SOPHOS
Cybersecurity delivered.

Cybersecurity for Integrated Care Systems in England

A Sophos Whitepaper. May 2022

The changing face of healthcare

Healthcare in England is undergoing major reform and this summer will see the arrival of 42 integrated care systems (ICSs)[1]. These are new partnerships between organisations that meet health and care needs across an area, and include hospitals, clinics, nursing homes, carers, GPs and other healthcare trusts. This development represents a major change in how healthcare has been run in England for the past decade.

The Health and Social Care Act 2012 abolished primary care trusts and strategic health authorities simultaneously transferring around £80 billion[2] in funding to several hundred clinical commissioning groups. This division of funding resulted in a fragmented landscape in terms of policy, staffing and technology deployment.

It is hoped that these reforms, which are part of the NHS Long Term Plan, will lead to greater collaboration and coordination of services, improve population health and reduce inequalities between different groups. There are, however, numerous technology challenges to overcome before this hope becomes reality. Not least of which is improving cybersecurity.

The changing face of technology in healthcare

Digital transformation has always been a part of the NHS Long Term Plan, but it accelerated as healthcare providers reacted to the onset and impact of COVID; from pulling together vast amounts of patient data to form the shielding patient database, to rapidly rolling out the NHS and Test & Trace apps. This is in addition to enabling thousands of staff to work remotely and millions of patients to receive consultations online. All of these changes meant that healthcare became much more digitally dependent. This progression will accelerate further thanks to the arrivals of the ICSs.

1 *https://www.leadinghealthcare.co.uk/2021/03/25/nhs-rolls-out-final-13-integrated-care-systems-across-england/*

2 *https://en.wikipedia.org/wiki/Health_and_Social_Care_Act_2012*

The use of technology is now, more than ever, critical for the delivery of successful patient care. Thanks in equal parts to the speed at which technology was rolled out and the previously very fragmented healthcare landscape, the new ICSs are faced with an uphill cybersecurity battle. Faster technology adoption, tighter budgets, fewer skilled IT people all point to major challenges ahead for ICS CIOs and boards, who would be mistaken to assume it will be business as usual when it comes to cybersecurity.

The changing face of cybersecurity

More technology and greater fragmentation mean more points of weakness, and therefore more potential for successful cyberattacks. Ransomware was the leading threat in healthcare as attackers sought to take advantage of disparate systems and dispersed people during the pandemic. The Sophos State of Ransomware in Healthcare 2021[3] reported 34% of healthcare organisations were hit by ransomware in the previous year, and 65% who were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack.

Ransomware attacks have moved on since WannaCry in 2017. Healthcare providers in England were not directly targeted but they did suffer collateral damage when it spread across networks, affecting over a third of English trusts and over 600[4] other NHS organisations, with an associated cost of £92 million[5]. 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 Windows Defender Advanced Threat Protection (ATP) on all devices.

3 *https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf*

4 *https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware*

5 *https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled-0*

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.

Cybersecurity is a multi-layered threat

The threat posed by ransomware attacks is particularly damaging for ICSs who are hamstrung to a certain degree by a UK government policy that refuses to pay out to ransom demands. According to Sophos data, the average bill for rectifying a ransomware attack in healthcare, considering downtime, people time, device cost, network cost, lost opportunity and the ransom paid in 2021, was in the region of £1.85 million[6]. Not a penny of any ransom paid came from the UK government. Ransomware gangs do not know or care that their demands will not be paid out by the UK government, they will launch attacks regardless.

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 Health Service Executive (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[7] 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 experienced 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.

Barriers to transformative security

As ICSs in England consolidate their operations, it will result in more data being shared across networks and greater commonality of systems. This will result in more points of weakness and more cybersecurity risk. All of which is coming at a time when ICSs are moving forward with wider digital transformation initiatives.

CIOs are faced with three key, immediate challenges with digital transformation. First is the complexity of the existing or legacy platforms and software across a fragmented landscape. Second is the requirement to address security and compliance - the immediacy of this requirement can lead to quick fix solutions, which does not help with long-term challenges. The third challenge is a lack of skills with new technologies such as cloud, AI and cybersecurity.

6 *https://www.itpro.co.uk/security/ransomware/359364/cost-of-ransomware-doubles-in-a-year*

7 *https://www.irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136*

Healthcare providers are increasingly looking towards managed service providers to help with these challenges. As the strategic importance of technology increases in line with its complexity, the role of the IT professional in healthcare is moving up the value chain, from implementation expert responsible for building, deploying and maintaining solutions, to technology orchestrator responsible for long term goals and strategy.

Long term prevention is better than the cure

Security, like insurance, is something you hope you never need, but absolutely must have in place from a compliance perspective and to manage risks. In fact, ICSs would be well placed to work on the assumption that an attack will happen and ensure they have a tried and tested incident response plan that can be implemented immediately to reduce the impact of the attack. Complicating matters, threats are constantly evolving as criminals try new avenues of attack against the latest security. For instance, phishing is become ever more sophisticated and difficult to spot, especially in environments with high staff turnover using fragmented IT architecture.

Too many cyber breaches are caused by the inadvertent actions of users. Therefore, it is important that users are educated about the cyber risks they face and the safeguards in place to protect them. They should also understand their individual cybersecurity responsibilities, be aware of the consequences of negligent or malicious actions, and work with other stakeholders to identify ways to work in a safe and secure manner.

As individual staff members' machines are often the gateways for cybercriminals, all employees should complete Data Security Awareness Training[8], as set out in the DPST[9] and participate in regular phishing simulations to raise awareness.

Avoiding breaches – the cybersecurity solutions

ICSs are faced with the choice to either manage IT themselves, locally or regionally, or outsource. Most healthcare organisations do not have the right tools, people, and processes in-house to effectively manage their security programme around-the-clock while proactively defending against new and emerging threats. Furthermore, healthcare organisations who do invest in cybersecurity solutions often fail to deploy them fully or use them to their full potential – significantly reducing their effectiveness and increasing the likelihood of a successful, but preventable breach.

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.

With XDR, 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 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 ICS organisations, which often lack the ability to run their own security operation centres in-house.

In these circumstances, buying into a Managed Detection and Response (MDR) service is an ideal 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.

8 *https://www.ncsc.gov.uk/information/cyber-security-training-schools*

9 *https://www.dsptoolkit.nhs.uk*

Conclusion

With a continually changing threat landscape, securing ICSs requires a proactive and collaborative team effort between the centre, local organisations and key suppliers, such as Sophos, to make sure that no ICS 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.

Having a specialist MDR 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.

Sophos MDR offers different levels of support, giving you options around the control you wish to retain or hand over to our team. Plus, there's a wide variety of trusted Sophos security products that work side by side with MDR, all managed from within the Sophos Central platform for total visibility of your estate. Choose from Standard or Advanced Sophos MDR[10] – whatever you decide – you'll be safe in the knowledge that our dedicated security personnel will identify and eliminate threats before they can even become an issue.

10 https://www.sophos.com/en-us/products/managed-threat-response/how-to-buy

To learn more about Sophos MDR or to talk to a Sophos expert about the service for your ICS

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.

© Copyright 2022. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2022-09-07 (WP-PC)

SOPHOS