SOCURA

HEALTH AND CARE EDITION

Cyber Security in a Post-Pandemic World

Managing advanced threats in a new digital era

“The world in which we work has changed and now, so must we. This year we have seen unprecedented digital transformation and we want to ensure that organisations can continue to evolve by enabling a secure environment 24/7.”

MARC CHANG – NED & FOUNDER

FOREWORD:

Preparing for WannaCry 2.0

It's nearly four years since the WannaCry ransomware campaign caused serious disruption to NHS IT systems. Today, the health service C-suite is better prepared for such a threat, but the goal posts have also moved somewhat. An explosion in remote working endpoints and new technology investments brought about by the pandemic has created fresh security challenges and visibility gaps. At the same time, malicious actors have responded with more sophisticated targeted threats, while long-standing issues around NHS funding remain. Are you ready for the next WannaCry, or something worse?

The NHS has come a long way with its cyber security posture under incredibly challenging conditions. The best practices that comprise good IT hygiene, like prompt patching and effective anti-virus are far more commonplace than they were four years ago. But adversaries have also been honing their skills and adapting their tactics with ample support from a vast cyber crime economy. Advanced Persistent Threat (APT) techniques, once the preserve of a limited few, are being widely adopted in "human-operated" ransomware campaigns.[1]

This goes far beyond ransomware, of course. Data theft, hijacked devices, crypto-mining and other threats all add to the burden on IT security teams. One estimate from 2020 claims over two-thirds (67%) of UK health and care organisations (HCOs) had suffered a security incident in the past year. [2]

Marc Chang, NED & Founder

AUTHORS

Marc Chang,
NED & Founder
Marc is passionate about building teams and organisations that at their heart use technology to bring positive change to society and improve people's lives. He founded Socura to help organisations address the rapid rise of cyber security threats and make the digital world safer.

Jamie Brummell,
CTO & Founder
Jamie is a cyber security leader with over 20 years of experience working with multinational organisations, security vendors, and systems integrators. Jamie works with senior executives, architects, analysts, and engineers alike; helping them manage cyber risk and improve their cyber defence capability.

Andrew Kays,
CEO
Andy is the CEO at Socura where he is responsible for delivering and optimising the company's services. He has over 20 years of experience growing and managing cyber security companies and specialises in building high performing teams to deliver outcomes for customers.

[1] https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
[2] https://www.clearswift.com/blog/2020/01/22/infographic-cybersecurity-challenges-uk-healthcare-sector

Contents

A Special Case

To an extent, security and business leaders in all sectors must contend with similar threats. Yet in health and care, the stakes couldn't be higher. The news of a patient's death following a ransomware attack on a German hospital is a tragic example of what can happen in a worst-case scenario.[3] A US study from 2019 revealed that even hospital data breaches can significantly increase the 30-day mortality rate for heart attack victims.[4] The proliferation of connected devices also exposes trusts to the risk of "cyber physical" attacks, where virtual threats, for example, sabotaging drug infusion pumps, have a real world impact.

It's also true that the NHS is a unique institution with some specific challenges of its own that set it apart from most others. These include well-publicised resource and funding constraints, and a complex organisational structure which, it has been argued, leads to overlapping competencies, and slow incident response.[5] In addition, most trusts do not have a dedicated Chief Security Officer (CSO) or similar. While an individual will be tasked to take on these additional responsibilities, for cyber security to work effectively in an organisation it has to be something that is part of everyone's role.

Like organisations in many sectors, the NHS is coming to terms with life in the shadow of a pandemic. The digital and workplace changes the crisis has accelerated are likely to become the norm long after it has receded, which means new approaches will be needed to secure more distributed IT systems and the data flowing through them. The good news is that progress here is possible - and it needn't break the bank.

Over the course of this paper we'll take a closer look at some of the key challenges facing NHS leaders and we'll detail how certain approaches can help to drive continuous proactive protection, rapid incident response and more efficient allocation of resources.

3. https://www.bbc.co.uk/news/technology-54204356
4. https://onlinelibrary.wiley.com/doi/abs/10.1111/1475-6773.13203
5. https://www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf

Health and Care's New Normal

The challenges facing health and care leaders today are not necessarily brand new. But they have certainly been made more acute over recent months. They range from industry skills gaps to human error, digital transformation to new cyber attack techniques.

