



STRATEGIC ADVISORY SERVICE

EXECUTIVE CYBER RISK MANAGEMENT

Tactical Cyber Command. Embedded. Adversary-Aligned. Outcome-Driven.

Embedded security leadership that combines strategic direction with hands-on execution. Not a shared advisor on a retainer. A dedicated command structure that operates as an extension of your organisation.

15+ YEARS

Specialist cyber security expertise and leadership

ISO 27001 & ISO 9001

Certified information security and quality management

TACTICAL COMMAND

Embedded execution, not just advisory

CYBER SECURITY THAT STOPS HACKERS

01

The Leadership Gap

Cyber security leadership is no longer optional. It is a board-level mandate. But the traditional approach to outsourced security leadership, the CISO-as-a-Service model, was built on a flawed premise: that a part-time, shared advisor can deliver the same outcomes as an embedded, operationally integrated security command function. It cannot.

Why Traditional CISO-as-a-Service Falls Short

1

Divided Loyalty, Divided Attention

Most vCISO providers serve multiple organisations simultaneously. Your security leader is also advising three, five, or ten other companies. When two clients have an incident on the same day, someone gets deprioritised. The average CISO tenure globally is roughly two years, and nearly a third have considered leaving the role due to stress. The vCISO model inherits this instability in an even more fragile form.

2

Advisory Without Execution

The most common failure is the gap between strategy and action. Traditional vCISOs deliver policy documents, maturity assessments, and roadmap presentations, then leave your internal team to implement alone. When recommendations stall because your team lacks capacity, the vCISO has already moved on to the next client.

3

Compliance-First, Threat-Last

The overwhelming majority of vCISO providers feel overwhelmed by regulatory frameworks. The result is predictable: engagements become compliance exercises rather than adversary-aligned security programmes. Your organisation ends up with frameworks on paper while real-world attack paths remain unaddressed.

4

Disconnected from the Business

Too many organisations still treat cyber security as an IT function tucked away in a corner. A part-time external advisor compounds this isolation. Without deep integration into your leadership team, a vCISO cannot translate technical risk into business-level decisions.

5

No Operational Continuity

When your vCISO engagement ends or your contact moves on, your institutional security knowledge walks out the door. There is no command structure, no operational playbook that persists, and no embedded team that carries forward.

02

Tactical Cyber Command

NEWORDER's Executive Cyber Risk Management service replaces the broken vCISO model with what your organisation actually needs: a Tactical Cyber Command structure that embeds strategic leadership, adversary-aligned thinking, and hands-on execution directly into your business. With our Head Office in South Africa and Global Head Office in the Isle of Man, we are strategically positioned to serve clients across Europe, the Middle East, and Africa.

What Makes This Different

1

Embedded, Not Remote

Your Tactical Cyber Commander integrates with your leadership team, attends your board meetings, understands your people, and operates within your business context. This is leadership from the inside, looking out at the threat landscape with your interests as the sole priority.

2

Execution, Not Just Advisory

We do not hand over a strategy document and walk away. NEWORDER builds, implements, and operates your security programme alongside your team. From policy development and vendor oversight to incident response planning and security architecture review, we execute what we recommend.

3

Adversary-Aligned, Not Compliance-First

Compliance is an output of good security, not the objective. We design your security programme around how real attackers operate, ensuring your defences are built for the threats that actually target your industry. Compliance follows naturally when security is done right.

4

Continuous Command, Not Fractional Attention

Your organisation gets a dedicated command structure with named analysts, defined escalation paths, and guaranteed response times. When an incident occurs, your Tactical Cyber Command team is already inside your environment and ready to act.

5

Full-Spectrum Integration

Tactical Cyber Command connects directly to NEWORDER's offensive security, exposure management, and threat intelligence capabilities. Your security leadership has immediate access to Red Team findings, attack surface intelligence, and dark web monitoring, all feeding a single, coherent strategy.

Why This Is Better Than vCISO

Seven reasons organisations are replacing their vCISO with NEWORDER's Tactical Cyber Command.

1

Embedded Command, Not Fractional Attention

A vCISO splits time across multiple clients. NEWORDER assigns a dedicated team to your organisation alone. When a crisis hits, your command team is already responding.

2

Execution Built In, Not Bolted On

The vCISO model ends where the real work begins. NEWORDER executes what we recommend. We build, implement, and operate your security programme alongside your team.

3

Adversary-Aligned, Not Compliance-Obsessed

Most vCISO engagements become compliance exercises. NEWORDER designs your programme around how real threat actors operate, using intelligence from our own Red Team and dark web monitoring.

4

Full-Spectrum Intelligence, Not an Isolated Advisor

A vCISO operates in a silo. NEWORDER connects your security leadership directly to attack surface management, threat intelligence, penetration testing, and Red Team services.

5

Board-Ready Language, Not Technical Reports

NEWORDER delivers quarterly executive risk briefings, security posture scoring, and strategic roadmaps that connect to revenue protection, regulatory exposure, and shareholder value.

6

Institutional Continuity, Not Knowledge That Walks Out

When a vCISO moves on, security knowledge disappears. NEWORDER's command structure retains continuity by design. Your programme never starts from zero again.

7

Proven Expertise With Accountability

Backed by 15+ years of specialist cyber security experience and ISO 27001 and ISO 9001 certification. We share accountability for outcomes with defined metrics and transparent reporting.

Tactical Cyber Command: Core Capabilities

Everything your organisation needs from security leadership, delivered as an embedded, operationally integrated command function.

