Department of Health & Social Care

Securing cyber resilience in health and care

Progress update October 2018

October 2018

DH ID box
Title: Securing cyber resilience in health and care: Progress update October 2018
Author: Cyber Security Policy
Document Purpose: Implementation Update
Publication date: October 2018
Target audience: Public
Contact details: Cyber Security Policy 39 Victoria Street London S1H 0EU CSI-Support@dh.gsi.gov.uk

Published to gov.uk, in PDF format only.

www.gov.uk/dh

Contents

Introduction

In February 2018 the Department published ‘Securing cyber resilience in health and care: A progress update’, which set out the actions taken by the Department and its Arm’s-Length Bodies to improve the cyber security of the health and care system both before and after the May 2017 WannaCry cyber attack, as well as our plans for the future. This document provides a further update on progress and development of our future plans.

In particular since February we have:

- increased our investment in securing local infrastructure in 2017/18 to over £60 million;
- signed a Windows 10 licensing agreement with Microsoft which will allow local NHS organisations to save money, reduce potential vulnerabilities and increase cyber resilience;
- agreed £150 million of investment over the next three years;
- procured a new Cyber Security Operations Centre boosting the national capability to prevent, detect and respond to cyber attacks;
- launched the Data Security and Protection Toolkit;
- agreed our plans to implement the recommendations of the Chief Information Officer for Health and Care’s review of the May 2017 WannaCry attack;
- Supported 25 local NHS organisations to improve their cyber resilience via the NHS Digital “Blue Teams” pilot, and;
- estimated the costs of the WannaCry attack.

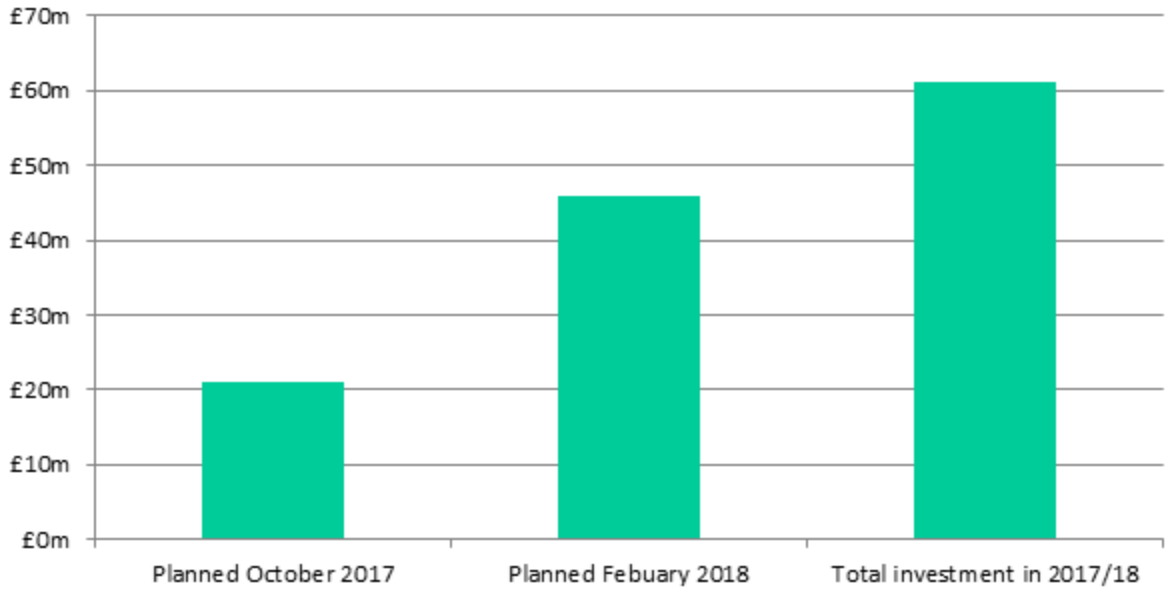
This work forms part of the Data and Cyber Security Programme being led by the Department with its Arm's-Length Bodies to improve the cyber security of the health and care system. The programme is underpinned by a robust governance framework including scrutiny from non-executive directors.