All hands on deck

The cyber security sector has for the past few years been facing something of an existential crisis. As digital investments grow and threat actors become more aggressive, the need for cyber security professionals across various disciplines has soared. Many of these roles have been newly created, and training is failing to catch up with the surge in demand. Employers sometimes exacerbate the problem by failing to cast the net wide enough when looking for new recruits. The result? A headline shortfall in cyber security professionals of just over three million, including hundreds of thousands in Europe.[6]

It's therefore a challenge that affects employers across all sectors in the UK today. But in health and care the problem is compounded by revenue constraints. Figures cited in a report in The Lancet claim that NHS investment in IT "can be as little as 1-2% of the annual budget on IT compared with 4-10% in other sectors.[7]" A separate poll of senior business decision makers in UK HCOs last year reveals that just a quarter (24%) feel cyber security budgets are adequate.[8] Attracting the brightest and best therefore becomes that much harder when pay scales are significantly below market rates. The idiosyncrasies of NHS funding mean that budget is often spent on technology, rather than on those needed to operate it.

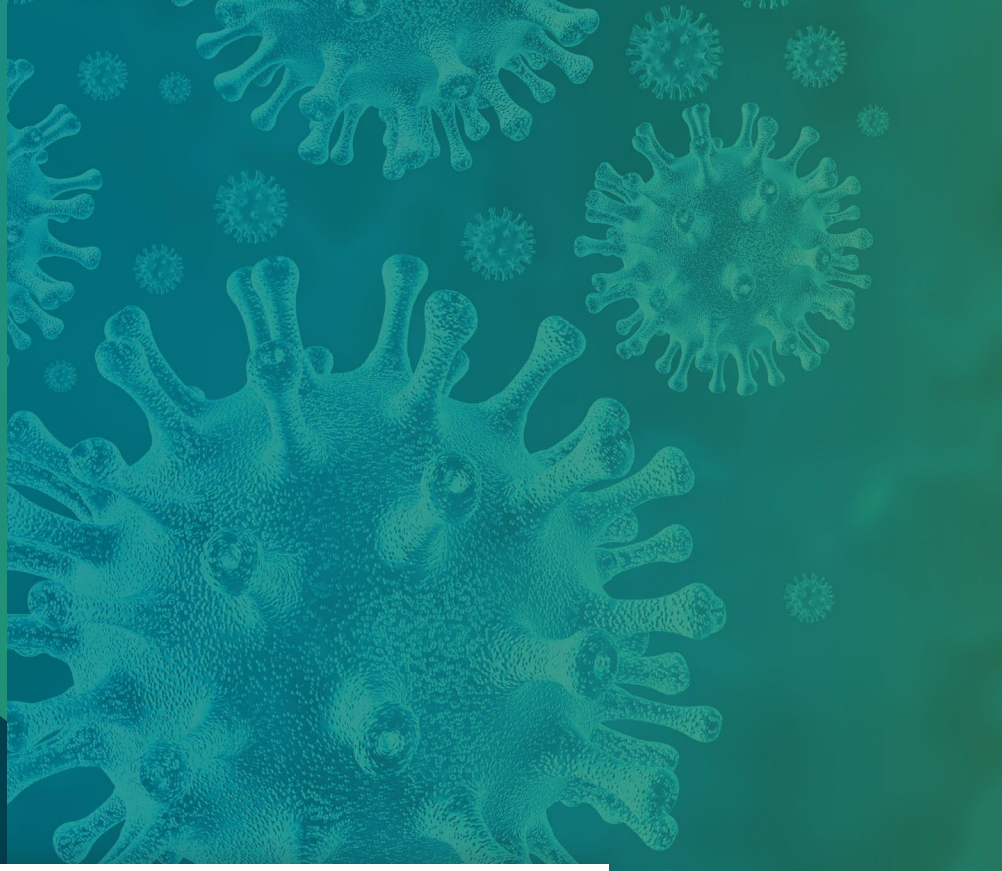
SOCURA
INSIGHT

It may not be possible to find candidates for cyber security roles with the exact experience you desire

Look further afield for expertise and experience, nurture and train people and teams

Outsource capability to gain from the economies of scale of cyber companies

6. https://www.isc2.org/Research/Workforce-Study
7. https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30005-6/fulltext#back-bib7
8. https://www.clearswift.com/about-us/pr/press-releases/healthcare-cybersecurity-research-2020



The COVID factor

With COVID-19, the pressure has been turned up even further on stretched IT security teams, with many being drafted in to help rewire IT as hospitals are reconfigured to focus on COVID related care. Others may have been called on to support the transition to remote working for many staff, further depleting the time they have to focus on high-value security tasks. One survey from early 2020 reveals that nearly half (47%) of global cyber security professionals had been taken off some or all of their typical security tasks to support other IT-related jobs.[9] Others may be struggling themselves with home working. Only 59% of global respondents to a separate April 2020 survey said they feel their cyber security team has the right tools and resources at home to perform their job effectively.[10]

Of course, these trends are not just COVID-related: the decentralisation of care in general has led to many employees working remotely and across multiple sites. As HCOs get used to new ways of working, these pressures will relax. But like their counterparts in many sectors, NHS cyber security professionals will continue to struggle with their workload, in the face of rising threat levels and remote working visibility challenges.

