Department of Health & Social Care

Securing cyber resilience in health and care

Progress update 2019

Published 04 November 2019

Contents

Progress update 2019: summary

This is the third in a series of progress reports published by the Department for Health and Social Care since the May 2017 WannaCry cyber attack.

We published our first progress report in February 2018. Our last progress report 'Securing cyber resilience in health and care: A progress update', published in October 2018, highlighted the procurement of the Cyber Security Operations Centre (CSOC), the launch of the Data Security and Protection Toolkit and the signing of a Microsoft Windows 10 licensing agreement. We have now worked with our delivery partners to collate a third progress report on action to build cyber resilience in health and care. This report describes our progress over the past 12 months and looks forward to 2020.

We have also continued our work to implement the recommendations of the Chief Information Officer (CIO) set out in Health and Care's review of the May 2017 WannaCry attack. Detailed information on this work is outlined in Annex A.

1. We are strengthening national leadership for cyber security

1.1 The publication of the NHS Long Term Plan in January 2019 reinforced the Government's commitment to digitalisation and the use of advanced technologies in the NHS.

1.2 In July 2019, NHSX was set up as a joint unit made up of teams from the Department of Health and Social Care (DHSC) and NHS England and Improvement (NHSE/I) to lead on the largest digital health and social care transformation programme in the world and deliver the Health Secretary's Tech Vision, building on the NHS Long Term Plan.

1.3 It is a key priority for NHSX to ensure NHS systems and data are secure through delivery of the cyber security transformation programme. NHSX will publish a Cyber Security Strategy for health and care in 2020, which will provide an overarching framework for cyber security in the NHS and social care. NHSX will engage and work collaboratively with stakeholders and industry partners to develop a comprehensive plan for what the sector needs and how it might be achieved.

2. We are addressing cyber security risks and vulnerabilities at local level by taking action at the centre

2.1 NHS Trusts now benefit from access to Microsoft Defender Advanced Threat Protection (ATP), which is providing real time detection and protection against potential threats by identifying suspicious behaviour on devices indicative of a cyber-attack. Roll out of ATP by NHS Digital is providing local organisations and NHS Digital with enhanced ability to see cyber activity at machine level across the NHS, as well as whether machines have been patched to protect them from new cyber threats. The presence of ATP has enabled the CSOC to provide a national view of the cyber threat across local organisations and also empower them to take immediate steps to manage and mitigate their own cyber risk across their local environments. In conjunction with new capabilities in protective monitoring, threat intelligence and threat hunting, the presence of ATP has meant the CSOC has been able to prevent a number of potentially significant threats from malware and phishing which could have otherwise had a significant impact. As of September 2019, deployment levels have reached over one million devices.

2.2 NHS Digital are also supporting NHS organisations to migrate to the Windows 10 Operating System to maintain secure and up to date systems. Windows 10 is more secure and significantly faster than Windows 7, saving NHS staff time in delivering patient care. This programme of work is critical as unsupported and unpatched systems were key risk factors in the WannaCry attack.

2.3 Rollout of Windows 10 is now underway and on track. Over half a million NHS devices have now been migrated. Through ATP, NHSD can see in real-time where every organisation is in relation to deployment of Windows 10. NHSX will closely track that information and will intervene where any organisation is failing to meet its agreed migration deadlines. If needed, NHSX will implement sanctions including using its powers under the Network and Information Systems (NIS) Regulations.

2.4 Extended support is in place to 2021 for those organisations involved in the Microsoft licencing deal who need longer to migrate and need to keep using Windows 7 in the meantime. All NHS organisations have agreed to migrate by no later than December 2020, the majority will do so by early next year.

2.5 We have now launched the Cyber Security Operations Centre (CSOC) which provides the ability to undertake protective monitoring at a scale and level of detail not previously possible. This makes it quicker and easier to predict, detect, prevent

and respond to data and cyber security incidents across the NHS. So far, the CSOC has also delivered:

- a new security monitoring platform that can detect incidents across the NHS, including five national applications such as the NHS Spine (the NHS's core information sharing infrastructure).

- an online cyber security training platform and roll-out of licences to around 500 IT and security staff across the health and care system;

- a threat intelligence and hunting framework which improves the CSOC ability to proactively search for, detect and address threats.

