BCHC PARTNERS WITH CYBERGUARD TO TACKLE CYBER SECURITY AND STRIDE TOWARDS MEETING DSPT STANDARDS

CASE STUDY

Birmingham Community Healthcare NHS Foundation Trust (BCHC)

NHS
Birmingham
Community Healthcare
NHS Foundation Trust

CyberGuard
Technologies

About BCHC

BCHC provide over 100 community-based clinical and specialist services to patients living in and around Birmingham. The services are accessed in a wide range of locations such as community hospitals, health centres, clinics, community centres, schools, care homes and dentists, as well as being delivered to patients in their own homes. As a community healthcare trust, one of its key drivers is to help relieve pressure on the acute health care system, namely the Queen Elizabeth Birmingham Hospital (QE).

The challenge at a glance

- Hugely dispersed workforce creating vast threat landscape
- Immense amount of highly sensitive patient data stored
- Internal IT team focussed on delivering frontline IT services
- Internal IT team without cyber security expertise
- Inability to recruit and retain cyber experts with the NHS

> **"...a silent but potentially devastating cyber threat lurking in the wings at BCHC."**
>
> Tom Godfrey - Business Consultant, CyberGuard

Number of employees: 5,500
Internal IT team: 77 staff / contractors
Partnered with CyberGuard since: April 2020
Location: 100 sites around Birmingham
Website: www.bhamcommunity.nhs.uk

The background

BCHC is a typical NHS Trust, with thousands of employees working in over one hundred sites across a large city – in this case Birmingham. The disparate nature of the workforce and the IT landscape was making cyber security extremely difficult to effectively implement for BCHC's stretched IT resources, compounded by a lack of in-depth cyber security knowledge internally. Furthermore, the Trust's IT team has an unwavering priority to deliver IT services that enables its clinicians to provide patient care, meaning cyber security was being reluctantly de-prioritised across the Trust.

This sizeable challenge was in the shadow of the infamous WannaCry ransomware attack that bought other NHS Trusts across the UK to a standstill in 2017. It resulted in the cancellation of thousands of appointments and operations, and the frantic scramble to continue NHS services with pens, paper and employees' own mobiles and laptops. Ever since there's been widespread acknowledgement that the NHS was suffering something of a cyber security crisis, being at serious risk of another attack. With responsibility for tackling cyber security down to each Trust, BCHC needed to devise its own cyber defence, gain funding for it and continue to support imperative front line IT services.

Joining forces with CyberGuard

Traditionally, CyberGuard offers its expertise to commercial entities to provide cyber security, however we recognised there was a potentially greater need in the public sector for better cyber security – in particular the NHS. We reached out to Trusts across our region to introduce ourselves and how we could help. BCHC were delighted we had made contact at a time when they had gained funding to invest in cyber security, with the goal of reaching DSPT compliance, spear-headed by their Head of IT, Gerard Kilgallon.

Tom Godfrey, CyberGuard Business Consultant said: "There was a silent but potentially devastating cyber threat lurking in the wings at BCHC when I first began talking with Gerard. I knew our team could offer everything needed to make the Trust so much safer in terms of its data and system security. They needed expertise, and we could offer that, within their budget constraints.

BCHC point of view

BCHC's Head of IT, Gerard Kilgallon, commented: "Ever since WannaCry in 2017, the Trust's Board of Directors and I recognised we needed to up our game in regard to cyber security and give it the resource it demands. That said, the IT function of the Trust is to support our clinicians to deliver healthcare services and that is always what comes first. Our staff need a working, supported, performing IT system and that's our focus."

At CyberGuard it's something we regularly hear: internal IT teams are at full capacity delivering the day-to-day IT infrastructure to keep their organisation operational. Dedicating resources to cyber security isn't realistic, despite understanding the substantial risk an unprotected, vulnerable network poses. For BCHC, the failure to have effective cyber security measures in place could have led to an impact in patient care and reputational damage to the Trust; it was a precarious position.

Finally, over 2 years after WannaCry, BCHC was awarded funding to build a robust defence of its systems and data (including some NHS Digital funds). Initially Gerard planned to recruit his own cyber specialists to join the Trust but it quickly became apparent that employing a cyber security team was easier said than done. A skills shortage in the UK means salaries were beyond the scope of BCHC's budget. "Paying market rates for such a person is just not feasible in the NHS," he said, "and every pound spent on IT is, quite simply, a pound of public money not spent on patient care, something I am acutely aware of, and responsible for."

"Tom [CyberGuard Business Consultant] opened the Trust's eyes to using third party expertise, and I clearly saw that CyberGuard was the missing part of the Trust's IT and cyber strategy. They could provide proper 24/7 network monitoring, threat detection, patch management, response mechanisms and regular network traffic inspections: all of which were taking a back seat to critical day-to-day work."

Project begins with a proof of concept

At the time of BCHC's and CyberGuard's first conversations in early 2020, another NHS Trust suffered a significant security breach which proved the importance of the discussion, and the urgency to act.

To kick off the project for BCHC, following a period of fact-finding, assessment, audit and solution design, CyberGuard ran a 'proof of concept' for the Trust for a number of weeks. This essentially allowed the Trust to see our security service and teams in action, and rigorously test it in situ, before committing.

Simultaneously, we set up a Critical Incident Response Service for the Trust. This enabled our Security Operations Centre (SOC) to investigate, react and remediate any threats at source; starting the pro-active protection of the Trust's systems and data.