The problem is also made harder by tooling, especially in detection and response, where overlapping solutions can add to complexity and coverage gaps. Tool sprawl is a major industry problem which saps productivity and overwhelms teams with alerts: one estimate claims most organisations today run over 50 security products.[11] A greater focus on efficiency and productivity targeting is required in this area.

[9] https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/04/28/ISC2-Survey-Finds-Cybersecurity-Professionals-Being-Repurposed-During-COVID-19-Pandemic
[10] https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2020/isaca-survey-cybersecurity-attacks-are-rising-during-covid-19
[11] https://panaseer.com/business-blog/cisos-tool-sprawl/

2 Shining a light on IT blind spots

As discussed, the arrival of COVID-19 lockdowns forced UK HCOs, like organisations operating in most sectors, to support mass remote working. According to official figures from April, nearly 50% of people in employment did at least some work at home, rising to almost three-fifths (57%) in London.[12] While absolutely necessary to help to prevent the spread of the disease and protect the NHS, this had major consequences for cyber risk in these organisations. As is often the case, cyber criminals reacted quickest to the changes - adapting phishing campaigns to target distracted remote workers desperate for news on the pandemic, and exploiting security gaps in remote working infrastructure itself.

Google alone said it was blocking 18 million daily malware and phishing emails related to COVID-19 by April 2020.[13] The National Cyber Security Centre (NCSC) claimed that a quarter of the threats it dealt with over the past year were COVID-related.[14] For the NHS and many other organisations this represents a challenge on several fronts:

[12]. https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/coronavirusandhomeworkingintheuk/april2020

[13]. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

[14]. https://www.ncsc.gov.uk/news/annual-review-2020

VPNs have struggled during the pandemic to do their job of supporting secure remote working. They were never intended to support such large numbers of workers, meaning many have become overloaded, harming employee productivity and potentially forcing users onto unmanaged channels to work and collaborate. As VPNs turned into remote working bottlenecks, many organisations also had problems deploying patches out to remote endpoints. One global study reveals that 43% of IT ops leaders had problems patching the personal devices of home users.[15] As we'll discuss, vulnerable VPNs also became a target for attackers in their own right.

Visibility problems are hampering security leaders' efforts to secure the remote workforce. This is partly connected to the VPN issues outlined above. But the more fundamental concern is, if IT leaders are unable to understand where their IT assets are and where individuals are using personal devices, they can't effectively manage cyber risk. One study from April claims that 94% of global IT decision makers have discovered endpoints in their organisation that they were previously unaware of and over half (54%) do so at least every week.[16] It goes without saying that what you can't see, you can't protect, with regular patches or mandatory anti-malware.

Remote workers are prone to making mistakes. Despite their best intentions, the truth is that cyber security is at its core a people problem. Phishing has become a top threat vector for attackers precisely because it works so well. There's strong evidence to suggest that those at home may be even more likely to click through on something suspicious.[17] The problem is amplified by the fact that many may be connecting to work networks from personal devices which aren't suitably protected.

One global study finds that even though most (72%) remote workers say they are more conscious of their organisation's cyber security policies since lockdown began, large numbers: use non-work apps on corporate devices (56%); use their work laptop for personal browsing (80%); and often or always access corporate data from a personal device (39%).[18] All of these scenarios represent varying degrees of security risk which training can help to mitigate, but which ultimately security controls and detection services are needed to manage.

SOCURA
INSIGHT

Use multi-factor authentication

Make your staff cyber aware through training

Remote workers may not be captured by network monitoring. Use an agent to monitor endpoint activity

Follow the principle of least privilege - avoid giving users admin permissions wherever possible

15. https://world-at-home.tanium.com/
16. https://www.tanium.com/blog/critical-it-visibility-gaps-persist-despite-tens-of-millions-spent-on-compliance/
17. https://www.mimecast.com/resources/ebooks/cybersecurity-awareness-company-issued-computers-survey/
18. https://newsroom.trendmicro.com/2020-07-01-Trend-Micro-Finds-72-of-Remote-Workers-Have-Gained-Cybersecurity-Awareness-During-Lockdown

3 Digital innovations must be secure by design

The health and care sector may not always have been on the cutting-edge of technology adoption, but that is changing, in part thanks to the pandemic. Most obviously it has forced many GP consultations onto digital channels, and home workers to collaborate with colleagues online. But there is more. The crisis has unshackled digital innovation as leaders see the necessity of accelerating change, just as it has in countless other sectors. This cultural change will long outlive the pandemic. But now it's time to focus on security as a vital pre-requisite of lasting digital success.