2.6 In December 2019, the NHS Secure Boundary will go live. It provides a cutting-edge perimeter security solution at no cost to NHS organisations, delivering additional security monitoring and prevention defences for the multiple internet connections in use across the system, providing visibility and control to local organisations so they can better manage their own risk. For NHS Digital it will provide highly enriched threat intelligence, enabling them to respond at pace and scale during incidents and emerging threats. It is designed to support the "Internet First" and "Cloud First" agendas which all contribute towards NHSX's Tech-Vision and the Long-Term Plan.

3. We have a clearer picture of cyber security maturity in the NHS

3.1 We are using the Data Security and Protection Toolkit (DSPT) to measure performance against the National Data Guardian's (NDG) 10 Data Security Standards. The DSPT is specifically tailored for different types and sizes of organisation and helps them understand their data and cyber security risks. Over 27,000 organisations have completed the DSPT with 97% of organisations meeting the NDG's 10 Data Security Standards. Large organisations, including NHS Trusts, assessed as "Standards Not Met" must submit an improvement plan to NHS Digital. The status for the majority of those organisations has now been raised to "Standards not Fully Met (Plan Agreed)". NHSX is now working directly with the remaining organisations to address outstanding issues.

3.2 Analysis of the complete first set of DSPT data provided us with an overall picture of progress made by NHS organisations and highlighted areas where challenges remain, for example with training, IT protection and continuity planning. It also provided an in-depth picture of Trusts' individual cyber resilience and maturity, so we can provide a more tailored approach to helping them improve. For example, NHSD is working with NHS Trusts to:

- review improvement plans and challenge any organisations which have claimed compliance with the toolkit standard where this is not visibly supported by the evidence provided.

- signpost Trusts to relevant offerings within the NHS Digital Cyber Security Support Model (CSSM).

- equip Boards with the right information (relative cyber risk exposure and position) through the development of a Cyber Business Intelligence and Risk platform and cyber metrics which is due to be rolled out in the first half of 2020.

4. We are supporting local organisations to strengthen their leadership for cyber security and to address capacity and capability issues

4.1 To further support the NHS to meet their cyber security responsibilities, keep patients safe and improve response and resilience to cyber security incidents, NHSD has developed the Cyber Security Support Model (CSSM). As a free wrap-around level of cyber support for local organisations it provides:

- a clearer picture of particular strengths and weaknesses at Trust level through the delivery of an on-site assessment. All NHS Trusts except one have now had an assessment and submitted action plans covering what they need to do to improve their resilience. NHSD are engaging with the one outstanding Trust to arrange their assessment in due course

- training for Board and Senior Information Risk Owners (SIROs) so that key individuals within an organisation understand the importance and nature of cyber security and risk. Since its launch in November 2018 over 170 boards have received the training with 61 organisations availing of SIRO training after its launch in July 2019.

- A national cyber communications and awareness campaign, the 'Keep I.T. Confidential' campaign. Ensuring the NHS can share data in order to support high quality, safe patient care is a priority; taking data security measures helps staff feel confident that they will be sharing the right information with the right people. The campaign aims to drive cultural change by educating all NHS staff on the direct impact of data and cyber security on patient care, and the steps they can personally take to reduce the risks of a cyber incident. Since its launch in September 2019, over 340 organisations have accessed the website and downloaded the available material.

- access to the Cyber Associates Network: a strong community of experts who share best practice and build resilience at grass roots level in local organisations.

4.2 NHS Digital continue to work with the Care Quality Commission (CQC) to cooperate more closely on assessments of how well-led organisations are in relation to cyber security, including information sharing and joint inspection activity. If NHSX has specific concerns about an organisation's leadership capability, these

joint inspections can be used to gain a deeper understanding and to help identify leadership improvements. NHSX is continuing work with NHS Digital and CQC to look at how greater cooperation with CQC can add value, including how it can be used to identify what good leadership for cyber security looks like.

5. We are applying cyber security standards across the health and care system

5.1 Our clear message to all NHS and social care organisations is that the cyber security standard they should aim for is to meet the cyber security requirements set out in the DSPT for their type of organisation.

5.2 NHS Digital have worked with National Cyber Security Centre (NCSC), to include the requirements of Cyber Essentials into the DSPT. The NCSC is the UK's technical authority on cyber security. Cyber Essentials, managed by the NCSC, is a scheme promoting the implementation of technical controls aimed at protecting organisations of all sizes against a range of the most common cyber attacks. For 2020/21, NHS Trusts will be expected to meet the additional requirements in the DSPT which provide equivalence to the Cyber Essentials Plus (CE+) standard when combined with NHS Digital's onsite assessments.