1. Local and National Investment

Investment in 2017/18

In October 2017 we outlined plans to invest £21 million to secure local IT infrastructure in 2017/18, and in February 2018 we set out our intention to invest an additional £25 million. From utilising underspends from elsewhere we were able to invest a further £15 million, bringing the total investment in boosting the security of local IT systems in 2017/18 to £61 million. Initial phases of investment were targeted at Major Trauma Centres and Ambulance Trusts, given their level of operational risk, with further phases supporting a broader set of provider organisations to address key vulnerabilities.

2017/18 Investment in Local IT Infrastructure



This investment has been targeted to address key vulnerabilities and has made a real difference to the cyber security of local NHS organisations, and to the protection of critical services for patients.

Case Study - Ambulance Trust

An NHS Trust which provides emergency 999, urgent care and patient transport services was awarded £260,000 through the capital funding programme.

Part of the funding was used to replace legacy firewalls and servers on a mobile data solution which is used to dispatch ambulances and provide navigation functions. This has made an immense difference to the Trust as the new firewalls provide better protection for the systems, without which all communications would need to be via voice, adding delay in delivering care to patients.

The Trust has enhanced their logging capacity by investing in more disc space. This has ensured that more detailed logs can be stored for longer time frames, which means that the Trust could recover its services more easily if a cyber attack occurred.

The funding has also been used to upgrade existing defence in-depth firewall technologies by adding next-generation anti-exploit, anti-ransomware, root cause analysis, and advanced system cleaning functionality. In addition the Trust invested in an Identity Services Engine which

provides better visibility of devices connected to the Trust's network, and can block unknown devices from connecting.

Case Study - University Hospital Trust

A large University Hospital Trust has used £1.5 million of capital investment to boost its cyber security know-how and capability. New technologies were introduced, including:

- a more cohesive anti-virus and patching mechanism;
- a Security Event Information Management system - which will give the Trust much stronger control over what happens within its network; and
- a new generation of smart high-performance firewalls to handle external data flows - which is increasingly important as more digital services are migrated to operate in the Cloud.

This work has coincided with the Trust's appointment of a dedicated Digital Risk Manager and further investment in the development of internal know-how. The Trust is also collaborating with other Trusts and organisations that are forming a wider response capability and defence against cyber-risks. This has taken the Trust's stance from reactive to a much more active and targeted capability that will safeguard its information and systems more effectively, enabling it to continue to deliver safe, high quality care to patients.

Investment from 2018/19 to 2020/21

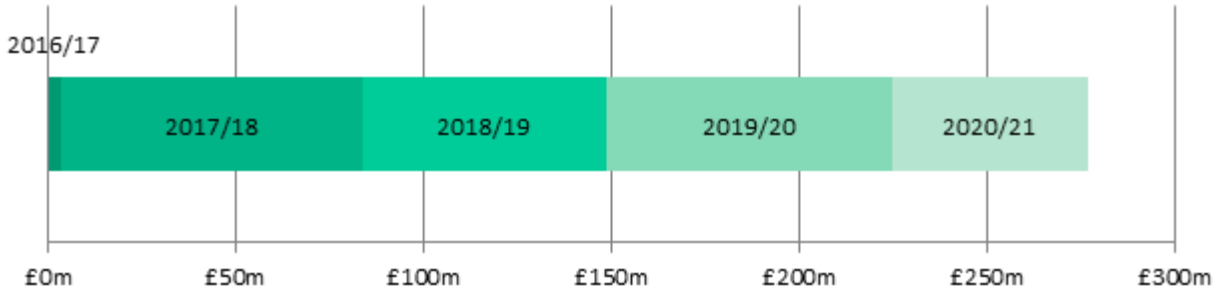
In addition to a multi-million pound licensing deal with Microsoft, over the next three years £150 million of funding will be used to support the health and care system, protecting key services from the impact of cyber attacks. This will be used to mitigate risks in the following areas:

- continued investment to improve the security of local infrastructure;
- nationally procured and locally deployed interventions to address common weaknesses across the NHS; and
- investment in NHS Digital's Cyber Security Operations Centre (CSOC) to enhance our national capability in preventing, detecting and responding to cyber attacks.

