NHS Digital submission for the Public Accounts Committee 5 February 2018 – Cyber Security

31 January 2018 – Version 1.2

Information and technology
for better health and care

Contents

1. Introduction 3

2. Impact 5

3. Preparedness 7

1. Introduction

1.1 Purpose

The purpose of this submission is to provide the Public Accounts Committee with key information about the role and actions of NHS Digital prior to, during and after the Wannacry cyber-attack.

1.2 NHS Digital

NHS Digital (NHSD) was established in 2013 under the Health & Social Care Act 2012 and is an executive non-departmental public body. Its work with data and technology, supports better health and care in the NHS and develops services and systems that empower citizens to access the health information they need to support their health and care. NHS Digital provides the national information and technology infrastructure that allows frontline professionals to access the digital services to deliver patient care. It also works in partnership with other government and public service agencies to further joine-up service provision for patients and citizens.

NHS Digital does not have the ability to mandate action by local NHS organisations.

1.3 NHS Digital's Data Security Centre

The Data Security Centre performs the following key functions within NHS Digital and across health and care:

- assures the integrity and security of critical national systems that underpin health and care.
- informs and advises organisations of best practice, cyber vulnerabilities and how to address them.
- provides threat information to health and care to enable local organisations to take action.

In future, the Data Security Centre will assume a stronger, lead role to:

- identify and communicate cyber threats to the health and care system, issue targeted remediation advice and track through to completion.
- assess the system-wide risks posed by vulnerable organisations and take steps to mitigate through support and technological intervention.
- perform greater monitoring of local infrastructure where organisations require.

1.4 Overview of IT in the health and care system

The NHS is one of the five biggest employers in the world, employing approximately 1.5 million people, serving a population of around 60 million. Its digital infrastructure (the Spine) connects more than 28,000 healthcare IT systems in 21,000 organisations, handling 6 billion messages every year with 250,000 users accessing the service at any one time.

Each Trust and Clinical Commissioning Group (CCG) is a separate organisation that is responsible for its own budget and provision of its own IT services, including cyber-security. As a result, there are widely varying levels of scale and maturity to IT provision across health and care.

This creates a significant challenge to the provision of national IT services and networks, as they will only be as secure as the organisations that access them. No central body currently mandates organisational IT policy or investment, therefore, assuring the integrity of the system is an ever-increasing challenge.

2. Impact

2.1 Wannacry and its origins

Wannacry or Wannacrypt, is a form of ransomware which demands payment in return for access to a computer and its associated files which it encrypts and locks out users from their files. Ransomware is not a new threat and can be traced back as far as 1989.

In 2016, it is understood a group of malicious actors weaponised a set of stolen malware to exploit flaws in the Windows operating system (OS); this allowed the actors to remotely gain access to computers and encrypt files. The tools to launch this attack were leaked online exposing the OS flaws to the wider threat community. Microsoft released an initial software patch to rectify the vulnerability in March 2017.

2.2 A Global Attack

In addition to the NHS, Wannacry affected computers in 150 countries. Large organisations such as FedEx, Renault-Nissan and Telefonica were affected and were required to halt elements of their operations.

2.3 What could have been done to prevent it?

On 14 March 2017, Microsoft released a software update that rectified the vulnerability that would be later exploited by Wannacry in the attack on 12th May 2017. Users were required to apply the update, or ‘patch,’ which would provide protection from that point forward. The patch was provided free of charge to all Microsoft users, including the NHS.

‘Patch’ is another term for software updates that are released by suppliers when they discover flaws. These include security vulnerabilities.

Updating one computer in isolation is not an onerous process, however, where multiple computers are connected via a network, the process of updating software can be much more complex. Networks running critical systems need to be patched carefully to avoid any break in service in the event of a crash. In complex environments such as health, this can be a difficult and diligent task to ensure key critical clinical systems are not affected.

Impact of Wannacry on the Health and Care System[1]

The attack impacted one third of hospital trusts in England[2]. NHS England data shows that at least[3] 80 out of 236 trusts were affected – with 34 infected and locked out of devices (of which 27 were acute trusts), and 46 not infected but reporting disruption.

A further 603 primary care and other NHS organisations[4] were infected by Wannacry, including 8% of GP practices. During the incident, devices in an additional 21 NHS organisations made calls to the Wannacry ‘kill switch’. Whilst this may indicate the presence of infected devices within those organisations, it may also have been the result of routine cyber security maintenance activities.

