



CASE STUDY · CYBER RESILIENCE & NETWORK ASSESSMENT

Aligning to NCSC Best Practice

A well-established UK prep school operating across a modern, technology-led environment. As with much of the education sector, the school relies on a complex mix of cloud services, on-premise infrastructure and connected devices, all of which sit within one of the most heavily targeted sectors in the world for cyber-attack.

IN THIS STORY

Formation Tech were engaged to assess the school's alignment to NCSC best practice across both the human and network sides of cyber security. The engagement uncovered critical oversights, including a CCTV system openly exposed to the internet on a network shared with core servers in Azure, and led to a strategic roadmap of prioritised improvements that delivered both stronger security and a better digital experience for staff and teachers.

01

CHALLENGES

A Sector Under Pressure, and Hidden Exposure Within It

Education is one of the most attacked sectors in the world. Schools hold significant volumes of sensitive data on pupils, parents and staff, and increasingly rely on technology to deliver day-to-day teaching. That combination, high-value data, broad attack surface and limited specialist security resource in-house, **makes the sector a consistent target.**

Most cyber incidents start with the human side: phishing and social engineering, the most common and relatable route in. But while the human layer is typically the way in, **the damage rarely happens at point of entry**, it happens because of what an attacker is able to do after they get in.

This prep school wanted an objective view of where it stood, in a way that could be communicated to governors, aligned to budget realities and used to set priorities. Behind that was a clear regulatory horizon: **NCSC guidance and the Cyber Assessment Framework, which all schools are expected to align with by 2030.**

02

SOLUTION

Two Foundational Assessments, One Strategic View

Formation Tech engaged the school using its two foundational assessments aimed at education: the Cyber Resilience Quick Assessment (CRQA), **focused on the human side of cyber security**, and the Cyber Networks Quick Assessment (CNQA), **focused on the network side**. Both are designed to give IT managers, governors and senior leaders an objective view of where the school's risks really sit, measured against NCSC best practice.

The assessment of the network environment surfaced several critical oversights that left the school significantly more exposed than the team had appreciated. A CCTV system had been left open to the internet, **sitting on a network equally exposed to core servers** running in Azure. Unsegregated networks meant that compromise of any lower-hanging fruit would have been felt far more widely across the school than it should have been.

These are exactly the kinds of issues an NCSC-aligned assessment is designed to surface, specific, fixable exposures no longer seen by those closest to the environment.

03

OUTCOMES

A Roadmap That Improves Both Security and Digital Experience

The assessment delivered a strategic plan to resolve the issues identified, structured around an initial set of quick wins that **immediately reduced the school's exposure**, followed by a longer roadmap of more significant improvements. Crucially, the **roadmap was designed to align with the school's budget** and funding cycles, recognising that the right plan is the one a school can actually deliver.

The outcome went beyond security. The network environment underpins teaching, communication and the day-to-day experience of staff and pupils. By addressing it at a foundational level, the work didn't just close down risk, **it improved the digital experience of staff** and teachers.

More broadly, the case illustrates how the CRQA and CNQA work as a pair. **NCSC best practice covers both the human and the network sides** of cyber security, and so does the assessment programme, giving leaders a communicable view of where to focus.

For schools navigating the path to alignment with the 2030 CAF educational frameworks, the value is not just in the technical findings, it is in giving leaders and governors an objective view of where to put their priorities, and a plan that fits how schools actually operate.

RESULTS AT A GLANCE

2

NCSC-aligned assessments covering human and network risk

Critical

Internet-exposed CCTV and core servers identified and resolved

Phased

Quick wins plus a roadmap aligned to school budget and funding

2030

Aligned to NCSC and CAF educational framework requirements

See where you stand against the NCSC best practices.

[Book a Discovery Call](#)