Detailed spending plans for the next three years have been developed through a Programme Business Case. Agreement has already been reached to release and spend funding to November 2018 to ensure work to make immediate improvements in cyber resilience can continue at pace. The Programme also receives funding through the Cabinet Office's National Cyber Security Programme which, to date, has supported work to test innovative approaches to building cyber resilience in health and care settings and work to better understand the current levels of cyber risk in the sector such as the on-site data security assessments and the social care discovery programme.

Local and National Investment

National Investment in Cyber Security in Health and Care through the data and cyber security programme



In total, over £250 million will be invested nationally to improve the cyber security of the health and care system by 2021. This excludes both investment by local organisations, and wider national IT investment which supports better security such as the Microsoft licensing agreement.

2. Improving Local Data and Cyber Security

Progress in 2017/18

In October 2017 the Department published ten priorities for 2017/18 for organisations in implementing the National Data Guardian's ten data security standards. In May 2018 NHS Improvement requested assurance from all NHS Trusts and Foundation Trusts on their progress in implementing these requirements. The results have shown that organisations have made good progress in implementing the data security standards related to people and process, but that those relating to technology continue to be challenging. The results on board level engagement are positive, with all Trust and Foundation Trusts (with one exception) having a board member with responsibility for cyber security. These results are being used to inform follow up with Trusts and Foundation Trusts to support them in increasing their security, and regulatory action will follow where sufficient progress is not made.

On-site Assessments

Overall, 265 independent on-site assessments have been carried out in total and 130 Trusts and Foundation Trusts were assessed in the Second Phase (comprehensive). The results of these assessments are helping local organisations understand what they need to do to improve their cyber security, and are being used to inform national support to improve cyber security across the system. These results informed the investment of £61 million in 2017/18 to address key vulnerabilities in local infrastructure, with further investment to follow over the next three years.

All 130 Trusts and Foundation Trusts who have undergone a comprehensive on-site assessment have been asked to provide their remediation plans to achieve Cyber Essentials Plus. All remaining Trusts and Foundation Trusts will undergo an NHS Digital Data Security on-site assessment by March 2019 and will be required to then submit their plans for achieving Cyber Essentials Plus.

Supporting Local Organisations

NHS Digital is trialling numerous intervention programmes to help organisations to accelerate progress towards achieving Cyber Essentials Plus. These programmes provide packages of support shaped by engagement with local organisations to understand their needs. NHS Digital is currently piloting the delivery of:

- GCHQ accredited board cyber security training;
- facilitating system hardening knowledge and trust level capability;
- triaging of risks and vulnerabilities to prioritise action; and
- reviewing and remediating identity and access management issues.

The training to boards is being delivered jointly by NHS Digital and NHS England to ensure that it is supplemented with specific tools to help boards understand and address the cyber security risk faced by their organisation. This approach combines meaningful technical improvements with equipping senior leaders with the knowledge and skills they need.

NHS Digital with NHS England has delivered 25 pilots to date. Feedback from pilot organisations has been overwhelmingly positive and following a successful pilot phase, these intervention programmes will be offered to all NHS Trusts and Foundation Trusts.

Social Care

The Department is working with the Care Provider Alliance and the Local Government Association to undertake a one-year discovery programme funded through the Cabinet Office's National Cyber Security Programme, to better understand the data and cyber security risks facing the adult social care provider sector, and what support is needed to address those risks in future. An external organisation has been commissioned to conduct on-site research and provide practical support to a range of adult social care providers. The providers selected will cover three local authority areas and reflect a broad range of service types, client groups, and levels of digital maturity. The discovery programme will help inform our future support offer to the adult social care sector.

3. Increasing National Support

As well as supporting local organisations to improve their own cyber security, the programme is investing in national services to increase security. This enables us to take advantage of economies of scale and ensure consistent quality services for all organisations.