[1] Data from NHSE, NHSI, NHSD and the NAO Report

[2] National Audit Office Investigation: Wannacry cyber-attack and the NHS (October 2017)

[3] Numbers are based on organisations self-reporting problems to national bodies and NHS England / NHS Digital analysis of internet activity and may be higher if some organisations did not report problems experienced in a timely or accurate way: National Audit Office Investigation: Wannacry cyber-attack and the NHS.

[4] “Other organisations” include CCGs, Commissioning Support Units, an NHS 111 provider, and non-NHS bodies that provide NHS care such as a hospice, social enterprise and community interest companies.

The NHS enacted its “mutual aid” processes in some parts of the country meaning that where one A&E could no longer take patients, nearby A&Es stepped up to take their demand. 1.2 % (6,912) first appointments were cancelled and re-arranged between 12 and 18 May. NHS England’s EPRR review identified at least 139 patients who had an urgent appointment for potential cancer cancelled between 12 and 18 May, representing approximately 0.4% of urgent cancer referrals.

Within social care, based on a 100% return from local authorities to COBR in the aftermath of Wannacry, no local authorities reported having been infected. However, a number of local authorities switched off their link to the NHS N3 network as a precaution against infection and, in some cases, quarantined emails being sent from nhs.net. This meant that business continuity arrangements needed to be implemented.

2.5 Was any data stolen or compromised?

Ransomware works by encrypting files at the source (within the affected computer), locking a user out until they pay the specified ransom. No NHS organisations paid the ransom. NHS Digital’s Data Security Centre worked with the National Cyber Security Centre (NCSC) to confirm that there was no exfiltration of data as a result of the attack.

3. Preparedness

The threat of cyber-attack is constant and like any other form of crime, the threat cannot be completely removed. In order to better protect the system, the risk of attack needs to be mitigated at both a local and national level.

This section describes some of the mitigations in place at the time of the attack and the improvements that have been made since.

3.1 What was in place before Wannacry to support health and care?

Prior to 2014, there was no central cyber security support function or centrally coordinated threat intelligence service for health and care organisations.

In 2014 NHS Digital, then known as the Health and Social Care Information Centre (HSCIC) developed their first cyber security strategy under the governance of the Information and Cyber Security Committee, a sub-committee of the NHS Digital Board.

It was proposed that four initiatives be delivered to support NHS Digital and the wider health and care system:

- an alerting and threat notification service – later known as CareCERT
- an internal monitoring service for national applications and services delivered by NHS Digital to give greater protection to information assets
- a service to provide a trusted source of guidance, learning and training for data security, and;
- a service to support large scale data security incident management in respect to technical support.

In 2015 the National Cyber Security Programme (NCSP) of the Cabinet Office funded NHS Digital for one year to set up these initiatives in a proof of concept phase to identify their necessity and operational viability. These services became collectively known as CareCERT.

In 2016 the National Information Board, through its Paperless Health and Care 2020 programme, funded the continuation of the CareCERT suite of services which NHS Digital optimised and enhanced to include additional capabilities:

- **Monitoring of the National NHS Network (N3)** – This monitoring could not only block traffic, but CareCERT could also alert an NHS organisation that a potential infection had been seen coming from their infrastructure along with remediation advice to enable the local organisation to check for infection and then remove it locally.
- **Data Security Helpline** – an in-hours service which health and care organisations can call for advice on data security, potential threats, or further information on the advisories CareCERT sends help. This service also there to support organisations in the event of a data security incident. The helpline is available out of hours with security specialist on call for serious issues.

NHS Trusts in the main have locally procured internet gateways and these currently cannot be monitored via CareCERT. Future plans need to have a much greater focus on local monitoring so CareCERT can further enhance existing security and to ensure threats can be shared across organisations and not just dealt with locally.

3.2 What warnings were given by CareCERT prior to the attack?

The Health and care system was alerted on March 17 2017 to the Windows vulnerability that Wannacry would exploit through a CareCERT Advisory. The advisory provided information on the Microsoft patch, but the information was included as part of a weekly summary and local organisations may not have recognised the importance of the information. It should be noted that the warning was not about Wannacry, as the ransomware had not been active at this point, but about the vulnerability Microsoft had identified in its operating system.