5.3 Where NHS Trusts have not met Cyber Essentials Plus equivalence (measured through the DSPT and an onsite assessment) by March 2021 they will develop and deliver action plans to achieve compliance with the regime within the following three months (June 2021), as set out in the original 2018 CIO Review. NHS Digital can assist such organisations in the development of their action plans through the Cyber Security Support Model. Where significant security orientated infrastructure and / or hardware investment is required, local organisations are able to apply to NHSX's Capital Infrastructure fund for assistance. If any organisation already holds an external standard like CE+ or ISO 27001 providing suitable evidence will mean they can automatically populate relevant areas of the DSPT therefore reducing the reporting burden on local organisations.

We have also worked to bring greater clarity around standards for other types of health and care organisations:

5.4 Cyber security in primary care (GPs): Clinical Commissioning Groups (CCGs) are responsible for providing IT services to general practice, on behalf of NHS England, in accordance with the Primary Care (GP) Digital Services Operating Model 2019-21. The model requires that CCGs commission services only from suppliers that meet the standards of the DSPT. As well as the publication of the 2019-21 Operating Model, the current agreements in place between each GP practice and their commissioning CCG will be updated through the new GP IT

Supply framework, to include an obligation on the GP practice to complete the DSPT annually. Around 90% of practices completed it voluntarily in 2018/19.

5.5 To get insight into cyber security in adult social care, NHSX has commissioned discovery reports into the Technology Enabled Care sector and the Adult Social Care sector. This provided the first in-depth picture of the cyber security risks and challenges these sectors face. We are now using this knowledge to run a series of local pilot projects that will explore how these risks and challenges can be addressed.

5.6 In spring 2018, NHS England and the Local Government Association launched the Local Health and Care Record (LHCR) programme with the objective of joining up Health and Social Care records digitally to enable a better information sharing environment that helps our health and care services continually improve. NHSX have developed with LHCR localities (and NHS Digital support) a comprehensive plan to manage cyber security across their regions, including conducting security assessments and system-based risk assessments. LHCR localities are developing their own local security improvement plans based on the outcomes of these assessments.

6. We are applying new regulatory levers to increase compliance in the NHS

6.1 Since May 2018, the Department has had new regulatory levers to ensure that 'Operators of Essential Services' are taking adequate steps to protect their systems and promptly report any cyber incident or network failure. Under the Network and Information Systems (NIS) Regulations, the Department may issue information, enforcement, and penalty notices to any organisation found to be in serious breach of the regulations.

6.2 We have built the use of NIS information notices into a High Severity Alert (HSA) Process Handbook, and this has proven an effective lever in dealing with non-responders to high severity alerts (i.e. cyber security threats deemed serious enough to demand immediate remediation by organisations).

Case Study - Response to two high-severity CareCERT alerts in 2019

Two high-severity CareCERT alerts have been issued by NHS Digital in 2019 (BlueKeep and DejaBlue). We have used the learning from both HSAs to develop and refine a High Severity Alert (HSA) Process Handbook.

As a result of this new process, NHS Trusts actioned the most recent High Severity Alert (HSA) "DejaBlue" significantly faster than the previous one "BlueKeep", with the whole process now taking 3 weeks, compared to 18 weeks for "BlueKeep".

We will now communicate the new HSA process more widely to ensure that all organisations are aware of the steps they need to take and the deadlines for doing so in the event that a high-severity CareCERT alert is issued.

6.3 We have also made use of NIS information notices to get information from Trusts when they have experienced network outages, in order to gain assurances that the Trusts have dealt quickly and effectively with technical issues and have sufficient plans in place to deal with such issues in the future.

6.4 This year we have used our NIS powers to designate some of the most critical independent providers to the health and care sector as Operators of Essential Services to ensure that the same standards of cyber security that we expect from NHS organisations are being met by private sector organisations. Operators of Essential Services are able to request a review of a decision to designate them or the issuing of a penalty. We have appointed an independent person (the National

Data Guardian for Health and Social Care) to review decisions if an Operator of Essential Services requests a review.

6.5 The application of NIS in the healthcare sector is a good demonstration of regulatory levers being effectively used to increase compliance in NHS organisations and we will continue to develop policy that will allow us to make use of our regulatory levers to drive up standards of cyber security.

7. We continue our programme investment in cyber security

7.1 The work described in this progress report has been delivered (and will continue) through the Data and Cyber Security Programme. The programme is underpinned by a robust governance framework including scrutiny from non-executive directors.

7.2 In total, over £250 million will be invested nationally to improve cyber security of the health and care system by 2021. This excludes monies local organisations have invested themselves into their own cyber security and wider national IT investment which supports better security such as the Microsoft Windows 10 licensing agreement.

