Department of Health & Social Care

Securing cyber resilience in health and care:

A progress update

February 2018

DH ID box
Title: Securing cyber resilience in health and care: A progress update
Author: DDP/Cyber Security and Innovation/13920
Document Purpose: Policy
Publication date: January/2018
Target audience: Parliament, Public, NHS providers, GP practices, Clinical Commissioning Groups, Commissioning Support Units
Contact details: Digital, Data and Primary Care, Department of Health, Quarry House, Leeds / 39 Victoria Street, London

Published to gov.uk, in PDF format only.

website www.gov.uk/dh

Introduction

The scale of the challenge

Cyber-attacks are an increasing global threat. There are regular reports of attacks impacting on different sectors and different countries around the world. The NHS has faced a number of cyber-attacks. The May 2017 WannaCry cyber-attack was unprecedented and the largest ever ransomware cyber-attack. And while it was not the target, WannaCry affected the NHS. With the next large-scale attack more of a question of "when" not "if", there remains a need for the health and care system to remain resilient against attack, to protect patient data and patient care.

Since 2010 the Department of Health and Social Care ('the Department'), working with its Arms-Length Bodies (ALBs), has led a significant programme to strengthen cyber resilience across health and care. In that time the Department has:

- Supported NHS organisations to move off unsupported software systems;
- Set up CareCERT[1], a pioneering sector-specific national cyber support service;
- Commissioned reviews by Dame Fiona Caldicott as National Data Guardian and the Care Quality Commission to reinforce cyber resilience across health and care, which recommended 10 Data Security Standards for health and care organisations;
- Included these 10 Data Security Standards in the NHS Standard Contract;
- Revised the Care Quality Commission "Well Led" inspection programme to include an assessment of cyber resilience; and
- Commissioned a review by the Chief Information Officer for Health and Care on the lessons to learn from WannaCry.

It was a result of the Department's programme of work and investment that most health and care organisations were unaffected by WannaCry last May. However, despite this programme of activity, WannaCry still affected at least 80[2] out of 236 NHS trusts. A further 603 primary care and other organisations were infected, including 595 out of 7,454 GP Practices. The NHS responded well to this attack, with no reports of harm to patients or patient data being lost.

Government response

There has been a long-standing Government-wide prioritisation of cyber security resilience, with the establishment of the National Cyber Security Centre to support this. The Department, together with its ALBs, has worked closely with the National Cyber Security Centre, the Cabinet Office and the National Crime Agency to ensure that the health sector plays its part in bringing cyber attackers to justice.

Immediately after WannaCry, the Department took a number of further actions to ensure health and care organisations had strong cyber security measures established to be best placed to mitigate against cyber-attacks. In July 2017, the Department published Your Data: Better Security, Better Choice, Better Care in which it formally accepted the National Data Guardian's

[1] CareCERT: Care Computer Emergency Response Team.

10 Data Security Standards. As part of this, an implementation plan on securing data and cyber security was published which set out how we plan to deliver key data and cyber security actions. This included commissioning a review of WannaCry from the Chief Information Officer for the health and social care system in England to analyse the lessons learned, assess the actions required to reduce the risk and impact of a future cyber-attack and to make clear recommendations as to how this learning can be shared and implemented across the whole health and social care system. All actions set out in that plan have either been delivered or are in progress. This document summarises these actions.

Making sure the NHS is as prepared as possible for cyber-attacks

Incident response

The Department reviewed its Data Security Incident Response Plan and NHS England led work to develop a system-wide Data and Cyber Security Operations Playbook. These set out clearly the roles and responsibilities of organisations and individuals during an incident. In December 2017, the Department tested these plans, alongside the key organisations, via a simulated table top cyber-attack exercise. Exercises such as this are an important part of the preparedness process, but in order to be most effective, lessons identified need to be reflected on, implemented, and then tested again. The Department and its ALBs held a de-brief after the exercise to capture the lessons identified, and are now taking these forward as the response plans go through their next iteration.

Helping NHS organisations to address infrastructure weaknesses

Patching

Patching (also referred to as patch management) is a security practice designed to pro-actively prevent the exploitation of IT vulnerabilities that exist within an organisation. Before WannaCry, NHS Digital had issued CareCERT alerts to health and care organisations on how to respond effectively and safely to cyber security threat. However, WannaCry highlighted inadequate patching systems by infected NHS organisations despite patching advice from NHS Digital.