In April, it was discovered that the vulnerability could be exploited by malicious perpetrators, while Wannacry as a specific piece of malware was not yet known, what was known was that there was a way to use this vulnerability for malicious purposes. As such, on the 28 April, again in its weekly bulletin, CareCERT issued an advisory stating this, the potential impact and what action organisations needed to take. It was also published on the CareCERT Information sharing Portal, available to anyone with access to the National NHS Network, on the 25 April as a standalone advisory.

As NHS organisations are not mandated to provide their local technology architecture, it is currently impossible for CareCERT to target specific threat advisories to individual organisations when specific vulnerabilities are found in specific hardware or software. Instead, advisories are sent to all organisations, who then have to consider if they are affected.

3.3 How have CareCERT alerts been improved since?

CareCERT alerts are now prioritised as High, Medium or Low to highlight the immediacy of action required. Organisations have to acknowledge receipt of high-severity alerts within 48hours and confirm they have a plan in place to remediate if they are susceptible to the issue. In addition, the following new capabilities and processes have been delivered;

- **CareCERT Collect**

CareCERT Collect was developed in the immediate aftermath of the Wannacry to provide organisations with a portal to input reliable contacts for future alerts and mitigate the risk of poor communications. In addition to contact details, the portal fulfils the following functions;

- Acts as a database for organisations’ IP addresses. These addresses are then tested for vulnerabilities by CareCERT and the results are sent to the organisation identifying any relevant vulnerabilities.
- Acts as the point of contact for organisations to acknowledge receipt of high-severity advisories from CareCERT within 48 hours, allowing remediation to be tracked centrally.
- Allows organisations to download patches available under the Microsoft CSA (described below) to ensure patching is up to date.

The portal has been utilised by over 240 organisations. NHS Digital liaised with both NHS England and NHS Improvement (NHSE / NHSI) to encourage user uptake, achieving 100% sign up of all NHS Trust and Commissioning Support Units (CSUs) by 31 December 2017.

- **SMS Alerting**

A key issue in the Wannacry attack was communication as some organisations opted to disconnect their e-mail services in an attempt to mitigate the threat. Future cyber-attacks may include the disruption of e-mail communication therefore, NHS Digital delivered the **CareCERT SMS** text message alerting system (using the existing gov.uk Notify system to reduce costs) to improve communications between key personnel in the event of a major incident. The system uses the detailed contact information that is gathered via CareCERT Collect.

To ensure NHS organisations understand the priority and potential impact of High Priority advisories, a CareCERT SMS is also sent to stakeholders to ensure they are aware of the issue.

Other SMS solutions have been developed by local organisations and partnerships, however, the CareCERT SMS system is the only one linked to the live CareCERT data feed. Local solutions may help spread the message further and will not be discouraged, provided that they do not contradict the core, operational messaging that will only be promulgated via CareCERT and eventually, the future NHS Digital Security Operations Centre (SOC).

- **Residual risk**

NHS Digital does not have a detailed view of local infrastructure. As a result, alerts require distribution system-wide, rather than being produced on a more targeted basis, with the exception of alerts produced by the new Microsoft Enterprise Threat Detection (ETD) service.

3.4 What was the reliance on Windows XP at the time?

At the time of the Wannacry attack, 4.7% of the NHS estate was running on Windows XP. Windows XP was not a causal factor of the vulnerability that was exploited by Wannacry. The majority of infected systems were running Windows 7, with the key issues being application of the necessary patch and firewall settings.

The percentage of organisations using Windows XP has reduced from 4.7% to 1.8% between Wannacry and now, but it cannot easily be phased out of some key systems. Medical devices such as MRI Scanners have embedded XP that cannot be updated without supplier intervention and a full medical re-certification of the machine. As a result, this residual risk has been mitigated by advising that these devices are segregated from an organisation’s wider network.

3.5 How were organisations supported to assess their vulnerabilities?

NHS Digital has been supporting organisations since 2016, through the provision of Data Security and cyber security on-site assessments (on-site assessments).

Prior to the Wannacry attack

On site assessments aim to support organisations towards attaining the National Cyber Security Centre’s Cyber Essentials[5] standard, providing them with;

- A report with accompanying action plan, helping them to understand their strengths and weaknesses and identifies key areas for investment to provide best value for money.
- 3 days’ centrally funded consultancy to remediate key issues.

