Northampton College

Strengthening Cybersecurity Compliance and Resilience

Northampton College is one of the UK's largest further education colleges, serving over 10,000 students across Northamptonshire, England. With campuses in Northampton and Daventry, the College offers a wide range of practical and technical qualifications, A Levels, T Levels, apprenticeships, and courses for adults. Committed to maintaining a secure and inclusive learning environment, the College prioritises the safety and integrity of its IT infrastructure.

The Challenge

As part of an Education and Skills Funding Agency (ESFA) mandate, Northampton College needed to complete a rigorous IT Health Check (ITHC) to secure compliance and ensure system integrity.

Educational institutions like Northampton College face unique cybersecurity challenges, including:

- Protecting sensitive student and staff data
- Managing a complex IT estate across multiple locations
- Mitigating risks from outdated software and unpatched systems
- Securing network access across diverse campus facilities

To meet these challenges, the College sought an experienced partner to conduct the ITHC and safeguard its systems against potential cybersecurity threats.

Exposure Management

Education

> Working with Celerity and their partner Cyber Crowd has been excellent. The expertise provided from both companies has enabled us to further secure our digital estate. I can always rely on Celerity to provide solutions or guidance to the college's projects

Northampton College
Technology Manager

Partnering with Celerity & CyberCrowd

Recognising the critical importance of robust security measures, the college turned to its trusted cybersecurity partner, Celerity, with whom it has maintained a longstanding relationship. To further elevate their security posture, CyberCrowd, an NCSC Level 2 Assured Service Provider, was also introduced into the project.

CyberCrowd's CREST-approved ITHC services include certified penetration testing and vulnerability scanning, essential for identifying and mitigating security gaps. With a collaborative approach led by ICT Services Manager Andy Seymour, the process was carried out seamlessly, minimising disruptions to college operations.

> Andy Seymour commented: "In today's digital age, ensuring the security and integrity of our IT infrastructure is paramount. Regular testing and compliance checks are essential to maintain our high standards and protect our community."

The comprehensive ITHC covered critical areas of the college's IT infrastructure, including:

- **External Infrastructure Testing:** Examining email and web servers, firewalls, and VPNs to prevent unauthorised access.

- **Internal Infrastructure Testing:** Sampling devices and servers across the network to assess security posture.

- **Wi-Fi Security Assessment:** Ensuring secure wireless access points and network integrity.

- **Firewall Configuration Review:** Verifying firewall rules to block unauthorised entry.

- **Device and Server Security:** Reviewing staff and student devices for updates and assessing server configurations to identify vulnerabilities.

Enhancing Security Outcomes Through Proactive Vulnerability Management

Prompt Vulnerability Reporting
Key vulnerabilities were identified and addressed during testing, strengthening the College's security posture.

Real-Time Visibility
The Client Pen Test Portal provided real-time access to test results and risk assessments.

Enhanced Incident Management
Improved capability to detect and handle future security incidents.

Actionable Remediation
Each vulnerability came with tailored recommendations for cybersecurity improvements.