SC INSIGHTS | HEALTHCARE REVISITED

CYBER SECURITY IN HEALTHCARE: CHALLENGES AND OPPORTUNITIES

The pandemic has changed the way people live their lives, and the way the world works - and it has important implications for any company working in healthcare.

According to the British Government's Cyber Security Strategy, 'The global expansion of cyberspace is changing the way we live, work and communicate, and transforming the critical systems we rely on in areas such as finance, energy, food distribution, healthcare and transport.'

In January this year, the Government announced it was investing £2.6 billion in cyber over three years as part of the Government Cyber Security Strategy - highlighting phishing and ransomware attacks against the NHS.

For companies in the sector, security has never been more important - with cyber risk increased by the fact that delivery teams are running at chronically low levels of attendance, elevating the need for vigilance. But technological transformation also brings opportunity.

The healthcare space is facing a time of unprecedented technological change, according to authors Peter H. Diamandis and Steven Kotler in 'The Future is Faster Than You Think' - with healthcare facing huge disruption from technologies such as wearables, 5G and wireless sensors.

Stratia Cyber can help your company stay cyber secure - while taking advantage of the latest technology to boost growth.

In this edition of SC Insights, we'll explore the challenges that continue to face the healthcare sector - and illustrate how enhanced cyber resilience can help your business grow.

What's inside

Transformation and security | the numbers you need to know

442 phishing campaigns used NHS branding last year, according to Government statistics

More than a third of incidents reported to the Information Commissioner's Office affected the health or education sectors, according to the NCSC

More than a quarter (27%) of businesses face cyber attacks on a weekly basis, according to DCMS statistics

80% of businesses in the healthcare/social work/social care sector hold personal data about customers, according to the Cyber Security Breaches Survey 2021

The **most common threat (83%)** facing British businesses remains phishing attacks, according to DCMS statistics

Three-quarters of businesses (77%) say cyber security is a high priority, according to the Cyber Security Breaches Survey 2021

Healthcare is among the sectors which attaches the highest importance to cybersecurity, with **56% of organisations** attaching high importance to it

59% of companies would find it difficult to respond to a cybersecurity incident due to a shortage of skills within their team

By 2022, annual total internet traffic increased by about 50% from 2020 levels, reaching **4.8 zettabytes**, according to the World Bank

Sources

Cyber Security Breaches Survey 2022
Weekly Threat Report 6th May 2022
Cyber Security Breaches Survey 2021
What you need to know about cybersecurity in 2022

WannaCry: Building the foundations for better security

How a global cyber attack focused attention on security

In May 2017, the WannaCry cyber attack paralysed companies around the world - and created havoc in Britain's NHS.

Wannacry infected 400,000 machines worldwide in 150 countries. Forty-seven NHS organisations were affected, in what was seen as a 'watershed' moment for healthcare organisations in Britain. The attack is believed to have cost the NHS £92 million.

In the wake of the attack, NHS Wales called on Stratia Cyber.

"The IT manager might have been talking about it for years, but when you have a major breach it becomes problem number one."

"Attacks like this can concentrate people's minds on cybersecurity and get leadership attention,' says Paul Massey, Director at Stratia Cyber. 'The reason why this particular piece of work was put out for tender is that for politicians in the Welsh Assembly, WannaCry put cyber on their radar for the first time.

Massey says that attacks like WannaCry can help IT leaders build a business case for better security.

'That is true in the private sector, as well as the public sector. Ultimately, if you have a big data breach, or you have a major cyber incident that makes the news, all of a sudden that's on the board of directors' radar. The IT security manager might have been talking about this for years, but only when you have a major breach, this becomes problem number one.''

NHS Wales had not been badly affected by WannaCry, because, Massey says, the organisation had 'smart, switched on network operators' who blocked the malware early on.

Massey explained, 'They commissioned this work to say, "Okay, we dodged this one. How can we make sure we dodge the next ones?"'