Since WannaCry, NHS Digital has implemented CareCERT Collect, a system through which all NHS Trusts and Commissioning Support Units (CSUs), on behalf of CCGs, have to report within 48 hours on action they have taken on High Severity CareCERT alerts (i.e. implementing security patches and updating their anti-virus software). 100% of NHS trusts and CSUs were signed up by January 2018.

Funding

Following WannaCry, the Digital Delivery Board (the governing board for the Personalised Health and Care 2020 programme which oversees better use of data and technology) reprioritised £21m capital for our major trauma centre hospitals and ambulance trusts. This funding is being used to upgrade firewalls and network infrastructure, and support the transition from outdated hardware and operating systems to improve resilience. These organisations were asked to undergo independent on-site assessments before applying for some of this funding which they could use to tackle high priority critical infrastructure vulnerabilities identified in their assessments. Trusts have now been allocated their share of the £21m. This funding is helping to build resilience by:

- Upgrading firewalls to secure networks;
- Minimising risk to medical devices i.e. MRI scanners and blood test analysis devices;
- Supporting use of software to fix security vulnerabilities or upgrades for software applications and technologies (also referred to as "patching") by replacing obsolete PCs and introducing device security tools; and
- Improving anti-virus protection.

A further £25m of capital funding has been identified in 2017/18 to support organisations that have self-assessed as being non-compliant against high severity CareCERT alerts, strengthening hardware and software across the system.

A rigorous reprioritisation exercise is underway across the NHS IT portfolio to identify additional cyber investment between 2018/19 and 2020/21. As part of this, an initial £150m has been identified focused on continuing investment in local infrastructure as well as national systems and services to improve monitoring, resilience and response. Options for further reprioritisation and additional investment for cyber security are being looked at as future plans are refined. In addition to this national funding, local organisations will need to commit local capital and revenue funding to maintain and refresh their own IT estates, and to ensure that these are operating on supported versions of software.

Unsupported systems

The National Data Guardian and the Department have been clear that organisations should not be operating IT systems which are no longer developed or updated as these lack modern security controls and cannot cope with large volumes of data and multiple users. Around 4.7% of NHS devices were operating on Windows XP at the time of WannaCry. This is now 1.8% as at January 2018. In July 2017, NHS Digital published guidance to help local organisations to move off unsupported systems and to minimise the risk of unsupported systems where they are in use.

As we move closer towards the end of extended support for Windows 7 in 2020, there is the need for organisations to continue to review and replace their systems, including where appropriate taking advantage of the guides and services offered by NHS Digital and through the Microsoft Custom Support Agreement (see below).

NHS Digital agreed a Custom Support Agreement with Microsoft at the end of June 2017 which provided the following free services to NHS organisations:

- Patching and support for Windows devices operating with Windows XP, Windows Server 2003 and Sequel server 2005;
- Improved threat awareness through Microsoft’s Enterprise Threat Detection (ETD) service;
- Windows 10 migration support, including health and care specific guidance for organisations to help in the pre-deployment, migration and operation of Windows 10; and
- Microsoft consultancy to help embed services, improve cyber-security resilience and prepare organisations to move to Windows 10.

Security Toolkits

The Information Governance Toolkit has provided health and care organisations with an audit tool during 2017/18 to help them to assess their data security capability and capacity. Compliance is mandatory for all organisations using the NHS Contract in 2017/18.

The Department, working with its ALBs, has led work to re-design this Toolkit into a new, more user friendly 'Data Security and Protection Toolkit' (DSPT). This has received positive feedback via extensive testing with health and care organisations. It will be launched in private beta in February 2018 with roll out from April 2018. Trusts will benefit from an accessible dashboard enabling them to track their progress in meeting the 10 Data Security Standards.

As with existing arrangements for the IG Toolkit, non-NHS organisations (including local authorities) will need to complete the DSPT. This will apply for adult social care, public health and other services that are receiving services and data from NHS Digital and / or are involved in data sharing across health and care where they process confidential personal data. For those social care providers who provide care through the NHS Standard contract, this will be a mandatory requirement from April 2018. For other social care providers, whilst there is no mandation to complete the DSPT, it is recommended that it is completed as this will demonstrate compliance with the 10 Data Security Standards and in preparation for the General Data Protection Regulation (GDPR) from May 2018 (see page 7 for further information about the GDPR).

The Department, with NHS England and NHS Improvement, published the 17/18 Data Security and Protection Requirements (DSPR) in October 2017 to ensure organisations know what they need to do to comply with the 10 Data Security Standards until the DSPT is launched. This includes specific advice for NHS providers, General Practices, local authorities and social care providers.

