# The Cyber Challenge for the NHS

EQUANTIIS

# Contents

# Addressing the Cyber Security Challenge

# Introduction

A year on from the WannaCry cyber attack in 2017 that severely impacted the NHS there was still found to be a shortfall in the number of NHS staff having received cyber security training and, at the last audit, all NHS organisations tested had failed to achieve the expected standard for cyber security.

With the highly sensitive nature of the personal data being processed and the potential consequences of failure to preserve quality, protect against misuse and loss, the NHS needs to do more on cyber security and data privacy, but there are significant challenges to overcome. In this Whitepaper we set out the key challenges and how to start addressing them. We're not going to pretend it's easy or a quick operation, but our tips will help put your organisation on the road to recovery.

# 1. Conflicting Investment Priorities

NHS organisations, while comparable to big corporations in terms of number of staff and complexity, lack the funding available to large corporates to invest in managing the cyber problem. Recognised standards for cyber security are not always seen as good value for money, as compared to other investment priorities.

We advise caution because the NHS is a serious target for hackers; not only is much of the customer data processed highly personal, valuable and consequently protected as 'special category' data under the General Data Protection Regulations (GDPR) but also, the NHS is dependent on technology to function and bringing the NHS to a halt is a very public show of failure as demonstrated by the WannaCry cyber attack. Added to this, the challenge of unsupported legacy infrastructure makes the threat very real.

## 2. Multi-Player I.T. Service

The IT function within NHS organisations tends to incorporate a mix of internal resources, cloud solutions and third-party service providers, which introduces the inherent risk that comes with relying on any third-party processor, along with a risk of gaps in service provision or ownership caused by lack of clarity in delineation of roles and responsibilities.

There is frequently some devolved IT capability within different departments in a trust which typically presents a risk to oversight, with unknown data and technology assets, third party providers and divergent governance processes.

## 3. Silos

There is a tendency for departmental and site-based silos to exist across NHS organisations, an arrangement which typically presents a risk to oversight, with undiscovered data and technology assets, and processes divorced from and non-compliant with the rest of the organisation.

With varying degrees of cyber security awareness and training existing across different departments, alongside distinct technology, processes and security regimes, the risk of cyber threat is heightened.

# 4. Third-Party Complications

With many NHS services now outsourced, it is crucial that those third-party service providers are meeting the same required cyber security and data privacy standards. In most cases, due diligence is carried out on third-party service providers at the outset of an agreement but, as the Marriott hotel chain GDPR fine in 2019 clearly demonstrates, due diligence must be adequate, and this is particularly true where the data is as sensitive NHS data.

A frequent omission is the need to monitor third parties on an ongoing basis, rather than just at one snapshot in time. Businesses change, threats change and this needs to be taken into consideration as part of the cyber governance regime.

# 5. Legacy Infrastructure

An issue for many organisations is legacy infrastructure which does not support compliance with data privacy legislation and is poorly supported, leaving it exposed to security vulnerabilities. Different NHS trusts, sites and departments are frequently using different systems and processes to do the same thing, and, in many cases, they are simply outdated.

An example is the prevalence of the fax machine to share patient data and, even as recently as two years ago, there was evidence to suggest that 90% of NHS organisations were running outdated unsupported Windows software somewhere on their network, which is why the WannaCry cyber breach impacted the NHS so heavily.

The fine handed out by the ICO to British Airways in 2019 demonstrates the importance of keeping infrastructure up-to-date and protected from the latest security threats. Outdated infrastructure, or lack of funding is no valid excuse for non-compliance with the GDPR.

The NHS has been given additional investment over the years to "go digital", but the current siloed digital infrastructure and nature of the NHS as an institution makes this a long-term endeavour.

Digital transformation in the NHS has historically been tackled in small, fragmented projects, with cyber security low on the agenda.

# Addressing the Cyber Security Challenge

# 1. Putting Cyber on the Agenda

Given the NHS's reliance on digital technology and the sensitivity of data being processed, it is crucial to get cyber security on the agenda. Using recent real-world examples, particularly those which have resulted in large fines or significant disruption, is a great way to get senior stakeholders to understand that the cyber risk is real and proximate.

The GDPR mandates privacy-by-design, which means that data privacy and security need to be proactively considered before any change project goes ahead and this regulatory requirement is a great way to link Cyber investment to NHS digital transformation project costs.