We ran a web check on outward-facing sites and assessed how the organisation was handling confidential data under the General Data Protection Regulations, as well as assessing the organisations under the Network Information Systems Directive (NISD).

"OK, we dodged this one - how can we make sure we dodge the next one?"

The task involved dealing with 12 organisations in just three months, each of which had hundreds or thousands of staff and thousands of PCs. With efficiency being a main driver, we recommended a Cyber Essentials Plus audit of each organisation plus a gap analysis against the international standard ISO 27001.

Finding weak spots

Massey simplifies the main benefit of Cyber Essentials Plus: 'This helps to find out where your weak spots are, or things that you've not thought about as an organisation. For example, you might be doing backups, but are you testing your restore procedures? It addresses those sorts of questions.'

We produced an action plan for each organisation and also a summary report and action plan for NHS Wales as a whole. 'We gave them a useful report with a lot of actionable points: it was a bit different from a management consultancy-style report which basically says, 'You're doing OK,' and there's nothing particularly actionable at the end of it.'

Massey says that NHS Wales subsequently invested in many of Stratia Cyber's recommendations.

Why healthcare is a target

'Wannacry had an economic motive. Ransomware works as a way of extorting money. You've got to consider your threat landscape. When it comes to healthcare, the main risk is people coming in and taking personal data. Because personal data records, particularly when they contain things like medical histories, are quite valuable.' Paul Massey, Director, Stratia Cyber

WHAT HEALTHCARE ORGANISATIONS CAN LEARN FROM WANNACRY

Cyber hygiene and the human factor must be prioritised, according to Paul Massey, Director, Stratia Cyber

1

Most attacks only require basic steps to stop

'Many attacks can be thwarted by basic cyber hygiene. About 80% of the attacks that you see will be thwarted by a Cyber Essentials Plus level of protection. If you're an organisation with a relatively low cybersecurity budget, and you're not particularly worried about high end threats from sophisticated threat actors (like nation states) you should still spend this money on basic cyber hygiene.'

2

Cybersecurity is a people thing

'Look at the human elements of the system. If I want to break into a system, it's normally easier to send somebody a dodgy link and get them to click on that than it is to technically defeat a router or some piece of hardware that's guarding your system. There are various relatively inexpensive tools and technologies you can use to mitigate that.

3

How to secure management buy-in

According to Paul, the NISD (The Network Information Systems Directive) was particularly useful when crisis hit, 'because it had this particular focus on monitoring. We were able to tell the Board of Management that it's not sufficient simply to have a logging system. It's all very well to log all this data (and then nobody looks at it) - but you need a system that interrogates those logs and automatically tells you when bad stuff is happening.'

SWANSEA BAY UNIVERSITY HEALTH BOARD |
CYBER ESSENTIALS+

Upgrading security for Swansea University Health Board in a time of change

The Covid pandemic has seen a 'massive, massive accelerated transition' to the cloud within the NHS and the organisations it works with, says Gareth Ayres, Cyber Security Manager, Swansea University Health Board.

Gareth worked with us to achieve Cyber Essentials Plus accreditation for a department within the Health Board - and says that the pandemic has sparked a wave of technological change.

He commented, 'It was already planned to move towards Microsoft 365 - but that was massively accelerated because of the pandemic. We transitioned from kind of the old way of doing it to cloud with SharePoint with OneDrive. It allows for really powerful collaboration between NHS Trusts in Wales.'

Ayres explained that NHS Wales had an established relationship with Stratia Cyber thanks to their gap analysis work in the wake of Wannacry. 'We turned to Stratia Cyber when we needed one department to qualify for Cyber Essentials Plus in order to secure a contract with the Welsh Government.'

Achieving certification within one department meant that they could get a feel for Cyber Essentials Plus - with a view to applying it eventually across the whole Swansea Bay University Trust.