Assurance

The 17/18 Data Security and Protection Requirements (DSPR) make clear that there must be a named senior executive responsible for data and cyber security in every health and care organisation. Ideally this person will also be the Senior Information Risk Owner (SIRO), and where applicable a member of the organisation's Board. This requirement will be in the Data Security and Protection Toolkit (DSPT) from April 2018 onwards.

NHS Improvement will be seeking assurance of compliance from NHS trusts with the DSPR in March 2018. NHS England will do the same for commissioners. From April 2018, that assurance will be available via the new toolkit.

The DSPR recognises that a proportionate response is needed for local authorities and social care providers given the context they work within, and that many social care providers will need time to enhance their level of digital maturity and develop systems and processes to achieve compliance. Local authorities already have quality assurance arrangements in place either through the Public Service Network, ISO or other quality standards. NHS Digital is working closely with the Cabinet Office to ensure these frameworks are aligned to help to reduce any additional requirements from local authorities.

NHS Digital is able to use information from its CareCERT Collect system to provide NHS Improvement, NHS England and the Care Quality Commission with the details of organisations who are non-compliant or where they are concerned about future compliance.

The NHS Standard Contract, mandated by NHS England for use by commissioners to fund all healthcare services other than primary care, has included a requirement to implement the 10 Data Security Standards since the latest two year contract was published in November 2016 (which came into effect April 2017).

Inspections

Since September 2017, data security has formed part of the Care Quality Commission's role in assessing whether NHS trusts have adequate leadership in data security. NHS GPs and adult social care providers followed from November 2017, with the Care Quality Commission's updated inspection framework to be further developed and rolled out by April 2018. In early 2018, the Care Quality Commission, working with NHS Digital, will test unannounced cyber security inspections in NHS trusts to decide whether to roll these out to target organisations which repeatedly fail to follow basic cyber security practice.

Forthcoming regulatory requirements

The General Data Protection Regulation (GDPR) and (for those organisations in scope) the Network and Information Systems Directive (NIS Directive) will come into force in May 2018. Together, these will strengthen the cyber security and data protection regulatory regime for health and care organisations. Whilst the NIS Directive will only apply to organisations in scope, the 10 Data Security Standards and wider regulatory framework will apply to all health and care organisations.

Ensuring we support staff and leaders to help them protect patients' data from cyber-attacks

All staff

A new e-learning package was developed and launched by NHS Digital in July 2017 to help all NHS staff to understand their role in in the safe and secure management of patient data. This package will be reviewed by Health Education England and revised later in 2018 in response to feedback.

Leaders

To support Executive / Board-level staff to ensure data security is embedded across organisations, the National Cyber Security Centre produced 10 Steps to Cyber Security in August 2016.

NHS Digital, Health Education England and NHS England are targeting Board-level leaders so that they actively ensure their organisation is competent in information governance practice through the Building a Digital Ready Workforce programme.

NHS England has commissioned the NHS Digital Academy to deliver a new learning programme "Postgraduate Diploma in Digital Health Leadership" to develop current and future health care digital leaders, drive professionalism and oversee transformational change.

IT and security staff

NHS Digital has been providing accredited training to IT and security professionals across health and care to build local capability in security best-practice, ensuring provider organisations have skilled operational staff to improve security control and preparedness.

Regional

NHS England and NHS Improvement are leading an engagement programme with providers and commissioners to ensure local areas are taking action to improve cyber security. This includes:

- NHS England regional cyber leads co-ordinating with local areas on cyber security;
- Working with Chief Clinical Information Officers and Chief Information Officers to establish a network of cyber leads and professional expectations for these; and
- Clarifying assurances expected at Board level, for example with Clinical Commissioning Groups Audit Chairs and Audit and Risk Committees.

Ensuring NHS organisations have the support they need to build their cyber resilience

NHS Digital has continued to provide health and care organisations with threat intelligence, information / advice and patches via CareCERT. NHS Digital has also:

- Carried out independent on-site data security assessments for NHS organisations to compare against the industry recognised “cyber essentials plus” standard and identify actions needed to improve cyber resilience. By January 2018, 190 organisations had completed assessments;
- Produced a series of good practice guides;
- Provided data security training to health and care staff to support them in recognising their personal responsibility in securing data;
- Worked with BT to scan NHS organisations to assess their vulnerabilities to cyber-attack;
- Implemented a text messaging alert service in November 2017 to ensure trusts have access to accurate information, even in the event that there is no access to the internet and email systems;
- Ensured contact and escalation lists are in place and up to date;
- Worked with the Crown Commercial Service to identify Cyber Security Services 2 (RM3764ii) (a list of National Cyber Security Centre certified cyber security services) for health and care organisations to use in ensuring their systems are safe and secure and that services are protected;
- NHS Digital has recently issued guidance to health and care organisations on how to safely and securely make use of cloud computing services, including data offshoring. These technologies offer benefits including increased data protection and resilience, and reduced running costs; and
- NHS Digital has secured an additional £4m to expand CareCERT services into an NHS Digital Security Operations Centre to improve monitoring of security threats, provide guidance and expert response to health and care organisations, and assure the public of the safety of their data. This will be operational from May 2018.

