatic change management to make organisations measurably safer . We are product-independent, so recommendations are driven by risk and business value rather than vendor quotas.

Our role is to translate security strategy into operating reality – controls deployed, people enabled, processes embedded – and to evidence progress to executives and regulators in clear, defensible terms.

Our approach turns cybersecurity from a grudge spend into a strategic enabler. We align investment to material risks, design the operating model that keeps you secure, and co-manage the transition so improvements stick. Throughout the engagement, we focus on predictable OPEX, transparent reporting, and outcomes key business stakeholders can trust.

Why CyberAntix™ – an implementation-led partnership

We operate as an extension of your IT, security and business risk teams, co designing the roadmap, implementing the controls, and sharing accountability for outcomes.

Product-independence

right-sized technology fitted to your environment

Measurable progress

SLAs and KPIs mapped to business risk

Implementation ownership

from architecture and configuration to cut-over and stabilisation

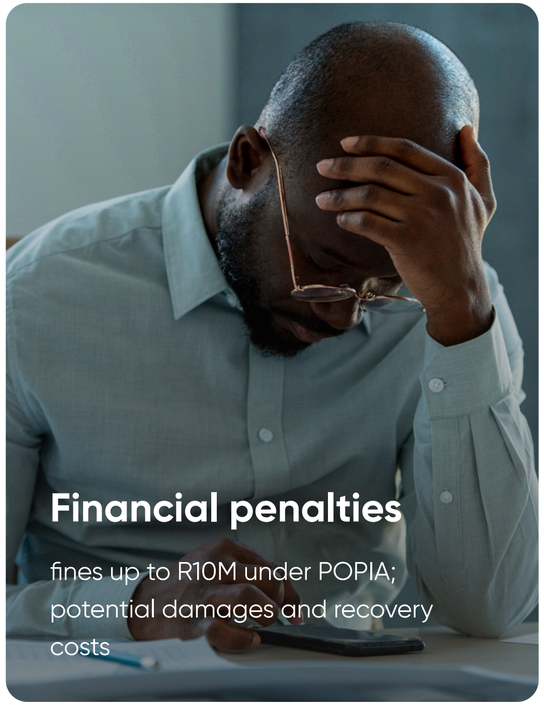
Predictable OPEX

commercial models that favour sustained protection over one-off projects

Co-managed operations

playbooks and a SOC that detects, responds, and hardens continuously

Risks of non-compliance with legal and regulatory requirements



Financial penalties

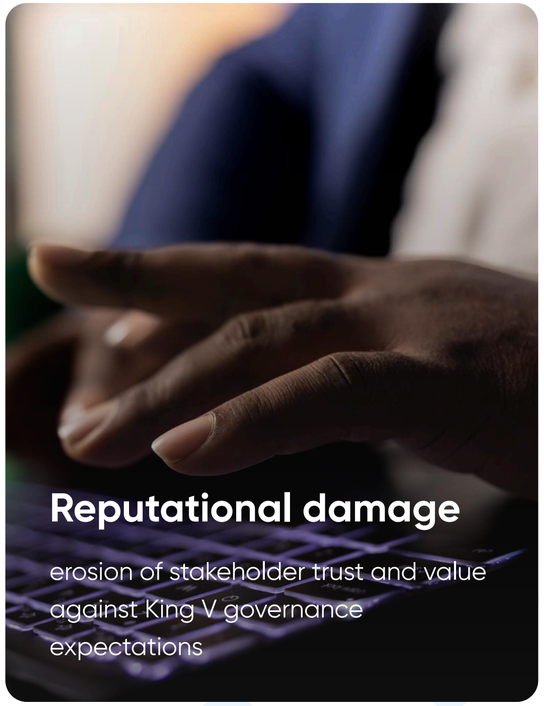
fines up to R10M under POPIA; potential damages and recovery costs

Regulatory scrutiny

enforcement notices for non-compliance with POPIA, ECTA and sector regulations

Legal accountability

director responsibilities under the Companies Act; offences under the Cybercrimes Act



Reputational damage

erosion of stakeholder trust and value against King V governance expectations

Emerging threats

AI-accelerated social engineering, ransomware targeting supply chains, skills shortages, and “harvest-now-decrypt-later” tactics are reshaping risk profiles.

The answer is disciplined execution

Identity controls, hardened networks infrastructure, resilient cloud posture, tested response, and continuous monitoring.

Execution Blueprint – From Baseline to Green

What “Green” means: a business-aligned and reduced cybersecurity risk posture where critical controls are operating effectively, compliance obligations are evidenced, incident response is rehearsed, and stakeholders have confidence in the organisation’s cyber resilience.

1 Discover & Baseline

Activities: evidence-based assessment across people, process and technology; control maturity mapping; architecture and data-flow review; regulatory gap analysis (POPIA, ECTA, King V).

Artefacts: risk register, control gap list, current-state view.

2 Strategy & Roadmap

Activities: prioritisation by business impact, dependency mapping, and quick-win selection; policy and standards uplift; investment planning with an OPEX view.

Outputs: 12-month roadmap with milestones, success metrics, and governance cadence.

3 Implementation & Enablement

Activities: deploy and embed appropriate controls across people, processes, and technology; strengthen governance, response planning and awareness; and ensure changes are adopted.

CyberAntix acts as your accountability partner, working side-by-side with IT, security and business risk owners to drive adoption and results.

Assurance: configuration and process reviews, handover packs, and stabilisation support, with clear ownership, milestones, and evidence of control effectiveness.

4 Operate & Optimise

Activities: co-managed SOC, incident response, exposure management, control health checks, and continuous tuning.

Outcomes: reduced mean-time-to-detect/respond, fewer false positives, steady uplift in resilience.

5 Assure & Report – G-RISE

Activities: transparent, board-ready reporting that converts technical risk into business decisions, aligned to governance, regulation and ESG.

Deliverables: annual G-RISE pack; executive dashboards; audit-ready artefacts for regulators and customers.

6 Continuous Improvement

Scenario testing, policy/standard refresh, skills uplift, and roadmap re-prioritisation to sustain “green” as the environment changes.

Experience that backs CyberAntix™

Our programmes are delivered by seasoned practitioners across governance, security engineering, SOC operations and risk reporting. The team brings deep industry standards leadership and real world delivery experience - from architecture and solution integration to incident response - using global and local threat intelligence to implement practical controls, provide clear executive reporting, and sustain resilient day to day operations.

What you gain

- Enhanced compliance and risk reduction
- Operational resilience and incident readiness
- Safeguarded reputation and stakeholder trust
- Competitive advantage through smarter, right-sized security
- Cost-efficient risk management – investment aligned to material risk

Start your Journey to Green. Contact us to explore a solution best suited to your business needs.

Telephone

+27 (0) 87 004 2220

Email

info@cyberantix.co.za

Website

www.cyberantix.co.za