scyberX

"Are We Secure?"

Nobody could give the board a confident answer.

This is the story of how a UK non-profit moved from security uncertainty to structured, defensible governance — and what it actually took to get there.

SECURITY GOVERNANCE | FRACTIONAL CISO | BOARD LEADERSHIP

The Situation: February 2025

A large UK non-profit — **~5,000 users, ~£300M revenue** — had security tools, security people, and security activity. Yet when the board asked, **"are we secure?"** — the honest answer was **"we don't know how to measure that."**

No Independence

Information Security buried under Technology. No separation. No authority.

No Risk Framework

Nothing the board could understand or act upon. Technical updates, not risk decisions.

No Budget for CISO

Full-time CISO (£120k–£150k) was not available. The leadership gap was real.

The problem wasn't capability. **It was leadership.**

What Changed in 15 Months

Security stopped being an IT problem and became a **business function**. Here is what that actually looked like.

Governance & Independence

Before: Security reported through Director of Technology. No separation between governance, assurance, and delivery.
After: Security reports to Chief Operating Officer as independent function. Three Lines of Defence model embedded. Board receives risk-based decisions using a 5-tier appetite model.

Board Confidence

Before: No confident answer existed when the board asked, "are we secure?"
After: Quarterly board reporting with clear risk position, forward-looking threats, and structured escalation. Every security decision is now defensible.

Vendor Control

Before: Passive vendor relationships. Suppliers held the power. MDR provider underperforming with no leverage.
After: Strategic vendor management established. Deep supplier assurance completed. **~£94k in hard savings** delivered through better contract negotiations.

Crisis Preparedness

Before: Leadership had never rehearsed a cyber incident.
After: Operation Guardian completed — Executive Leadership Team ran full cyber crisis simulation (Gold and Silver). They have now rehearsed what most boards never do.

> "Thank you, Sandeep. We now know what mountain we're climbing. Before this, we didn't even know if we were climbing the right mountain."
>
> **— Chief Operating Officer**

The Business Case

Full-time CISO at £120k–£150k didn't fit the budget — but the strategic leadership gap was real. The fractional model delivered exactly what was needed.

What They Actually Needed

- **Intensive transformation:** 12 months governance redesign, Security function restructure, Three Lines of Defence, risk framework, board integration (3–4 days/week)
- **Ongoing oversight:** Quarterly board reporting, independent assurance, supplier oversight (2 days/week)
- **Flexibility:** Dial up during critical periods. Dial down once foundations embedded

What Was Delivered

- Same CISO-level leadership, matched to actual organisational need
- Head of Information Security recruited £13K under budget
- Security Analyst roles established — permanent team built
- **~£140k total commercial value** (~£94k hard savings + ~£50k added capability)
- **ROI positive within 8 months**

When This Model Works

Fractional CISO makes sense when you need **strategic governance transformation**, not 40 hours per week of operational firefighting. You probably recognise this situation.

Security Sits Within IT

No independent voice. Governance, assurance, and delivery are not separated.

Board Has No Confident Answer

"Are we secure?" — and nobody can give a structured, defensible response.

Budget Gap Is Real

£120k+ full-time CISO is not feasible, but the strategic leadership gap is genuine.

Vendors Hold the Power

Contracts are not optimised. No leverage for change. Suppliers drive the relationship.

Regulatory or Audit Pressure

Recent audit, incident, or regulatory scrutiny has exposed governance weakness.

Translation Gap

Security speaks technical. The board speaks risk. Nobody bridges the two.

If that sounds familiar, **this is the conversation worth having.**

Sandeep Jaryal

scyberX

Fractional CISO | Security Governance & Leadership

I help organisations move from security uncertainty to structured, board-ready governance. Currently engaged with 2 organisations with **limited capacity for new clients in 2026**.

Security Governance

Three Lines of Defence, risk frameworks, board integration

Strategic Leadership

CISO-level expertise without full-time cost

Vendor & Commercial

Supplier assurance, contract optimisation, hard savings

If your board is asking **"are we secure?"** and you don't have a confident answer — **let's talk.**