SOCURA

Cyber Security in Healthcare

“No industry is immune to threat actors and the healthcare industry is in fact further disadvantaged. A rise in telehealth has fuelled an expanding attack surface, with more practitioners needing secure remote access to patient records, against a backdrop of threat actors intentionally targeting health data more than ever.”

JAMIE BRUMMELL – CTO & FOUNDER

FOREWORD:

Managing advanced threats in a new digital era

The NHS has come a long way with its cyber security posture under incredibly challenging conditions. However over the last 18 months the health and care industry has been inundated with headlines regarding repeated vulnerabilities and cyber attacks that not only threaten health systems' and providers' digital infrastructure, but that also jeopardise the health and safety of patients themselves.

Whilst best practices that comprise good IT hygiene, like prompt patching and effective antivirus are far more commonplace than they were in previous years, adversaries have also been honing their skills and adapting their tactics with ample support from a vast cyber crime economy.

From ransomware attacks with the potential to cripple back-office operations and expose patient data, to more sinister 'killware' that can compromise vital healthcare equipment – and in turn patients – the past two years have introduced a wave of new threats that healthcare providers must address. Data theft, hijacked devices, crypto-mining and other threats all add to the burden on already stretched IT security teams.

This increased risk, coupled with a rise in demand for digital services, means that cyber security is no longer just a concern for the IT department, but can pose a serious threat to a company's performance and brand reputation. Information security is now a Board priority.

Effective cyber security practices are no longer a bolt-on or an afterthought, but an imperative.

Marc Chang

Marc Chang, NED & Founder

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, as demonstrated in May 2021 when Conti ransomware hit the Irish Department of Health and the Health Service Executive. According to a recently released post incident review by PwC analysts, "many hospitals were forced to cancel outpatient appointments completely, while others were operating with significant delays." Also, the incident had a "significant impact" on diagnostic services and radiotherapy services, "with cessation of radiation treatment across the five HSE centres." For some of the affected patients, this incident likely had severe consequences.[1]

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. 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 how to provide appropriate levels of security against a backdrop of a dissolved perimeter, where staff work from anywhere and workloads are everywhere. This is particularly poignant as the NHS works to put the new Integrated Care System (ICS) structure in place and must implement effective security controls not only locally but across regions too.

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.

"Many hospitals were forced to cancel outpatient appointments completely, while others were operating with significant delays."

"Significant impact" on diagnostic services and radiotherapy services, "with cessation of radiation treatment across the five HSE centres."

[1] HelpNet Security - Healthcare Cyber Security Report Q1 2022

An evolving threat landscape

It is reported that if cyber criminals continue operating at their current rate, then, by 2025, research indicates that global cyber crime costs will reach $10.5 trillion.[2] 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.

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.

In the healthcare industry, the sheer size and complexity of the supply chain, including nuances of data access and privileges, combined with how data is increasingly moving in and outside of the system via third-party vendors has created several points of failure.

[2] Evalian - Just how big a threat is online crime? 2022

An expanding attack surface

We’ve seen several high-profile attacks on supply chains in healthcare and other industries, the most recent, a ransomware attack, which caused a major outage of multiple health and care systems. This attack resulted in disruption for many customer groups, including those who use the NHS 111 service, with Doctors saying it could take months to process mounting piles of medical paperwork.[3]

The disruptions of service that some cyber attacks lead to have immediate negative consequences, like the example above, but the compromise of sensitive data also leads to long-lasting ones. For example: identity theft, extortion, loss of patients’ trust, and considerable monetary loss by the organisation.

According to the results of the 2021 HIMSS Healthcare Cybersecurity Survey, threat actors usually go after patient information but often grab employee information, as well.

Also, cyber attackers that go after organisations in the healthcare sector don’t limit themselves to stealing only patient records. According to the results of the 2021 HIMSS Healthcare Cybersecurity Survey, threat actors usually go after patient information but often grab employee information, as well.

Compared to organisations in other sectors, healthcare organisations have the added disadvantage of dealing with a constantly expanding attack surface fuelled not only by the diverse supply chains and partnering third parties , mentioned above, but also the increased digitisation of services, a rise in IoMT and legacy devices. Many healthcare organisations use devices that run on legacy operating systems and many older healthcare IoT devices have not been designed with cyber security in mind but replacing them is out of the question because of associated cost. More on this later.

[3] BBC News - Advanced cyber-attack: NHS doctors’ paperwork piles up

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 2.7 million[4], including hundreds of thousands in Europe.

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." 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. 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.

A poll of senior business decision makers in UK HCOs last year reveals that just a quarter (24%) feel cyber security budgets are adequate.

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

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

[4] (ISC)² - Cybersecurity Workforce Study 2021

Remote working and ICS impact

Digital is central to the development of ICSs. Meaningful integrated care is not possible without the infrastructure of shared care records, interoperability and staff mobility.

This need for staff mobility, with employees working remotely and across multiple sites. increases pressure on already stretched NHS cyber security professionals. Remote working still poses a significant challenge to NHS organisations as assets move from the corporate network to untrusted networks. In many cases the security controls are no longer active or effective when devices traverse locations.

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.[5] A greater focus on efficiency and productivity targeting is required in this area, especially when organisations within an ICS will be starting from different points in terms of their digital maturity and the end goal is ubiquitous digital capabilities across the system, consolidation of services and eventually the frictionless movement of staff.

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.

[5] Security Magazine - 78% of Organizations Use More than 50 Cybersecurity Products to Address Security Issues

The Future's Cloudy

In January 2020, NHS Digital 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. 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.

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. It's somewhat concerning that a majority of cyber security professionals misunderstood the model, when quizzed about it last year.[6] Such an oversight could leave these organisations exposed to attacks.

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.[7] 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. 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.

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.

[6] AWS - Shared Responsibility Model
[7] Flexera - State of the Cloud Report 2020

Connecting Everything

Another trend in health and care is digital transformation and IoT, 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 (Operational 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. It's no surprise therefore that Enterprise IoT is the latest category of service to be added to DSPT for cyber assurance. E-IoT covers Connected Medical Devices, OT and IoT devices.

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 Endpoint Detection and Response (EDR) enabled. Data shows that 53% of connected medical devices and other IoT devices in hospitals have a known critical vulnerability.

Digital innovations must be secure by design

A recent **IoT Device Security 2022 report** lays bare the extent of the problem:

- IV pumps and patient monitors are the most common healthcare IoT devices in hospitals (38% and 19% of IoT/IoMT devices, respectively), and 73% of those IV pumps have an exploitable vulnerability
- Healthcare IoT running outdated Windows versions are prevalent in critical care sectors like pharmacology, oncology, and laboratory services (65%, 53% and 50%, respectively)

Manufacturers of healthcare IoT are much more diverse than computer or mobile phone manufacturers, and keeping all those devices secure - even just patched within a reasonable timeframe - is a complex endeavour.

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.

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 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.

Good cyber hygiene - 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.

Bridge the maturity gap - engagement from strategic senior level leadership is required to drive information security maturity.

Defend as One - Leverage the cyber community and partners to defend-as-one. Cyber is now a recognised "team sport" and requires collaborative working.

Build defence in depth - 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.

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 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**

SOCURA

Socura Limited Registered in England No. 12200836 I Email: hello@socura.co.uk I SOCURA 2022. All rights reserved