



Overview

BCIS is the UK's leading provider of construction cost and pricing data. For 65 years the organisation has supported the built environment with trusted data, forecasts and consultancy services used by surveyors, insurers and developers.

BCIS collects, collates, analyses, models and interprets construction cost and carbon data, delivered through online applications, data licensing and publications. The company's head office is in Coventry, with an additional office in Harrogate.



Challenge

In May 2025 an admin account without MFA was compromised, risking systems and client trust. BCIS needed clear forensics, decisive containment and practical steps to stop recurrence.

Like many growing organisations, BCIS wanted always-on coverage without a 24x7x365 SOC. Attacks span identities, endpoints, email and cloud. Without unified telemetry and automation, teams drown in alerts while real threats slip through.

They also wanted to maximise their existing Microsoft investments. The challenge was stitching controls, tuning detections and driving fast response. MXDR had to deliver outcomes, not another tool to manage.

BCIS®

At a Glance

Customer: Building Cost Information Service (BCIS)

Organisation Size: 100

Industry: Business Services - Construction Data & Analytics

Solution: MXDR as a Service, Cyber Incident Response

Products: Microsoft Defender XDR, Microsoft Sentinel,



Solutions

Cyber Incident Response

CyberOne mobilised within hours, isolating the threat and confirming no data was exfiltrated. Our NCSC certified Cyber Incident Response service produced a plain-English forensic report with regulator-ready Information Commissioners Office (ICO) guidance, then enforced urgent guardrails including global MFA and hardened privileged access.

Managed eXtended Detection & Response

Post-recovery, BCIS onboarded CyberOne's MXDR for 24x7x365 monitoring and response. We integrated Microsoft Defender XDR - unified detection and response across identities, endpoints, email and SaaS - with Microsoft Sentinel the cloud-native SIEM, to provide full visibility, high-fidelity detections and rapid containment.

Why Microsoft?

BCIS wanted to maximise existing Microsoft investments and use integrated security rather than build a patchwork of tools. Defender XDR and Sentinel work as one platform across Microsoft 365 and Azure, reducing complexity, speeding investigations and lowering cost to serve. As a Microsoft Security Solution Partner with a MISA-verified Managed XDR solution, CyberOne brought proven methods to tune signals, automate playbooks and demonstrate value quickly.



Results

CyberOne operates as an extension of the BCIS team, providing continuous detection, investigation and response backed by monthly service reviews and continuous tuning.

- **Incident Contained With No Downtime Or Loss:** Operations remained stable throughout.
- **100% Coverage:** All endpoints and cloud services integrated with Defender and Sentinel.
- **Faster Response With 24x7x365 Security Operations Centre:** With average response time under 1 minute.
- **Enhanced Security Posture:** Enforced MFA, hardened privileged access, increased detection coverage.
- **Operational Confidence:** Leadership and clients have assurance backed by always-on response.
- **High Satisfaction:** 100% customer satisfaction rating from BCIS since onboarding.
- **Zero Breaches Since Partnering With CyberOne:** Validated through continuous SOC oversight.
- **Cost-Effective Resilience:** Leveraging Microsoft's enterprise-grade security platform, ensured BCIS maximised existing investments, avoiding multiple third-party vendors, resulting in cost savings and operational simplicity.

This integrated Microsoft-led security approach positions BCIS to protect services and data more effectively, enabling confident growth with a resilient always-on defence.



"CyberOne gave us a clear explanation of how the breach happened and what to do next - exactly what we needed."

Alan Churley, Product & Engineering Director, BCIS

"CyberOne has become an extension of our team. We're extremely pleased with the service."

Mattia Colombo, Senior DevOps Engineer, BCIS

About CyberOne

A Microsoft Security Elite Partner and member of the Microsoft Intelligent Security Association (MISA), delivering world-class AI-augmented Managed Extended Detection & Response (MXDR) services. Our Microsoft-verified Managed XDR solution combines Microsoft's security platform with CyberOne's accredited experts to help organisations prevent, detect and respond to modern cyber threats faster while accelerating cyber maturity and maximising Microsoft investments.

Through our 24x7x365 Global Security & Network Operations Centre (SNOC), CyberOne provides continuous protection supported by NCSC-accredited Cyber Incident Exercising and Response, CREST-accredited SOC services and Penetration Testing, alongside clear, measurable service level agreements (SLAs). CyberOne's Consulting, Professional and Managed Security services help organisations protect critical operations, strengthen compliance and move confidently from cyber risk to cyber resilience.



+44 (0) 3452 757575

hello@cyberone.security

cyberone.security