As intended, the proof of concept irrefutably demonstrated that our service could be integrated with the NHS's complex infrastructure to ensure visibility, and therefore detection, of threats against their infrastructure from both an internal and external point of view.

Soon after, we expanded the scope of the SIEM solution (Security Information & Event Management) to transform the communication between all the Trust's existing security products, that were active but not being monitored. This provides us with a clear picture of any threats to the Trust, along with possible attack vectors, so we can escalate & respond accordingly on their behalf. Then, we performed a CREST-approved internal and external penetration test on both the standard internet line and on the Trust's HSCN connectivity, identifying specific flaws and weaknesses needing our remediation.

Gerard reflects on the first stage of the partnership: "The proof of concept went as well as it possibly could have from our point of view. Tom, and others at CyberGuard, Paul Colwell and Sean Tickle in particular, managed the process of integrating new systems and protocols seamlessly, not an easy feat within a complex NHS organisation. From there, we've built things up gradually, passing more and more responsibility to CyberGuard until they now manage the entire infrastructure's security."

Dealing with security and sensitive data is second nature to us at CyberGuard so we absolutely understand the requirement for us to build trust with our clients over time. Each and every Trust that we deal with will hopefully welcome our ethos to take the journey to a cyber secure position step by step, building confidence as we go, all the while ensuring proper and efficient spend of public funds.

"The department works well within the spirit of the DSPT and I can confidently assert we're meeting the criteria thanks to our CyberGuard partnership."

Gerard Kilgallon, BCHC

"All Trusts know there is a very real cyber threat but the skills shortage within the NHS means there is not the in-house expertise to tackle it... I've basically chosen to give this part of the problem to CyberGuard, who have been unfailingly helpful in this process of getting us cyber secure."

Head of IT, BCHC, Gerard Kilgallon

One year later

Twelve months on from the beginning of the partnership, our responsibility for BCHC's cyber security has developed to include a whole suite of security services and TTPs (tactics, techniques and procedures.)

"Previously, when completing the Trust's DSPT submission, it was a challenge to tick all of the boxes regarding cyber security," reflected Gerard. "Now, the department works well within the spirit of the DSPT and I can confidently assert we're meeting the criteria thanks to our CyberGuard partnership. One of the main things for me is a team of highly skilled people at our disposal, a true extension to our team. We even have a WhatsApp group for making urgent contact in the event of an incident. It's very reassuring at a time when the growth in cyber crime is prolific."

BCHC summarises

"All Trusts know there is a very real cyber threat but the skills shortage within the NHS means there is not the in-house expertise to tackle it, nor the time to monitor and manage the various security systems. I've basically chosen to give this part of the problem to CyberGuard, who have been unfailingly helpful in this process of getting us cyber secure. NHS organisations can be difficult to work with at times, due to the pressure of working somewhere where life and death is the priority, but CyberGuard are true professionals and really understand what it takes to work with us. This project brings a huge amount of relief to the Trust; knowing we're now more than adequately protecting ourselves."

"A big, faceless organisation wouldn't have suited us as a security partner. CyberGuard's relatively small size means we have been able to develop a tight relationship because it's a consistent group of professionals that we deal with. It's a huge advantage for us, and reinforces the Trust's preference for Tier 2 suppliers."

"I would absolutely recommend the team at CyberGuard and have full belief that my decision to outsource cyber security is the right decision for this Trust."

Working with the NHS

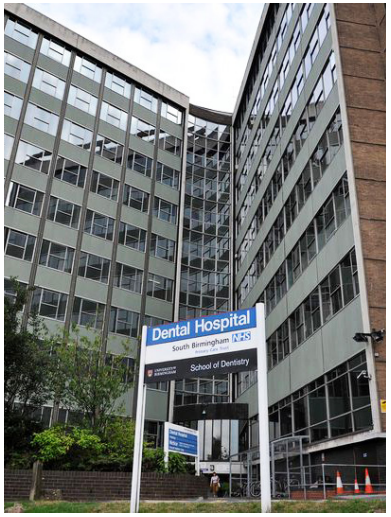
Taking our skills and expertise into the public sector has been thoroughly rewarding for CyberGuard, particularly at a time when the NHS has suffered unprecedented pressure due to the pandemic. The NHS is a precious public service and we're proud to be working in partnership to keep BCHC's network and highly sensitive data protected from cyber threats.

Technical solutions at a glance...

- Manage, Detect & Respond service: Managed SIEM and SOC solution utilising Microsoft Sentinel and ATP for endpoint
- 24/7/365 server infrastructure support with remote monitoring
- Patch management for 5,500 end user devices
- Penetration testing: Standard internet line and HSCN connectivity
- Working towards recommendations of Cyber Essentials
- Flexible retainer-based support
- Temporary helpdesk
- Tabletop exercises
- Ongoing consultancy

"...full belief that my decision to outsource cyber security is the right decision for this Trust."

Head of IT, Gerard Kilgallon



YOUR TRUSTED CYBER PARTNER

Speak to us about protecting your NHS organisation

- Trusted cyber experts
- Proven NHS experience
- Technical excellence

Tom Godfrey
Cyber Security Business Consultant

Sean Tickle
Head of Cyberguard

Paul Colwell
Technical Director

CyberGuard Technologies

NHS

01299 873 800
nhs@cg-tech.co.uk
www.cg-tech.co.uk/nhs

Worcester Road, Stourport-on-Severn, Worcestershire DY13 9AT
0967 CYB CSC 100821 A