Cyber Security Operations Centre

NHS Digital has entered into a three-year deal with IBM to deliver the new Cyber Security Operations Centre (CSOC), which will increase the capability to monitor, detect and respond to a variety of security risks and threats across the NHS, and offer expert advice and guidance. The CSOC will provide a range of new services to health and care organisations, enhancing data and cyber security response and defending against evolving threats. The CSOC expands on the existing cyber security services provided by NHS Digital and will include:

- incident response support for NHS organisations, ranging from remote advice to rapid on-site deployment of a specialist team of cyber experts in the case of a cyber security incident;
- support from IBM to deliver new services such as vulnerability scanning, malware analysis and digital forensics in individual NHS organisations, meaning that NHS Digital can offer tailored and specialist advice;
- an enhanced monitoring service which analyses data from multiple sources to detect and respond to threats across NHS Digital's national systems and services;
- threat intelligence to provide insight, guidance and advice, enabling health and care organisations to take appropriate action to prepare for, or mitigate against, identified risks and threats;
- piloting of local monitoring solutions with selected NHS organisations to test a range of security technologies and identify appropriate solutions that can be rolled-out across the system; and
- an Innovation Fund which will allow NHS Digital to quickly access new tools, technologies and expertise in response to new threats and the changing needs of the sector.

Secure and up-to-date systems

Following the Custom Support Agreement signed with Microsoft in June 2017, a new multimillion pound package was agreed with Microsoft in April 2018. This national agreement allows local NHS organisations to save money, reduce potential vulnerabilities and increase cyber resilience. The agreement includes Windows 10 licences to ensure the NHS is using the most secure and up-to-date software, as well as Advanced Threat Protection which gives the NHS advanced real-time monitoring and remediation capabilities. Advanced Threat Protection has already been deployed to more than 130 local organisations.

Case Study - Mental Health Trust

A large mental health NHS Trust is very impressed with Advanced Threat Protection and is already experiencing the benefits this provides. A member of staff opened a phishing email containing a malicious excel spreadsheet attachment. Advanced Threat Protection highlighted

the opening of the attachment within minutes. Technical staff were able to check the email server and identify another 20 staff that had received the same email and blocked it.

Advanced Threat Protection also identified that a member of staff had downloaded malware from a website. This was a new threat and was not originally picked up by anti-virus software, however Advanced Threat Protection identified the potential threat retrospectively and generated an alert.

Common solutions for common issues

To address common vulnerabilities and issues identified through the on-site assessments and Trusts' Cyber Essential Plus plans, NHS Digital will procure a suite of security solutions at a national level which can be deployed locally. While being flexible to changing needs, it is planned that the solutions will include:

- further deployment of Blue Team activity to priority organisations;
- providing organisations with dedicated follow-on support following Blue Teaming, to improve local policy and configuration and supporting operational readiness;
- central solutions to improve local secure configurations and asset and threat identification;
- deployment of cloud based security services, incorporating local web proxies and next-generation firewalls;
- support for organisations to make best use of the National Cyber Security Centre's (NCSC) freely available services, such as Webcheck and the Public Sector Domain Name System (DNS); and
- continued access to specialist online and industry-leading training packages to build local expertise and capability.

These solutions will be available to local NHS organisations for free. National procurement will allow for greater leverage while addressing common vulnerabilities at scale across the NHS.

Through combining the recent £60 million capital investment in infrastructure weaknesses and future capital investment as part of the £150 million, the Blue Team programme delivering local support, the CSOC, and nationally procured security solutions, it will be possible to deliver a step change in the level of data and cyber security across the NHS that would not be possible from taking one of these actions on its own.

4. Updating the regulatory framework

In April 2018 the Data Security and Protection Toolkit ("the toolkit") was launched to replace the previous Information Governance Toolkit. The toolkit allows organisations to track their progress in implementing the National Data Guardian's ten data security standards and acts as a national assurance framework for data security and protection in health and care. Organisations should complete their initial toolkit submission by March 2019, with an interim submission for larger organisations in October 2018. The new toolkit has been developed with extensive input from a broad range of users to ensure it is appropriate for all organisations using it. In particular, the new toolkit has been developed to be more suitable for adult social care providers to encourage greater uptake within that sector.

The toolkit incorporates key legal requirements for complying with the General Data Protection Regulation (GDPR) and, where relevant, the Network and Information Systems (NIS) Regulations, which came into force in May 2018.

