SOPHOS
Cybersecurity evolved.

NHS Cybersecurity in 2022

Keeping patients and their data safe

As one of the world's largest employers, with over 1.5 million staff and comprising hundreds of individual organisations, the NHS is undoubtedly challenging to protect. Although digital transformation had always been a part of the NHS Long Term Plan, it accelerated due to the pandemic. The use of technology is now, more than ever, critical for the delivery of successful patient care. However, as we become more digitally dependent, is the NHS at risk from not paying enough attention to cyber threats?

A Sophos Whitepaper. October 2021

Post-Wannacry – what did we learn?

In 2017, WannaCry was the cybersecurity wake up call that no NHS trust wanted to have. NHS organisations weren't targeted specifically – they were simply collateral damage. However, the ransomware spread rapidly across networks, affecting over a third of English trusts and over 600 other NHS organisations, with an associated cost of £92 million. As the dust began to settle, it was recognised that a coordinated approach to cybersecurity, underpinned by investment, would be crucial. NHS Digital created an NHS Cybersecurity Operations Centre (CSOC) to provide a bird's eye view of the network; developed the Data Security and Protection Toolkit (DPST) to ensure that organisations were working towards the same standards; upgraded machines to a common operating system (Windows 10) and asked organisations to install Microsoft ATP on all devices.

Digital transformation in the NHS

In the late nineties, the NHS identified the need for seamless sharing of data between IT systems and began developing the national standards to accompany this. Just over 20 years later, NHSX was launched to drive digital transformation in the NHS, with a target of 2024 for trusts to reach a 'core level of digitisation'. However, no one foresaw the rapid changes that would lie ahead. When the pandemic hit, the NHS leveraged technology to help solve the challenging problems that COVID-19 posed for continuity of patient care. In the beginning, NHS Digital pulled together vast amounts of patient data to form the shielding patient database; people rapidly adopted the NHS app and the Covid app was developed for Test and Trace. The ability to carry out remote consultations using video technology became critical, as did the sharing of data and radiographic images between clinicians. And we can't forget the vaccine rollout, which relied on data sharing to identify the order in which people were vaccinated and to book their appointments. Together with many staff switching to remote working, these changes meant that suddenly healthcare became much more digitally dependent. This progression will only continue as integrated care systems develop and link hospital and community services across regions.

The high level of additional connectivity and data sharing that the NHS has achieved in a short space of time is impressive, but also opens organisations up to significant risks from cybercriminals. Healthcare is very much in the sights of cyberattackers: it seems it is no longer a case of 'if' but rather 'when' the next severe breach will happen.

An underfunded area

The NHS Long Term plan stated that it expected trusts to contribute £3 billion towards digital transformation between the financial years 2019–20 and 2023–24. However,

according to the National Audit Office's 'Digital Transformation in the NHS' May 2020 report, it was considered that there was a 'significant risk' that trusts would either be 'unwilling or unable' to fund this. It also states that at a local level 'trusts' expenditure on IT varies widely and collectively they spend less than the recommended level'. With cybersecurity spend only making up part of the overall IT budget, and with resources often prioritised by trusts towards those that appear to impact patient care directly, it is easy to see how cybersecurity could be undervalued. Underinvestment has serious consequences, one of which is the burden of legacy equipment. Although progress has been made to secure it, there is still more work to do.

Organisational structures and the cybersecurity skills gap

Although the CSOC provides guidance, the responsibility for cybersecurity, and the burden of risk, remains squarely with each trust. Across the NHS, cyber capabilities vary greatly. Some organisations are considered to be 'exemplars', while others struggle to meet standards. Due to the interconnectedness between organisations, this disparity in digital maturity could put the whole NHS network at risk if a significant breach occurs.

IT teams within the NHS are often stretched and confusion around roles and responsibilities exists. Typically, fewer staff are assigned to cybersecurity than a corporate organisation of a similar size, with employees having to divide their time between a variety of different tasks. To make matters worse, the NHS often has difficulty attracting and retaining cybersecurity professionals because they aren't as well paid as their corporate counterparts. Clearly, work needs to be done to create fulfilling careers for IT staff by investing in their personal development. This could involve formalising an NHS cybersecurity career path, with opportunities for IT staff to collaborate with different trusts, contribute to journal articles and work with the centre.

The role of the board and all employees

With memories of Wannacry fading, there is a concern that trusts are forgetting the lessons learnt and are no longer as cybersecurity-focused. However, the present-day risk of cyberattacks poses a significant threat to patients' safety, both from disruption to their clinical care and the security of their data. Cybersecurity should no longer be IT teams' sole responsibility, and a whole organisation approach is needed. This begins at the top with board engagement: members control budgets, set strategies and if a significant breach occurs, they are ultimately responsible. CEOs, CIOs and CCIOs need to understand why not investing in cybersecurity is a false economy. Bringing in people, such as non-executive directors with cybersecurity experience, can be helpful, as can board packs to translate cybersecurity concepts into language that is relatable.