The data security assessments are designed to give an organisation a situation report on their strengths and areas for improvement. This helps identify critical areas for investment that organisations can focus mitigating, ensuring their highest risk vulnerabilities are removed. This ensures that any available funding is maximised on high risk areas, while the organisation creates a further medium-term plan, for lower risk areas the assessment identifies.

[5] https://www.cyberessentials.ncsc.gov.uk/advice/

Since Wannacry

The structure and content of on-site assessments has not changed, however, the attack led to a re-prioritisation of organisations receiving the assessments. The re-prioritisation ensured that all Major Trauma Centres (MTCs), Ambulance Trusts and Commissioning Support Units (those organisations who support primary care including GPs) were prioritised for an assessment, with those experiencing a Wannacry infection being given even greater priority.

Organisations undertaking an assessment in this cohort were able to bid for capital funding, to support weaknesses identified from the assessments, from a £21m fund. NHS Digital, as part of this bidding process, assured local bids against the relevant on-site assessment action plan to ensure the efficacy and the value of the investment.

NHS Digital receives a monthly return on the results of the assessments. The intelligence from these assessments has helped NHS Digital create an evidence-based list of critical and systemic data security risks to the health and care system.

3.6 Software support

In the aftermath of Wannacry, NHS Digital signed the **Custom[6] Support Agreement (CSA)** with Microsoft to protect health and care organisations for a limited period to allow them to modernise their systems. The agreement was one of 7 signed across government in June 2017 and provides critical security patches and support for the following Operating Systems (OS) to facilitate safe migration;

- Windows XP (Support until November 2017).[7]
- Windows Server 2003 (Support until July 2018).
- Windows Sequel Server 2005 (Support until April 2018).

These updates are downloaded through the CareCERT Collect portal, allowing them to be tracked by NHS Digital. However, whilst it can track downloads, NHS Digital currently does not have the ability to track whether the downloaded patches have actually been applied within an organisation.

In addition to software patches, Microsoft provided a re-investment to health and care comprising of;

- An Enterprise Threat Detection (ETD) service which provides CareCERT with an additional feed to monitor for threats which covers all devices in health and care in England, once roll out is complete. The service provides alerts and reporting tailored by organisation down to individual machine level, together with expert remediation advice. Over 180 alerts have been issued and remediated since the service went live.
- 2000 Hours of Microsoft Premier reactive support that can be made available to the health and care system in the event of a major incident.
- Consultancy to embed services, improve cyber-security practice and provide Windows 10 Migration Support.

[6] 'Custom' as the support has to be custom developed. Support is no longer available on a commodity basis.

[7] This support was the most time-bound due to cost, but also due to the fact that Trusts had been warned to remove the operating system since 2015.

The value of the CSA contract was not released due to commercial sensitivities. The nature of the agreement allows it to be used to support a wide range of migration and modernisation activity.

Further improvements delivered since Wannacry

In addition to mitigations above, NHS Digital has delivered the following improvements to improve preparedness across the system;

Security Information and Event Monitoring (SIEM) brought in house

The SIEM is the central database of all information received by the Data Security Centre. It provides a central hub for all information feeds and allows data to be analysed through automation, cross correlating threat feeds to identify areas for consideration by in-house security specialists. These result in alerts and notifications to health and care organisations to enable them to take appropriate action. After Wannacry it was decided that the function should be brought in house delivering the following benefits:

- greater control over the analysis and processing of data by specialist staff.
- ability to connect multiple new information feeds from any source.
- greater resilience over the previous system, which had no back-up.
- 400% extra capacity to consume information, allowing new information feeds to be connected quickly.
- addressed a number of vulnerabilities that existed with the old system.
- provides a low-cost transition environment to migrate to the new Security Operations Centre

The contract for the legacy SIEM allowed it to be ceased early without bearing additional legal costs. The SIEM was delivered in house in December 2017.

- **Data Security Awareness e-learning**

The Data Security Awareness e-learning package addresses National Data Guardian Standard 3: ***All staff to complete annual data security training***. The training covers the following four key areas;

- Introduction to security awareness
- Information and the law
- Data security - protecting information
- Breaches and incidents

The package was launched in August 2017. Since that date, 88,805 staff across the system have completed the training pilot activity with a satisfaction rating of 89%.