The NIS Regulations give the Department greater powers to take action where Trusts and Foundation Trusts (as well as independent providers of NHS services who are individually notified) do not take sufficient action to secure their networks and systems. As the competent authority for the health sector in England, the Department has published a guide to the NIS Regulations. While the regulations do not apply to all health and care organisations, all are held to the same high standard that reflects the sensitivity of data and criticality of systems in health and care. All health and care organisations must comply with the National Data Guardian's ten data security standards and the GDPR.

Since September 2017, data security has formed part of the Care Quality Commission's (CQC's) role in assessing whether NHS Trusts and Foundation Trusts are 'well led'. NHS GPs and adult social care providers were included from November 2017. In the first half of 2018 the CQC has been working with NHS Digital to understand how the two organisations can work together more effectively and test the use of unannounced cyber security inspections in NHS Trusts and Foundation Trusts.

5. Implementing the CIO Review

As set out in 'Your Data: Better Security, Better Choice, Better Care' the Department and its national partners took several immediate actions in response to the WannaCry Attack. At the same time the Chief Information Officer for Health and Care was commissioned to conduct a lessons-learned review. The recommendations of that review build on the immediate actions taken in the wake of the WannaCry attack.

The Department and its national partners have agreed the approach to implementing the recommendations of the Chief Information Officer's review as part of the wider cyber security programme. **The agreed CIO Review Implementation plan is set out in Annex A**.

6. Counting the Cost of WannaCry

The WannaCry attack disrupted services across one-third of hospital trusts and around 8% of GP practices. This had a knock-on impact on patients with over 19,000 appointments cancelled. While this may only be a small proportion of overall NHS activity, it represents disruption to the care of a significant number of patients.

No data was systematically collected on the costs of recovering IT systems or the extent to which patient care was disrupted. Accurately assessing the costs would require collecting data from all organisations which itself would impose a disproportionate financial burden on the system. At the time, the focus nationally was on responding to the incident and remediation rather than collecting data, which would make an accurate retrospective data collection challenging.

It is not possible to estimate with certainty the financial impact of the WannaCry attack. The following estimate considers the financial costs in relation to two broad categories covering two time periods: during the attack between 12 and 18 May 2017, and the recovery period in the immediate aftermath to June-July 2017. The two categories of cost are:

1. Direct impact - lost output of patient care caused by reduced access to information and systems required for care leading to cancelled appointments etc.

2, Additional IT support provided by NHS organisations or IT consultants to restore data and systems affected by the attack.

It is anticipated that 1% of care was disrupted over a one week period, based upon an estimate of the average level of care provided by the NHS in a one week period. It is estimated that there was approximately £19m of lost output. However demand for NHS services fluctuates, therefore this should only be considered an approximate estimate.

Assuming each of the 80 severely affected Trusts would have required the equivalent of 5 days FTE additional resource of an IT specialist, the cost of IT support at the time of the attack would have been £0.5m. After the attack we have estimated an average level of resource required by organisations based upon their size and the severity of disruption. There were a few anecdotal reports of costs by individual organisations, but not enough data to make a robust estimate. Therefore the figures quoted below should be considered an approximate estimate.

These costs, using the mid-range estimates for lost output, are shown below.

Financial Cost

The estimated financial costs consider the direct costs to the NHS of lost output and IT support.

	During attack (£m)	Aftermath (£m)	Total (£m)
1. Lost output	19	0	19
2. IT cost	0.5	72	73
Total	**20**	**72**	**92**

Annex A - CIO Recommendations Implementation Plan

Recommendation 1

All NHS organisations are to develop local action plans to achieve compliance with the Cyber Essentials Plus standard by June 2021, as recommended by the NCSC. These plans will be provided to NHS Digital on behalf of the Chief Information Officer for health and social care by 30 June 2018. NHS Digital should produce a framework to support organisations, drawing on security assessments undertaken to date.

Approach to Implementation

All Trusts and Foundation Trusts will be required to develop plans to meet the Cyber Essentials Plus Standard. Plans have been requested from all Trusts and Foundation Trusts who have undergone a full on-site assessment. All Trusts and Foundation Trusts will be required to provide a plan once they have undergone an on-site assessment. NHS Digital will also work with ten accelerator sites to support them in achieving the Cyber Essentials Plus Standard more quickly. The sites selected will have varying levels of cyber readiness and lessons learned from the accelerators will be used to inform how the wider sector can be supported to achieve Cyber Essentials Plus.