The Future's Cloudy

In January 2020, NHS Digital finally completed migration of two key public-facing services, the e-Referral Service (e-RS) and the NHS 111 Directory of Services (DoS), to public cloud infrastructure. Many more are set to follow under the government's Cloud First policy.[19] On the one hand, outsourcing IT to a proven provider can offer major benefits in terms of reliability and cost savings. It's also increasingly recommended from a security point-of-view.[20]

NHS organisations must remember that their security responsibilities continue even under these new contracts. Providers are very clear about where they begin and end, under the Shared Responsibility model.[21] It's somewhat concerning that a majority of cyber security professionals misunderstood the model, when quizzed about it last year.[22] Such an oversight could leave these organisations exposed to attacks.

SOCURA INSIGHT

When used appropriately and configured correctly, public cloud can be more secure than on-premises environments. However, you must make sure that you understand the risks, what the cloud provider is securing, and what you are responsible for.

19. https://digital.nhs.uk/news-and-events/news/two-national-nhs-services-move-to-the-cloud
20. https://www.ncsc.gov.uk/whitepaper/security-benefits-of-a-good-cloud-service
21. https://aws.amazon.com/compliance/shared-responsibility-model/
22. https://www.centrify.com/resources/reducing-risk-in-cloud-migrations/

A second major risk associated with enhanced spending in the cloud is that it can both increase IT complexity and create a broader attack surface for cyber criminals to aim at. Organisations like the NHS aren't just spending with one cloud provider, they're putting data into multiple cloud environments from multiple vendors, creating multi-hybrid clouds. Nearly three-quarters (74%) of global organisations are estimated to have a hybrid cloud strategy, and even more (93%) are investing in multi-clouds.[23] This creates challenges in managing security policies, processes and protection, especially given the dynamic nature of such environments.

In-house skills shortages have already led to countless cloud data breaches and leaks, as IT administrators misconfigure settings, exposing highly sensitive customer data and IP to the public-facing internet. Even the tech giants themselves have on occasion made these mistakes.[24] The bad news is that attackers are now actively scanning for exposed cloud systems to compromise. Healthcare records would be an attractive haul for such threat actors.

Connecting Everything

A second trend in health and care is digital transformation which can create security challenges is the growing adoption of connected devices. We have seen, in some cases, 50% of devices in a Trust are OT (operation technology), rather than IT-related. These are being deployed in an increasing range of use cases, from drug infusion pumps to chemotherapy delivery and MRI scanners. They're also making their way into non-clinical areas such as smart lighting and HVAC systems for hospitals.

There's no denying the potential for such devices to radically enhance patient care, reduce costs and streamline operations, but IoT devices also represent a security risk. Why? Because they may be more difficult to patch: even if a vendor provides prompt updates, they may take longer to test given the criticality of such devices, allowing attackers a crucial window in which to exploit them. Some may not be protected with adequate access controls, while visibility gaps and a lack of network segregation further increase the risks. Further, many OT and clinical devices will only run on old versions of Windows without EDR enabled.

Fortunately, we have yet to see a major campaign against such devices. However, the challenge for IT leaders is that device volumes are growing, and they could theoretically be hijacked to conscript into botnets, held to ransom or even used to infiltrate NHS networks as part of information-stealing raids. Visibility and control is essential.

[23] https://resources.flexera.com/web/pdf/report-state-of-the-cloud-2020.pdf?elqTrackId=8e710f56b1c44fe39130b0d6168944ed&elqaid=5770&elqat=2

[24] https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/

4 The threat landscape is evolving

The cyber crime economy is estimated to be worth $1.5 trillion annually.[25] That's more than the GDP of many countries. Dark web forums and trading sites provide a readymade place to buy and sell stolen data, hacking tools, service offerings and knowledge. This, and the fact they have the advantage of surprise, gives attackers a significant head start.

