Cyberfort
Expert-led. Security Driven.

Virtual CISO Starter Service

Fractional cyber leadership without full-time overhead

Introduction

Every organisation needs experienced cyber leadership. Not every organisation can justify a full-time CISO on the payroll.

The gap between those two realities is where most mid-market organisations find themselves: growing fast enough to face serious cyber risk, regulated enough to need formal governance, but not yet at the scale where a six-figure permanent hire makes commercial sense. The result is a board that knows it needs cyber leadership but has no clear owner for it, and a security programme that stalls, drifts, or simply never gets started.

Cyberfort's Virtual CISO Starter Service changes that. You get immediate access to a senior cyber professional who understands your business, can speak credibly to your board, and can drive your security programme forward, without the overhead, the recruitment risk, or the delay of a permanent appointment. This is not a helpdesk. It is strategic cyber leadership, on your terms.

What is the situation organisations are facing?

Cyber risk has become a board-level issue, but governance hasn't kept pace. Boards are being asked to sign off on cyber strategies, respond to insurer questionnaires, demonstrate regulatory compliance, and take accountability for data protection, without a qualified senior professional to advise them or own the programme.

The most common consequence is not a dramatic breach. It is a slow accumulation of risk: policies that exist on paper but aren't enforced, risk registers that haven't been reviewed in a year, a security roadmap that was written once and never updated.

By the time the gap becomes visible through an incident, an audit finding, or a failed insurance renewal, the work to close it is significantly harder than it would have been with consistent oversight.

At the same time, hiring a full-time CISO is out of reach for many organisations. The market for experienced cyber leaders is competitive, salaries are high, and the role requires a level of ongoing demand that many businesses cannot sustain. The fractional model exists precisely because most organisations need a CISO's judgement.

What our customers say about this service

"We had a board that kept asking about cyber and an IT team that kept saying everything was fine. Our Cyberfort vCISO was the first person who could speak both languages, and what they found in the first few weeks made it very clear that everything was not fine. Within three months we had a risk register that actually reflected reality, a board pack that made sense, and a roadmap we could fund. It changed the conversation completely."

Chief Operating Officer, Financial Services

"We were going through an acquisition and the buyer's due diligence team asked for a security programme overview. We didn't have one. Cyberfort stepped in, got us to a credible position quickly, and helped us present it in a way that gave the buyer confidence. It almost certainly saved the deal."

CEO, Technology Business

Key Challenges Without Cyber Leadership

No clear ownership of cyber risk
When nobody owns it, nobody drives it. Security initiatives sit in IT backlogs, risk registers gather dust, and the board has no single point of accountability.

Governance without substance
Many organisations have a cyber security policy and not much else. Without a senior professional to operationalise governance - running reviews, tracking risks, holding teams accountable ,documentation becomes a compliance exercise rather than a genuine control.

Inability to speak the board's language
Technical security teams often struggle to translate risk into the financial and reputational terms that boards understand and respond to. A vCISO bridges that gap, turning technical findings into business-level insight.

No roadmap, no momentum
Without strategic direction, security investment is reactive, driven by the last incident, the most recent audit, or whoever shouted loudest. A vCISO provides the forward-looking programme management that turns isolated activity into measurable improvement.

Pressure from outside is increasing
Cyber insurers are asking harder questions. Enterprise customers are issuing security questionnaires as standard. Regulators are raising expectations. Without qualified leadership to respond, organisations lose contracts, face premium increases, and fail audits that should have been straightforward.

Who is this service for?

Cyberfort's Virtual CISO Starter service is designed for organisations that:

- Have no dedicated CISO or Head of Security, and are feeling the gaps in their security strategy
- Face increasing pressure from regulators, insurers, or customers to demonstrate formal cyber governance
- Have a cyber security programme that has stalled or lacks clear direction and ownership
- Are going through growth, M&A, or digital transformation that is outpacing their existing security maturity
- Want board-ready reporting and risk oversight without building an internal function from scratch

If your board is asking "who owns cyber?" and the honest answer is "nobody, really" - this service is for you.

What does a typical engagement look like for this service

1 Step 1 - Onboarding & Current State Assessment
Your assigned vCISO spends structured time with your leadership team, IT function, and key stakeholders to understand your business, risk environment, current security posture, and strategic priorities. This produces a clear baseline and an agreed focus for the engagement.

2 Step 2 - Governance Framework & Risk Register
We establish or refresh the foundational governance structures: a working risk register, a security policy framework, and the reporting cadence that will keep your board informed and your programme on track. Where formal documentation exists, we assess and update it. Where it doesn't, we build it.

3 Step 3 - Security Roadmap Development
Drawing on the assessment and governance baseline, your vCISO develops a prioritised security roadmap that reflects your risk profile, budget, and business objectives. This is not a theoretical framework, it is a practical, owned plan with clear milestones, accountabilities, and investment guidance.

4 Step 4 - Ongoing Leadership & Board Reporting
Your vCISO provides regular leadership sessions, attends board or risk committee meetings as required, tracks progress against the roadmap, responds to external stakeholders (insurers, auditors, customers), and evolves the programme as your business and threat landscape change.

This is the ongoing value of the engagement - consistent, expert oversight that keeps your cyber programme active and effective.

Key deliverables

- Monthly Virtual CISO Leadership Sessions
- Board and Risk Committee Reporting Pack
- Cyber Risk Register (established or refreshed)
- Security Policy Framework
- Prioritised Security Roadmap
- Governance Oversight and Programme Management
- Stakeholder and Insurer Response Support

Business Value

- Provides immediate, credible strategic cyber leadership
- Improves governance maturity and board-level accountability
- Accelerates risk management and security programme delivery
- Reduces commercial and regulatory exposure from governance gaps
- Supports compliance, insurance renewal, and customer assurance requirements
- Lays the foundation for broader cyber transformation at a pace that fits the business

Key outcomes from this service

Organisations that use Cyberfort's Virtual CISO Starter Service gain:

A credible senior cyber leader - An experienced Cyberfort vCISO who understands your business, can represent your security programme to any audience, and provides the board with a named, accountable owner for cyber risk.

A working governance framework - Risk register, policy framework, reporting structure, and accountability model, built to be proportionate to your organisation, not copied from a template.

A prioritised security roadmap - A forward-looking, business-aligned programme that turns security investment into measurable improvement, with clear milestones and owners.

Board and executive reporting - Regular, jargon-free reporting that gives leadership the visibility they need to discharge their responsibilities and respond confidently to external scrutiny.

External stakeholder confidence - The ability to respond credibly to insurer questionnaires, customer security assessments, regulatory enquiries, and audit processes, backed by a documented, active programme.

Next Steps

Your board is asking who owns cyber. The honest answer shouldn't be "nobody."

Book a 30-minute call with one of our cyber leadership specialists to understand where your governance gaps are, what the consequences of leaving them unaddressed look like, and how a Virtual CISO Starter engagement could close them - faster and more cost-effectively than you might think.

Contact us at **info@cyberfortgroup.com** or call **+44 (0)1304 814800**.

To find out more about our full range of cyber security services visit **cyberfortgroup.com**

Cyberfort
Expert-led. Security Driven.

DATA SHEET