Gareth concluded, 'If we tried to do it across the whole organisation, you're looking at hundreds of servers, we're looking at 14,000 endpoints, plus all of the medical devices. Working with Stratia Cyber allowed us to scope it in a way that we can absorb the lessons learned, expand where these are applied, and then widen the scope. It's still the end goal - but we need to do it incrementally.'

HOW STRATIA CYBER HELPED DRIVE CHANGE

Gareth Ayres, Cyber Security Manager, Swansea University Health Board on taking things one step at a time

Hitting business goals

Cyber Essentials Plus helped inform the trust on wider business goals

The main driving force at the minute in the NHS in Wales is something called the NIS regulation (Network and Information Systems). We do a lot of work in that area across Wales. Cyber Essentials Plus has also been beneficial to inform the work we're doing with NIS compliance.

Hands on reassurance

Cyber Essentials Plus helped Swansea Bay test its defences

Thankfully we don't have that many cyber incidents. So it's always really reassuring to be able to test our controls that we have in place. We've recently moved our endpoint security from Kaspersky to Microsoft defender, given what's happening in Ukraine. Cyber Essentials Plus allows us to actually test that by running through the practical tests. It's a hands on assurance more than, you know, than a tick box theoretical assurance.

Taking the next steps

Building security at the right pace for the organisation

We've got funding from the South Wales police commissioner's office to do Cyber Essentials Plus for the cyber team, there's five of us in the cyber team. The cyber team is not particularly big, but the services and the devices that we use are different, compared to standard users. We've already engaged with Stratia Cyber and we're going to start doing that soon.

WHAT THE EXPERTS THINK

Experts from leading UK organisations on how the pandemic has changed the playing field for cybersecurity - and what needs to happen next

'Don't just talk to the board, listen to them'

Sarah Janes, CEO, Layer 8

'If you only have a few minutes to talk to the board, don't just go through the list of things you want to do. You can spend much better quality time if you spend that five or seven minutes trying to ask one or two really good questions where you can understand them, and build trusted relationships with people at board level. Then next time you can have a better conversation on how you can link security, strategy and needs with what they are doing.'*

'The pandemic shone a light on how cybersecurity works'

Simon Lacey. Principal Consultant, CRMG and former cyber lead at NHS and Bupa

'During the pandemic, the business imperative was just to deliver and worry about the rest afterwards. I think that gives us an opportunity to shine a light on business as security professionals. I think that's helped us to engage with senior leaders: it's a great opportunity to say we're going to deliver efficiently and securely and in multiple flexible ways, because things are never going to quite go back to the way they were.'*

'Get the basics right'

Paul Massey, Director Stratia Cyber

'The importance of cybersecurity is growing in health, as it is in most sectors. But basic cyber hygiene will significantly reduce your risk of exposure to many of these attacks. It boils down to the things it's always boiled down to which is reducing the vulnerabilities of your system - because there needs to be a way in.'

Source: **Healthcare, now and in the future: Protecting your digital transformation strategy**, SC Unlocks: Healthcare Cybersecurity Risk, 26 April 2022

SC INSIGHTS | HEALTHCARE REVISITED

CYBER SECURITY IN HEALTHCARE: CHALLENGES AND OPPORTUNITIES

Cybersecurity has become a patient safety issue, with threats such as ransomware delaying operations and putting patients at risk, according to Saira Ghafur, lead for digital health at the Institute of Global Health Innovation.

The Government's Active Cyber Defence took down 2.3 million malicious campaigns in 2021, including fake NHS apps.

If cybersecurity can really spell the difference between life and death, are you doing enough? Stratia Cyber can help.

Stratia Cyber's experts can help strengthen your security culture, understand where your data assets are and help you reduce your cyber risk.

Our analysts always talk in plain language, and will help you navigate the standards you need to keep your data (and your patients) safe.

If you'd like to contribute to a future edition of SC Insights, let us know here.

cyber@stratiacyber.com
www.stratiacyber.com