A risk assessment is recommended to understand and prioritise the threat cyber security presents to NHS organisations and this will help to build the business case for investment.

# 2. Joined-up I.T.

A joined-up IT service does not mean it has to be provided by one company or by one group. However, to minimise the risk and impact of a security incident, it is critical that the same level of IT governance and security is applied across the organisation, including to any third parties. We recommend that there is one group regulating the IT provision for an NHS trust, which is responsible for defining and maintaining: direction; strategy; policy; governance process; the assets register; IT and cyber requirements; and the specific responsibilities of each party involved (internal and external).

**A technology audit is a great place to start to understand what infrastructure exists, where, what for and how it is currently being managed.**

Outsourcing IT service in an environment which is heavily dependent on technology for critical services such as patient care, necessitates that relationship function as a partnership, rather than a supplier-purchaser style relationship. Cyber security requirements and expectations need to be clearly defined, monitored and tested on a regular basis across all parties involved in providing the IT service to ensure it is fit for purpose and meets an adequate level of security and continuity.

# 3. Opening Up Silos

It is fair to say that the NHS is unique in its size, scale and complexity, but NHS organisations will need to break through the silos that exist within them to take a robust, consistent approach to cyber security and data privacy.

Change programmes need to be inclusive of representatives and resources from all divisions to have the greatest chance of success; involvement is key to buy-in, understanding and application of policy at a local level. There are benefits aside from improving the cyber security posture to working together, and this can be evidenced by Greater Manchester NHS organisations working together, pooling resources and expertise for common solutions, resulting in better outcomes and reduced cost.

Crucially for cyber security, there needs to be a clear understanding of assets (data and technology) across NHS trusts and a central data audit and processing inventory will support this and help in identifying what needs to change.

Employees and contractors across the NHS need to receive the same level of training in order to have the same level of awareness of cyber security. Training and awareness may need to be customised at lower level to support the application of policy in context, and the use of subject matter experts to represent each division can also support this.

# 4. Manage Third-Party Risk

A technology audit and GDPR mandated record of processing activity (or data audit) are great places to start in order to understand what third-party risk exists within an NHS organisation. A high-level risk assessment of third parties will allow a decision to be made as to how much due diligence is adequate in each case.

For some third parties, a checklist of questions may be considered adequate, while for others it may be necessary to see their security certification or, where the risk is higher, adequacy may be judged to be an independent audit of their processes and systems.

One thing is clear, adequacy needs to be determined through clear assessment of the risk and if there are lessons to be learned from the fines handed out by the ICO to date, they are that the core concept of 'privacy by design and default' mandates adequate and continuous adherence to the regulatory environment.

Consequently, regular monitoring of third-party processors needs to be implemented as part of the cyber governance regime to ensure that organisations stay on top of the risk they present.

# 5. Legacy Infrastructure

Legacy infrastructure isn't going to be replaced overnight within the NHS. However, there are immediate steps which can be taken to reduce the risk it presents.

**First,** get a clear picture of your technology landscape.

**Second,** replace anything no longer being supported as a priority.

**Third,** put in place short term policies and plans to minimise the risk associated with the rest, e.g. have a clear maintenance schedule, actively monitor cyber threats and updates and have a quick route for making necessary changes, have a clear plan for how to respond to GDPR subject access requests and a schedule for routine security testing.

One of the contributory factors in the recent Dixons Carphone fine from the ICO was the lack of routine security testing and this is demonstrative that taking your eye off the ball can result in a fine from the ICO. In the NHS, it could also result in highly sensitive data being stolen or time critical technology being unavailable.

# The Key Message

The key take-away is that there is a lot of work to be done in the NHS, including developing a real understanding of the possible impact a cyber breach could have on day-to-day critical operations and on personal data.  All of this will take time, but the current goal to "go digital" provides a great opportunity to embed cyber security into the culture, the technology, the processes and the people.

If any of this has struck a cord, please get in touch.  Equantiis has a wealth of experience around cyber security, data privacy and digital transformation.  A good first step we recommend is our Cyber Security and GDPR audit, which will help you to understand how effective your current regime is and what you can do to improve it.

## Author

Tanya Sewell

Associate Consultant

www.equantiis.com

hello@equantiis.com

+44 (0) 203 376 7447

EQUANTIIS