Preparation for a breach is critical – all NHS trusts should have an incident response plan, which identifies key stakeholders. This should cover areas such as how to notify staff of a breach, provide continuity of care in the absence of digital systems and protect critical assets. In addition, trusts should carry out tabletop exercises (role play scenarios) so that IT teams and technical staff know how to respond. The NCSCs 'Exercise in a Box' is a highly recommended toolkit to help with this.

As individual staff members' machines are often the gateways for cybercriminals, all employees should complete Data Security Awareness Training, as set out in the DPST and participate in regular phishing simulations to raise awareness.

Today's threat landscape

In recent years, ransomware groups have become more professional, with well organised company-style structures and ransomware as a service (RAAS) affiliate schemes. It is not the case that threat actors only encrypt data and demand payments for decryption keys, but they increasingly exfiltrate valuable data and threaten to publish or sell it on the dark web.

The impact of any cyberattack can often be felt long after the criminals move on. In the case of the Conti ransomware attack on the Irish HSE, healthcare organisations suffered widespread disruption, with cancellation of outpatient and radiology appointments and some hospitals reverting to paper records. Despite the later release of the decryption key without payment, disruption endured for several months. On 28 May 2021, the HSE also confirmed that confidential data from 520 patients had been leaked online. Unlike WannaCry, the HSE disruption was not a product of collateral damage caused by untargeted malware; it was a deliberate attack.

During the pandemic, cybercriminals, including state actors, have focused their attention on the healthcare sector, particularly in relation to vaccine research and rollout. The NCSC Annual Review 2020 reported that between 1 September 2019 and 31 August 2020, they 'handled 723 incidents, with around 200 related to coronavirus'. NHS trusts are experiencing regular attacks on their infrastructure and the fact that we aren't hearing about them in the news doesn't mean that a battle isn't going on behind the scenes.

In today's world, it is no longer enough to simply deploy antivirus software across networks and expect to be protected. Malware and hacking used to be two different threat landscapes; however, they have merged over the last five years. Attackers are stealthy – if IT teams don't play an active part in looking for signs of a breach, then cybercriminals can use (often legitimate) tools to enter and move around a network undetected, simply waiting for the right opportunity to strike. 'Hands-on attacks', where the adversary goes interactive within a customer's estate, are becoming increasingly common and can unfold at lightning speed, quickly overwhelming staff. If this happens, it's crucial that an organisation has the expertise to respond rapidly at any time of day or bring in incident response services to assist.

Avoiding breaches – the cybersecurity solutions

For an organisation to mount an effective defence against cybercriminals, IT teams often use Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) tools. These monitor and scour the network for suspicious behaviour and Sophos XDR is one such solution.

With XDR tools, cybersecurity staff can analyse and contextualise critical data from multiple sources, including endpoints, servers and firewalls, allowing them to have a holistic view of precisely what is happening within their environment. Potentially suspicious activity can be interrogated and actions taken, even for devices that have been knocked offline.

However, it takes real expertise and time to use XDR tools effectively. One issue with XDR is that it can throw up numerous alerts that require investigation and triaging, burdening already overstretched IT staff. This can pose a problem for NHS organisations, which often lack the ability to run their own security operation centres in-house.

In these circumstances, buying in a Managed Threat Response (MTR) service is a solution. At Sophos, a human-led threat hunting team works together with AI technology to hunt, detect and respond to suspicious activity 24/7/365, maintaining an ongoing dialogue with IT staff. More than just a notification service, the team's level of involvement is entirely within an

organisation's control – from validating threats and removing all the 'noise' of false positives to carrying out targeted actions on an IT team's behalf. Because these threat hunters are so familiar with malicious behaviour, once detected the issue is often resolved within the hour.

Having a specialist MTR team in your corner at all times – whether it is in the middle of the night, at a weekend or on a bank holiday – ultimately provides you with peace of mind, knowing that you're doing all you can to keep your core services running and your patients safe.

Conclusion

With the provision of tools and guidance from the centre, NHS organisations have made significant progress in bolstering their cyberdefences since the WannaCry outbreak.

However, with a continually changing threat landscape, securing the NHS as a whole requires a collaborative team effort between the centre, local organisations and key suppliers, such as Sophos, to make sure that no NHS organisations are left behind. By working together, we will have the best opportunity of minimising security incidents and keeping patients and their data safe as digitalisation continues apace.

Learn more about ransomware and how Sophos can help you defend your organization.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2021-10-05 (SB-NP)

SOPHOS