

Cygnnet Healthcare

Case Study

Delivering efficient, next-generation cyber security consultancy.



Overview

Founded in 1988, Cygnnet Health Care has, for more than 30 years, provided specialist mental health treatment, rehabilitation and support services, working closely with the NHS to ensure the highest quality of care is provided to all patients.

With a dedicated care team of more than 8,800 employees, working across 150 sites nationally, Cygnnet Health Care continually strives to make a positive difference to the lives of more than 3,000 individuals, through a wide range of specialist services for individuals with mental health needs and earning disabilities within the UK.



Challenge

As a large and diverse organisation, spread across 150 UK locations, Cygnnet Health Care's IT footprint is both large and complex, supported by a dedicated in-house IT team to allow Cygnnet to efficiently manage their network.

Working in healthcare, Cygnnet has always understood the importance of prioritising the security of patient data amongst other sensitive data. In 2018, Cygnnet wanted to engage with a specialist cyber security provider to assess and review their cyber security controls and current security posture.

Specifically, Cygnnet sought to stay ahead of the security battle with a comprehensive assessment to understand what was needed to remain secure, given the increased complexity of threats and the size of their estate, which had grown through acquisition.

At a Glance

Customer: Cygnnet Healthcare

Organisation Size: 5,000–9,999

Industry: Healthcare and Social Care Services

Solutions: Cyber Risk Assessment, Cyber Essentials PLUS and Penetration Testing



“Given the complexity of today's cyber threats, Cygnnet wanted to review their security to understand what was needed to keep them secure from such risks.”

Dominic List, CEO, CyberOne

The identified programme of improvements and ongoing security assessments would ensure Cygnnet was employing best practice security processes, with an ongoing programme of assessment to identify and address any new cyber security risks faced.



Solution

The first phase was to baseline Cygnet's current security posture, to review and understand existing security processes, technologies and controls.

To do this, CyberOne conducted a range of security assessments and consultancy projects to provide both a holistic and objective grading of the current state of Cygnet's security controls, with additional penetration tests and vulnerability scans to uncover any critical security exposures in Cygnet's network.

From this baseline, CyberOne were able to provide a graded programme of improvement, which broadly fell into three core activities:

1. Programme of identified improvements across Cygnet's people, processes and technologies, prioritised by risk based on CyberOne's review and identified recommendations.
2. An on-going programme of penetration testing/vulnerability scans to validate improvements, identify any new known vulnerabilities and drive a continual programme of testing, improvement and review to ensure the highest levels of security governance are maintained.
3. Elevate Cyber Essentials certification to Cyber Essentials PLUS - While Cyber Essentials certification provides a good baseline, Cyber Essentials PLUS provides a higher security bar and will become a requirement for NHS suppliers to achieve the highest level of certification.



Results

• Understanding Current Cyber Security Posture

CyberOne helped Cygnet realise where they stood in terms of security and addressed any discovered vulnerabilities to protect them from potential risks.

• Level of Risk Defined

Cygnet gained an objective understanding of the risks faced, specific to their business, and what their security priorities were.

• Ongoing Security Programme

An improvement programme, together with ongoing security assessments has provided Cygnet with a comprehensive cyber security strategy and robust programme to continually assess and improve.

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