We recognise that CE plus was not designed specifically for NHS Institutions. The new system wide Chief Information and Security Officer (CISO), appointed by NHS Digital in response to CIO Review Recommendation 9, will work with the NCSC and the system to review where the NHS is currently in relation to CE+ compliance. Medium to long term ambitions for the sector in relation to cyber standards will be identified.

Timeline for Implementation

Plans from Trusts and Foundation Trusts who have already undergone an assessment will be analysed by October 2018. All Trusts and Foundation Trusts will have undergone on-site assessments against the Cyber Essentials Plus Standard by December 2018 and will be required to provide a plan for analysis shortly after receiving the report following their assessment. The ten accelerator sites will aim to achieve Cyber Essentials Plus by March 2019.

The CISO and NCSC review will complete early 2019.

Recommendation 2

In the first quarter of 2018/2019 financial year, the Chief Information Officer for health and social care will convene an expert panel to define and consult on a set of IT infrastructure, application and service management guidelines for organisations hosting clinical systems and patient data.

Approach to Implementation

This work is being taken forward through the Applications and Infrastructure Design Authority. An expert panel has been convened to review proposals.

Timeline for Implementation

Further discovery and scoping work will be conducted in the 2018/19 financial year.

Recommendation 3

By 31st March 2019, all health and social care organisations that provide NHS care through the NHS Standard Contract must provide NHS Digital, on behalf of the Chief Information Officer for health and social care, details of their position against the Data Security and Protection Toolkit. This will help audit compliance against the National Data Guardian's 10 security standards and CQC's well-led Key Lines of Enquiry (KLOE). Position statements are expected to include an action plan setting out how organisations will address any shortfalls in their compliance and plans for the forthcoming GDPR.

Approach to Implementation

All organisations are required to complete the Data Security and Protection Toolkit which will give NHS Digital data at an individual organisation level.

Timeline for Implementation

All organisations contracted under the standard contract are required to complete a final return by 31 March 2019, with an interim return for larger organisations in October 2018.

Recommendation 4

Research will be commissioned by the Chief Information Officer for health and social care to build an evidence base to understand the level of cyber security maturity in social care organisations. This research will be used to identify where additional support to the social care sector can be most effective.

Approach to Implementation

A one-year social care discovery project is being funded through the Cabinet Office's National Cyber Security Programme. This is being carried out jointly by the Department, the Local Government Association and the Care Providers Alliance to understand the current level of data and cyber security in adult social care, and what support would be most effective.

Timeline for Implementation

The discovery project will run until March 2019 and inform support to the adult social care sector from the 2019/20 financial year.

Recommendation 5

All NHS organisations are to ensure that every board has an executive director as data security lead, cyber security risks are regularly reviewed by the board, appropriate counter-measures are in place to mitigate and response plans are in place to address service restoration in the event of a successful attack. As CCGs are the responsible commissioner for GP IT services for general practice, a board member or equivalent senior manager should fulfil this role for CCGs.

Approach to Implementation

The requirement for having a board level executive with responsibility for data security was followed up as part of the 2017/18 Data Security and Protection Requirements survey undertaken by NHS Improvement in May 2018. Wider requirements on leadership will be assured through the Data Security and Protection Toolkit.

Timeline for Implementation

The 2017/18 Data Security and Protection Requirements survey showed that all but one NHS Trusts and Foundation Trusts had a board level executive with responsibility for data security as of May 2018. The Data Security and Protection Toolkit went live in April 2018 and will assure wider leadership requirements on data security with full returns due in March 2019.

Recommendation 6

Health and social care organisations should ensure that local contracts, processes and controls are in place to manage and monitor third party contracts for local IT systems, and that the provisions for software updates and business continuity are understood. CCGs are responsible for this for GP practices.

Approach to Implementation

This requirement will be assured through the Data Security and Protection Toolkit.

Timeline for Implementation

The Data Security and Protection Toolkit went live in April 2018 with full returns due in March 2019.

