How We Rescued a Failed Network Security Programme: A Case Study in Programme Recovery

Introduction

Three failed implementations. £2.3 million spent. Zero endpoints secured. A global retail organisation facing regulatory pressure, reputational risk, and a team that had lost confidence in the programme.

This is the story of how we turned a failing network security programme into a success. Not by starting from scratch, but by applying structured governance, disciplined change management, and clear accountability to rescue a programme that had already consumed significant resources.

The recovery took 18 months. The outcome: 100,000+ endpoints secured, global deployment with zero disruption, and a knowledge transfer strategy that sustained the solution beyond go-live.

The Situation: A Programme in Crisis

Scale and Scope:

The client is a major UK retailer with over 300+ stores, 15,000+ employees, and a complex IT estate spanning multiple data centres, remote offices, and retail locations. Their network security programme aimed to implement:

- Network Access Control (NAC) across all endpoints
- Endpoint protection and vulnerability management
- Security policy enforcement at scale

- Real-time threat monitoring and response

The Problem:

Three previous implementation attempts had failed over five years:

First attempt (Year 1): Big-bang rollout across all 100,000 endpoints. The organisation applied a software deployment model to a security governance problem. Endpoints became locked down without adequate preparation, user support, or communication. Within two weeks, store operations ground to a halt. IT teams spent weeks reverting changes. The programme was abandoned.

Second attempt (Year 2): Phased rollout by geographic region. Insufficient testing in live environments. Compatibility issues with legacy systems only discovered during regional deployments. Regional IT teams pushed back against enforcement policies they hadn't agreed to. Rollout stalled at 15% completion. The programme was paused.

Third attempt (Year 3): Gradual enforcement with centralised control. Lack of stakeholder alignment. Business units discovered that the security policies conflicted with operational requirements that they hadn't communicated. Escalations to the CFO stalled the programme for six months. By the time alignment was attempted, the original business case had expired, and funding was reallocated.

The Impact:

After more than three years and £2.3 million in consulting, software licenses, and internal resources:

- Zero endpoints were secured
- Leadership confidence in programme delivery had collapsed
- The security team was blamed for "failed change management"
- Regulatory auditors had flagged the lack of network controls as a compliance risk
- The original programme sponsor had moved on, leaving no clear ownership

A change in thinking was needed to address the mess and recognise it as a governance problem, not a technical one.

Our Approach: Structured Governance and Stakeholder Alignment

The Root Cause Analysis:

We spent the first two weeks understanding what had gone wrong. The issues weren't technical:

1. **No clear governance structure** - No one owned accountability for the programme. Decisions were made by consensus, which meant no decisions got made.

2. **No stakeholder alignment** - Different leaders had different expectations. Security wanted enforcement. Operations wanted flexibility. Business units wanted no disruption. These conflicts were never explicitly resolved.

3. **Inadequate change management** - Previous attempts treated this as a technical deployment, not an organisational change. IT teams and end users weren't prepared.

4. **Scope creep and scope misalignment** - The original business case covered NAC. By attempt three, the scope had grown to include vulnerability management, threat monitoring, and policy enforcement without corresponding budget or timeline adjustments.

Our Recovery Plan:

We recommended a fundamental shift: treat this as a programme governance and change management problem, not a technical one.

Phase 1: Reset and Alignment (Weeks 1-4)

We established explicit governance:

Decision Rights Matrix: One person (the CIO) owned go/no-go decisions. The Security Director owned technical decisions. The COO owned operational impact decisions. Clear escalation paths for conflicts.

Stakeholder Alignment Workshop: We brought together all stakeholders—Security, IT Operations, Business Units, Finance, Compliance—and made them agree on:

- What success meant (not just "endpoints secured," but "endpoints secured with zero operational disruption")
- What trade-offs were acceptable (enforcement vs. flexibility)
- What the rollout approach should be (phased, not big-bang)
- What would trigger a pause or reset

Scope Baseline: We documented exactly what was in scope (NAC) and what was out of scope (vulnerability management, threat monitoring—phases 2 and 3). We got stakeholder sign-off.

Phase 2: Proof of Concept and Learning (Weeks 5-12)

Instead of jumping to rollout, we proved the approach worked:

IT Staff Pilot: We deployed NAC to 100 IT staff endpoints first. Not to "test technology," but to teach IT teams how to support the solution and develop workarounds for edge cases.

Iterative Learning: We held weekly retrospectives with IT staff. What broke? How did they fix it? What documentation did they need? What training would end users need?

Policy Refinement: We worked with IT staff to refine security policies based on real operational constraints they discovered. If a policy broke a legitimate business process, we either changed the policy or found an alternative enforcement approach.

Phase 3: Test Store Rollout (Weeks 13-24)

With IT staff as advocates, we moved to test stores:

Five volunteer stores: We picked five geographically diverse stores with different operational profiles (high-traffic urban, suburban, rural).