Next Steps

The Department will continue to work with its ALBs and across Government to learn from the lessons identified from the simulated cyber-attack. From this, we will refine the Department's Data Security Incident Response Plan and system-wide Data and Cyber Security Operations Playbook to make sure the NHS is as prepared as possible for future cyber-attacks.

We will support NHS organisations to take immediate action to address infrastructure weaknesses which leave them vulnerable to future cyber-attacks. We will seek assurances of compliance with the DSPR from NHS trusts and commissioners and the new DSPT thereafter, and decide whether to roll out unannounced cyber security inspections in NHS trusts.

Over the next few months, the Department is committed to further work with the social care sector to enhance our collective understanding of both cyber and data security across the care provider sector and consider the most effective future support.

We will review and revise the e-learning package, work with Board-level leaders to ensure their organisations are competent in Information Governance, and develop the Postgraduate Diploma in Digital Health Leadership to develop health and care digital leaders to support staff and leaders to help them protect patients and their data from cyber-attacks.

NHS Digital's Security Operations Centre will help ensure local NHS organisations have the support they need to build their own cyber resilience via help monitoring security threats, providing guidance and expert response to health and care organisations, and ultimately assure the public of the safety of their data.

1. Appendix A: Timeline of actions

Before 2015

- NHS offered free upgrade from Windows XP - May 2010
- Government funded additional year of support for public services to move from Windows XP - April 2014

Before 2016

- NDG & Care Quality Commission (CQC) reviews commissioned by Secretary of State - September 2015
- CareCERT established - October 2015
- Additional £4.2bn spend committed for technology. Over £50m available for CareCERT - November 2015

Before 2017

- NDG & CQC wrote to NHS Trusts outlining key data security steps to take to mitigate cyber risks - May 2016
- NDG & CQC published their reviews and recommendations for data and cyber security - July 2016
- National Cyber Security Centre published 10 Steps to Cyber Security for leaders - August 2016
- The Chancellor launched UK's new National Cyber Security Strategy. Nearly £2bn public funding provided for transformational investment over next 5 years - November 2016

Before 2018

- Her Majesty the Queen opened the National Cyber Security Centre - February 2017
- Requirement for adherence to the NDG recommendations came into effect in the NHS Standard Contract 2017/18 - April 2017
- NHS impacted by WannaCry - May 2017
- DHSC Data Security Incident Response Plan reviewed. System-wide Data and Cyber Security Operations Playbook developed - June 2017
- Customer Support Agreement with Microsoft - June 2017
- DHSC response to NDG Review published including cyber security plans - July 2017
- NHS Digital published unsupported systems guidance - July 2017
- e-learning package launched for NHS staff - July 2017

- Data security now part of CQC's assessments of well led NHS trusts. GPs and Adult Social Care Providers followed in November - September 2017
- 2017/18 Data Security and Protection Requirements published - October 2017
- Text messaging relay service launched - November 2017
- First health cyber-attack simulated table top exercise - December 2017
- 34 of our major trauma centres and ambulance trusts completed on-site assessments - December 2017

Before 2019

- 190 organisations completed on-site assessments - January 2018
- Additional £25m funding secured to support major trauma centres & ambulance trusts with their critical infrastructure - January 2018
- Initial £150m identified via reprioritisation across NHS IT portfolio to continue investment in local infrastructure & national systems and services to improve monitoring, resilience and response - January 2018
- 100% of NHS trusts and CSUs signed up to CareCERT Collect - January 2018
- New Cloud guidance published - January 2018

Planned actions

Before 2019

- New CQC unannounced cyber security inspections to be tested - February 2018
- All major trauma centres and ambulance trusts to have completed on-site assessments - February 2018
- New Data Security and Protection Toolkit rolled out - April 2018
- New NHS Digital Security Operations Centre operational - May 2018
- The General Data Protection Regulation and Network and Information Systems Directive come into force - May 2018