Recommendation 7

During the first quarter of the 2018/19 financial year, a working group will be established by NHS Digital on behalf of the Chief Information Officer for health and social care, to define standards around the management and patching of diagnostic equipment.

Approach to Implementation

A working group has been established to consider standards for the management and patching of diagnostic equipment. The Medical Devices Regulations and In Vitro Diagnostic Medical Devices Regulations will include a greater focus on cyber security in the regulation of the manufacture of medical devices.

Timeline for Implementation

NHS Digital is reviewing standards for the management and patching of diagnostic equipment with a view to updating guidance and relevant standards by March 2019. The Medical Devices Regulations and In Vitro Diagnostic Medical Devices Regulations will take effect in 2020 and 2022 respectively.

Recommendation 8

Local organisations' business continuity and disaster recovery plans should include the necessary detail around response to cyber incidents, and must include a clear assessment of the impact of the loss of these services on other parts of the health and social care system. In addition, these plans must identify critical third-party services (provided by other health, social care and private sector organisations), setting out the impact of the loss of these services on their operations and necessary business continuity actions required to address the loss of such services. Plans should be regularly tested across local areas both with the NHS and its partners, and reviewed and updated locally with board level oversight.

Approach to Implementation

This requirement will be assured through the Data Security and Protection Toolkit.

Timeline for Implementation

The Data Security and Protection Toolkit went live in April 2018 with full returns due in March 2019.

Recommendation 9

It is recommended that NHS Digital appoint a system-wide Chief Information and Security Officer (CISO). In addition, it is recommended that NHS Digital appoints a dedicated Cyber

Security Lead working across NHS England, NHS Improvement and other partners such as local government in each of the NHS England regions (North, Midlands and East, London, South East and South West).

Approach to Implementation

NHS Digital has recruited a CISO and recruitment of regional leads is underway.

Timeline for Implementation

These roles are expected to be filled by December 2018.

Recommendation 10

We recommend that, where they exist, NHS providers join and collaborate with local Warning Advice and Reporting Point groups to share trusted up-to-date advice on information security, cyber threats, incidents and solutions.

Approach to Implementation

This recommendation will be reflected in best practice guidance.

Timeline for Implementation

Best practice guidance will be updated in 2018/19.

Recommendation 11

In addition to local boards assuring themselves that they have sufficient quality and capable IT technical resources to manage and support their local IT infrastructure, systems and services, we recommend that pooled resourcing arrangements are formalised and captured in Sustainability and Transformation Plans or Accountable Care System wide continuity plans in relation to system wide cyber-attacks.

Approach to Implementation

Pooled resourcing arrangements in Sustainability and Transformation Plans or Accountable Care System areas are a local responsibility based on local resourcing requirements and possible efficiencies.

Timeline for Implementation

Organisations will be encouraged to develop business continuity plans with other local organisations as part of their Sustainability and Transformation Plans.

Recommendation 12

Professional community network models should be encouraged for cyber and information security, working in conjunction with organisations such as NHS Digital, The British Computer Society, Health Education England and the NHS Digital Academy.

Approach to Implementation

This is a best practice recommendation.

Timeline for Implementation

To be implemented locally depending on local priorities.

Recommendation 13

Boards for NHS organisations should undertake annual cyber awareness training and further consideration should be given to the training needs for social care providers arising from

recommendation 4. The standards for training will be established nationally in 2018 by the Chief Information Officer for health and social care. In addition, whilst we do not formally recommend it, all organisations should consider whether access to IT systems and services should be removed from members of staff who have not successfully completed this mandatory training.

Approach to Implementation

NHS Digital is delivering board training to local organisations as part of its “Blue Team” intervention programme. This training is GCHQ accredited and is supplemented by tools which will support boards to understand their cyber risk and the steps they need to take. The training to boards is being delivered jointly by NHS Digital and NHS England to ensure that it is supplemented with specific tools to help boards understand and address the cyber security risk faced by their organisation. This approach combines meaningful technical improvements with equipping senior leaders with the knowledge and skills they need.