Over the past year, this underground economy has helped to foment a new breed of advanced, targeted attacks using techniques that were once the preserve of only a few APT groups. Unfortunately, many of these efforts have been aimed at HCOs. In the US, the government was forced to issue an alert after cyber crime group known as Wizard Spider went after at least 20 hospitals with Ryuk ransomware.[26]

These are carefully thought-out, multi-stage efforts, far removed from the automated commodity attacks that comprise the majority of cyber threats today. Most recently they have begun by exploiting internet-facing systems such as: unpatched VPNs; end-of-life platforms like Windows Server 2003/8; misconfigured web servers and electronic health record software; and RDP/virtual desktop endpoints without multi-factor authentication enabled. They use tools like Mimikatz, Cobalt Strike and legitimate Windows features like WMI and PowerShell to steal credentials and move laterally. Persistence is sometimes maintained for months before the final ransomware payload is deployed.[27]

Just the Start

What does this mean? That UK health and care leaders should be on high alert for similar campaigns. HCOs are seen as particularly vulnerable to extortion given the strain they're under with the surge in COVID-19 patients. The relatively new tactic of stealing sensitive data before encrypting could also put trusts in a difficult position-exposing even those who have backed-up to serious cyber risk. A recent breach and extortion incident at a Finnish psychotherapy clinic shows how damaging medical information can be in the wrong hands.[28]

As more cyber criminals attain the tools and know-how they need to launch similar attacks, the risk will only increase. And while classic IT hygiene measures will work to an extent, the growth of digital infrastructure and the determination of financially motivated attackers is not to be underestimated.

What Happens Next?

The health and care sector is certainly not alone in experiencing the challenges we've discussed. Many organisations struggle to gain full visibility and control of their IT assets, especially in a new era of mass remote working. They're also impacted by an ever-expanding digital infrastructure to attack, security tool sprawl, the growing expertise of attackers and cyber security skills shortages. But having experienced disruption on a mass scale back in May 2017, the NHS knows first-hand the operational, reputational and financial damage that a serious cyber attack can have.

So where do health and care leaders go from here? What are the security steps you need to put in place to tackle WannaCry 2.0 and drive vital digital change?

A commitment to best practices as outlined in Cyber Essentials Plus and the Data Security and Protection Toolkit (DSPT) is important to provide a baseline of good security to keep threats at bay. Prompt patching, anti-malware on end-user devices, regular end-user training, network segmentation, strict user access controls and more can often be enough to repel commodity threats. The NHS secure boundary service is also a great start and will help protect trusts at the perimeter.

However, the threat from sophisticated cyber crime groups, hackers-for-hire and occasionally even nation state actors means IT security leaders must go one step further in their efforts. That means going beyond protection, to detection and response.

[25] https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

[26] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[27] https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

[28] https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland

A Three-Point Plan

When it comes to detecting and responding to advanced threats, We would recommend the following principles:

1

Understand what assets your organisation holds. A regularly updated inventory is essential here to accurately catalogue assets. You can't protect what you can't see.

2

Collect and centralise as much security telemetry from these assets as possible.

3

Invest in services that can analyse this telemetry and spot anomalous patterns indicating unauthorised activity.

These services should be capable of acting upon detections in near real-time and containing confirmed threats.

What does this mean in practice?

Many NHS IT and security leaders will have heard of endpoint detection and response (EDR) solutions, which collect and analyse data about events and behaviours on endpoints to act as an early warning against sophisticated attacks. But increasingly, organisations need to go beyond the endpoint, and collect and correlate data from across networks, and hybrid cloud environments where remote working users and highly regulated data reside.

The Value of MDR

This is where extended detection and response (XDR) and managed detection and response (MDR) come in. MDR is increasingly favoured, as building and manning a 24/7 security operations centre (SOC) in-house is hard to justify from a cost perspective. Organisations can instead utilise the economies of scale that a specialist provider offers, and the enhanced visibility they have into multiple customer environments.

For health and care leaders, MDR offers:

24/7 threat detection and response across remote, endpoint, network, cloud and OT environments.

An extension of your security team, freeing up in-house resource to be more strategic.

Rapid response to mitigate threats before they have had a chance to impact the organisation.

Swift detection and containment provides an extra layer of defence, because prevention can't catch everything.

However, in a fast-growing market, not all MDR services are created equal. Many, for example, are limited by the amount of data they can store, retain and analyse, which can impact their efficacy. Here are three questions to ask of a prospective vendor:

1. **How much security data do you collect, and is this cost-constrained?** Telemetry must be collected from every asset/device, and across all parts of the IT infrastructure (including IaaS, PaaS, SaaS, endpoints, firewalls, email, directory services, DNS, Proxies, VPN, etc). Data should go back a year for maximum visibility.

2. **By how much can you reduce attacker dwell time?** Modern threat actors often move fast. You need to reduce dwell time from days or hours to minutes through threat hunting, automated containment actions, and pre-approved playbooks.

3. **How closely will you work with my existing security team?** The best providers will work seamlessly as an extension of your in-house team, with a dedicated security analyst and customer success manager.

If you would like to find out more about how we can help you, **please contact the team at hello@socura.co.uk**