STRATEGIC LEADERSHIP

- Embedded security leadership integrated with your executive team
- Board and executive cyber risk briefings in business language
- Security posture scoring and quarterly risk reporting
- Strategic cyber roadmap development (12, 24, 36 months)

PROGRAMME EXECUTION

- Security programme development and maturity advancement
- Policy development, review, and implementation
- Security architecture review and improvement
- Security culture assessment and awareness programme design

RISK AND COMPLIANCE

- Adversary-aligned risk management framework design
- Regulatory compliance across POPIA, GDPR, ISO 27001, SOC 2, PCI DSS
- Cyber insurance alignment and evidence preparation
- Vendor and third-party security oversight

OPERATIONAL READINESS

- Incident response planning and playbook development
- Breach simulation and tabletop exercises
- Detection capability assessment and SOC tuning
- Crisis management rehearsals and post-incident review

FULL-SPECTRUM INTEGRATION

Every capability is directly connected to NEWORDER's Red Team operations, penetration testing, external attack surface management, dark web intelligence, and threat monitoring. Your security leadership does not guess at risk. They see it in real time and act on verified intelligence.

Traditional vCISO vs Tactical Cyber Command

A side-by-side comparison of what you get with a traditional outsourced CISO versus NEWORDER's embedded command model.

DIMENSION	TRADITIONAL vCISO	NEWORDER TACTICAL CYBER COMMAND
Engagement Model	Part-time shared advisor	Dedicated embedded command team
Delivery Approach	Advisory reports and documents	Strategy, implementation, and execution
Client Priority	Divided across multiple clients	Your organisation is the sole focus
Security Philosophy	Compliance-driven, framework-first	Adversary-aligned, threat-driven
Incident Response	Called in after the fact	Already embedded with pre-built playbooks
Board Engagement	Periodic technical reports	Quarterly briefings in business language
Continuity	Knowledge leaves with the person	Retained within command structure
Integration	Standalone advisory in a silo	Connected to Red Team, EASM, and intel
Accountability	Recommendations without ownership	Shared accountability for outcomes

Who Is This For?

- Organisations that need senior security leadership but cannot justify or find a full-time CISO
- Companies with internal IT teams that lack dedicated cyber security expertise and executive oversight
- Organisations undergoing digital transformation, cloud migration, or rapid scaling
- Businesses preparing for ISO 27001, SOC 2, POPIA, or GDPR compliance certification
- Companies that have experienced a breach and need immediate, embedded security leadership
- Organisations where the board or investors are demanding visible cyber risk governance
- Any business renewing cyber insurance that requires evidence of proactive security management

How It Works

Engaging NEWORDER for Executive Cyber Risk Management is straightforward. We handle the complexity so your leadership team can focus on running the business.

1

Discovery and Assessment

We begin with a comprehensive assessment of your current security posture, governance maturity, threat landscape, and business context. This is not a generic checklist. It is a deep dive into your specific risk reality, conducted by our senior analysts.

2

Command Structure Design

Based on the assessment, we design a Tactical Cyber Command structure tailored to your organisation. This includes your dedicated command team, escalation paths, communication cadence, reporting framework, and integration points with your existing teams and technology.

3

Programme Build and Implementation

We build and implement your security programme from the ground up or evolve your existing one. This includes policies, controls, vendor oversight, incident response playbooks, compliance alignment, and security architecture improvements. We execute, not just advise.

4

Embedded Operations

Your Tactical Cyber Command team operates as an extension of your organisation. We attend leadership meetings, deliver board briefings, manage vendor security, run tabletop exercises, and maintain continuous oversight of your security posture.

5

Continuous Improvement

We track progress against defined metrics, adjust the programme as your threat landscape evolves, and deliver quarterly strategic reviews. Your security posture score is measured and reported over time, demonstrating measurable risk reduction to your board and stakeholders.

FLEXIBLE DELIVERY MODEL

Tactical Cyber Command is delivered as a retainer engagement with embedded access. Scope and cadence are tailored to your organisation's size, maturity, and risk profile. Whether you need full-time command presence or structured strategic oversight, we configure the model to fit.

07

Take Command of Your Cyber Risk

The gap between where your security programme is today and where it needs to be is not a technology problem. It is a leadership problem. NEWORDER's Tactical Cyber Command closes that gap with embedded expertise, adversary-aligned strategy, and hands-on execution.

What You Gain

- A dedicated security command team embedded in your organisation
- Board-ready cyber risk intelligence your leadership can act on
- A security programme that is built, implemented, and operated, not just documented
- Measurable risk reduction tracked with defined metrics over time
- Compliance readiness across POPIA, GDPR, ISO 27001, SOC 2, and PCI DSS
- Direct access to NEWORDER's offensive security, threat intelligence, and exposure management
- Institutional continuity that survives personnel changes
- 15+ years of specialist cyber security expertise backed by ISO 27001 and ISO 9001 certification

Next Steps

- 1 Schedule a Discovery Call**
A 30-minute conversation to understand your current security posture, business context, and leadership requirements.
- 2 Receive a Tailored Proposal**
NEWORDER designs a Tactical Cyber Command structure specific to your organisation, including scope, team composition, and engagement cadence.
- 3 Activate Your Command Team**
Your embedded security leadership begins operations, integrating with your executive team and building your programme from day one.

Ready to Replace Advisory with Command?

Contact NEWORDER to schedule your discovery call today.

EMAIL: info@newordergroup.net

WEB: www.newordergroup.net