Timeline for Implementation

Following engagement with local organisations to understand their training needs, pilots have been completed and the programme will now be rolled out nationally to all Trusts and Foundation Trusts.

Recommendation 14

In addition to mandatory and statutory training, organisations should ensure that their staff receive regular and targeted cyber and information security awareness training appropriate to their job role. This may range from internal phishing attacks to test the awareness of staff to the danger of opening spam email, through to specific training associated with the management of cyber incidents.

Approach to Implementation

The programme will establish national standards for training. The timing of training requirements to systems access is a matter for local organisations depending on their circumstances.

Timeline for Implementation

National e-learning for health and care staff has been delivered. Accredited board training is being rolled out to all Trusts and Foundation Trusts following a successful pilot phase. Training will be maintained and updated reflecting feedback and ongoing training needs analysis.

Recommendation 15

It is recommended that NHS Digital proactively publish guidance about the CareCERT service and maintain a clear and consistent view of the technology landscape across local organisations. In the longer term, NHS Digital should have the ability to isolate organisations, parts of the country or particular services in order to contain the spread of a virus during an incident.

Approach to Implementation

NHS Digital proactively publishes guidance about their data and cyber security services and maintains a clear and consistent view of the technology landscape across local organisations. In the longer term, NHS Digital should have the ability to isolate organisations, localities or particular services to contain the spread of a virus during an incident.

Timeline for Implementation

NHS Digital continues to promote its data and cyber security services and continuously improve communications. The ability to isolate organisations is being explored as part of the

implementation of Microsoft Advanced Threat Protection and iterative development of the Cyber Security Operations Centre in 2018.

Recommendations 16, 17 & 18

It is recommended that NHS Digital enhance its procedures to support regional Emergency Planning and Rapid Response planning (EPRR) and long running incidents and ensure that it works jointly with NHS England's EPRR process, including developing appropriate back-up processes in the event of a cyber incident.

It is recommended that NHS England, working with its partners, describe the EPRR processes for managing incidents on areas such as diagnostic equipment, NHS suppliers and logistic firms, high street pharmacies, dentists, care homes and private providers in the event of a local cyber attack.

It is recommended that NHS England, working with its partners, develop scenarios to ensure that it can manage a co-ordinated or multiple attack whereby, for instance, a terrorist bombing attack is combined with a cyber attack.

Approach to Implementation

These recommendations have been incorporated into Emergency Planning and Rapid Response planning, the cyber incident playbook, and NHS Digital services.

Timeline for Implementation

Implemented.

Recommendation 19

It is recommended that an annual national cyber rehearsal is undertaken by the DHSC, NHS England, NHS Improvement and NHS Digital, and that regional and local organisations similarly undertake regular tests of their EPRR in the event of a cyber incident.

Approach to Implementation

Regular incident exercises have been incorporated into the data and cyber security programme.

Timeline for Implementation

Key elements of incident response will be tested by Autumn 2018 with the next large scale exercise in Spring 2019.

Recommendation 20

The DHSC, NHS England, NHS Improvement and NHS Digital should develop joint protocols for clear and consistent communications to local organisations to provide updates, advice and guidance incidents and for local reporting. This should include working with local organisations and relevant networks to identify alternative communication channels in the event of distribution to standard channels.

Approach to Implementation

Updated communications protocols have been incorporated into the cyber incident response playbook.

Timeline for Implementation

Implemented.

Recommendation 21

NHS Digital should develop their on-call and major operating guidelines to ensure the right expertise and seniority of decision making is available in the event of another cyber attack. NHS Digital's contact centre also needs to be sufficiently resourced to address information requests during an incident.

Approach to Implementation

NHS Digital have reviewed and updated their on-call protocol.

Timeline for Implementation

Implemented.

Recommendation 22

CSUs must be cyber accredited and responsible for coordinating a cyber response across primary care and CCGs. All parts of the country must be covered by a CSU and all GP practices and CCGs must receive IT support from cyber accredited suppliers. NHS Digital should draw up a national response protocol and all approved IT suppliers must comply with it to ensure 24/7 on call care and linkages to CSUs.

Approach to Implementation

Appropriate data security requirements have been included in the GP IT operating model.

Timeline for Implementation

Implemented.