Embedded IT support: We placed dedicated IT support staff on-site. Their job: solve problems in real-time and document solutions.

User feedback loop: We conducted daily stand-ups with store managers, till operators, and staff. What was working? What caused friction?

Communication strategy: We didn't just deploy technology. We explained why security policies existed, what users needed to do differently, and how to get help.

Phase 4: Regional Rollout (Weeks 25-78)

Once test stores proved the approach worked, we rolled out to regions:

Regional IT ownership: Each region got trained and certified IT staff who owned deployment and support in their region.

Graduated enforcement: We deployed with monitoring first (collect data, identify issues), then phased enforcement (apply policies gradually, allow time for workarounds).

Executive steering: The CIO attended regional rollout kickoffs. This signalled that the programme mattered and had leadership support.

Phase 5: Knowledge Transfer and Sustainability (Weeks 79-78)

Before declaring victory, we built internal capability:

Support team training: We trained 40 internal IT support staff to own NAC support permanently.

Documentation and runbooks: We created detailed documentation of how to diagnose issues, apply policies, and troubleshoot problems.

Escalation procedures: We established clear procedures for when issues needed expertise beyond internal staff.

The Results

Delivery Metrics:

- 100,000+ endpoints secured across 600+ stores, all regional offices, and data centres
- Zero operational disruption - stores remained operational throughout rollout
- 95% schedule adherence - completed in 78 weeks against an 82-week plan
- 5% budget variance - delivered within budget despite the previous three failed attempts

Quality Metrics:

- Zero security incidents post-go-live related to NAC policy conflicts
- User adoption: 98% of users completed required security training
- Support tickets: Dropped 60% after month 4 as users became proficient

Business Impact:

- Regulatory compliance: Passed full security audit with no network control gaps
- Risk reduction: Eliminated the compliance audit finding
- Cost avoidance: Avoided an estimated £800k in additional security incidents if the programme had continued to fail
- Capability: Built internal expertise that sustained the solution beyond go-live

Key Lessons: Why This Worked

1. Governance Precedes Technology

The first three attempts failed because they treated this as a technology problem. It was a governance problem.

Clear decision rights meant we could make trade-offs quickly. When enforcement conflicted with operations, we didn't debate endlessly. The CIO made a call, and we moved on.

2. Stakeholder Alignment Must Be Explicit

We didn't assume stakeholders agreed. We made them sit in a room and explicitly resolve conflicts before we deployed anything.

This changed the conversation from "How do we deploy NAC?" to "What do we need to achieve together, and what trade-offs are we willing to make?"

3. Change Management Is Not IT Support

Previous attempts provided IT support. We provided change management.

We taught IT staff to support the solution. We prepared users to use it. We communicated why the policies existed. We gathered feedback and refined the approach. This is fundamentally different from deploying software.

4. Proof of Concept De-Risks the Programme

By proving the approach worked with IT staff first, then test stores, we eliminated the risk of a global rollout failing again.

Leadership gained confidence. IT staff became advocates. Users saw it work before it affected them.

5. Phased Rollout Enables Learning

A 100,000-endpoint big-bang deployment is too risky. Phased rollout allowed us to learn from each phase and adjust the next.

We discovered policy conflicts in test stores, not after the global rollout. We improved support processes in the first few regions, not retroactively across all regions.

The Broader Pattern

This case study reflects a pattern we see repeatedly in mid-market programmes:

Programmes don't fail because of technical complexity. They fail because:

- Decision rights are unclear
- Stakeholders have conflicting expectations
- Change management is treated as IT support
- Scope grows without explicit approval
- Accountability is diffused

These are governance failures. They're fixable, but they require structure.

Conclusion

The retail organisation didn't need new technology. They needed a different approach to programme governance and change management.

By establishing clear decision rights, explicitly aligning stakeholders, applying disciplined change management, and proving the approach worked at scale before the global rollout, we transformed a failing programme into a success.

The security endpoints are now protected. The internal team owns the solution sustainably. The organisation learned how to deliver programmes at scale.

And the Leadership Team learned a critical lesson: governance precedes technology. Invest there first.

Next Steps

If your programme is at risk, or if you've experienced failed implementations like this, the path forward starts with governance.

We work with organisations to:

- Diagnose governance gaps

- Establish clear decision-making structures
- Align stakeholders around explicit trade-offs
- Apply change management discipline
- De-risk rollout through proof of concept and phased approaches

If your programme is at risk, or you want to assess your governance gaps, book a free 15-minute Discovery Call.

We'll review your programme against these five failure points and identify specific governance improvements that will get you back on track.

Email: info@sjhsolutions.co.uk
Phone: 07857 315259
Website: sjhsolutions.co.uk/resources

SJH Solutions
Fractional Programme Director Services
Email: info@sjhsolutions.co.uk | Phone: 07857 315259
Website: sjhsolutions.co.uk/resources