7.3 The Programme also receives funding through the Cabinet Office's National Cyber Security Programme. This funding has supported work to test innovative approaches to building cyber resilience in health and care settings including the recent social care discovery programme.

8. Next steps

8.1 The creation of NHSX will bring stronger strategic direction for cyber security in the NHS and social care. Being a joint unit of DHSC and NHSE/I it will enable the centre to more easily to address systemic issues impacting cyber resilience. Whilst significant improvements have been made since WannaCry, the system still faces challenges. We can do more to help organisations in the sector to address those challenges.

8.2 One of our immediate next steps will be providing better guidance and information to the leadership of organisations in the NHS on how their organisations are doing, crucially in the form of metrics and information that give them an objective view of their own cyber resilience.

9. Implementation of the recommendations of the CIO Report

9.1 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 (CIO) 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.

9.2 In our last progress update we set out our approach to implementing the CIO Review recommendations. An update on progress is set out in Annex A.

9.3 NHSX is now closing the implementation of the CIO Review. The majority of recommendations have now been implemented and the remaining recommendations will continue to be addressed through the forthcoming work to develop a future cyber strategy for health and care.

Annex A - CIO Recommendations Progress Update

Recommendation 1

All NHS organisations are to develop local action plans to achieve compliance with the Cyber Essentials Plus (CE+) 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.

Progress update towards Recommendation 1

This recommendation is partially implemented and will be completed by 2021.

All NHS Trusts except one have now had an independent on-site CE+ assessment and submitted action plans covering what they need to do to improve their resilience.

NHS Digital have worked with NCSC to include the requirements of Cyber Essentials into the DSPT. For 2020/21, NHS Trusts will be expected to meet the additional requirements in the DSPT which provide equivalence to the Cyber Essentials Plus (CE+) standard when combined with NHS Digital's onsite assessments. Whilst not mandatory for 2019/20, the Cyber Essentials requirements have been built into the DSPT for this year for NHS Trusts, so they can start to measure their progress.

Where NHS Trusts have not met Cyber Essentials Plus equivalence (measured through the DSPT and an onsite assessment) by March 2021, NHS Digital will ensure they develop an action plan to help them achieve compliance with the regime within the following three months (June 2021) as set out in the original 2018 recommendation.

If any organisation already holds an external standard like CE+ or ISO 27001, providing suitable evidence will mean they can automatically populate relevant areas of the DSPT therefore reducing the reporting burden on local organisations.

The CE+ assessments carried out to date demonstrate that the level of resilience is improving. The assessments help organisations to understand their strengths and vulnerabilities. Based on analysis of the assessment reports, NHS Digital have developed a comprehensive set of free services and support solutions to help Trusts deliver action plans.

This recommendation will continue to be delivered through the new Cyber Strategy for health and care.

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.

Progress update towards Recommendation 2

This recommendation is ongoing and will be delivered in full through the forthcoming work on a Cyber Strategy to be published in 2020.

The Cyber Design Authority has reviewed proposals for IT infrastructure standards. A number of standards have been identified and are in development. Agreement on relevant standards will now progress as part of strategy owned by NHSX.

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 DSPT. 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.

Progress update towards Recommendation 3

This recommendation has been implemented.

The DSPT has been in place since March 2018. Over 27,000 organisations have published a self-assessment. All NHS Trusts, CCGs and CSUs completed the DSPT in 2018/19 with the programme working to improve returns for social care, dentistry and optometry sectors.

DSPT service delivery continues to work to increase submissions and achieve full compliance with the National Data Guardians 10 Data Security Standards by 2021.

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.

Progress update towards Recommendation 4

This recommendation has now been implemented.

The Adult Social Care Data and Cyber Security Programme Report was published in May 2019. The report is now informing the piloting of products and services to improve resilience in adult social care. Future work will be taken forward through the new Cyber Strategy.

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.

Progress update towards Recommendation 5

This recommendation has now been fully implemented.

The DSPT went live in April 2018 and full returns were submitted in March 2019. The DSPT provides assurance on board level representation and wider leadership requirements on data security. Organisations are asked to improve through continual assurance where the standards are not met. As part of the CSSM offering, NHS Digital also provides local organisations with access to the Unified Cyber Risk Framework to further help them achieve compliance with this recommendation.

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.

Progress update towards Recommendation 6

This recommendation has now been fully implemented.

The DSPT went live in April 2018 and full returns were submitted in March 2019. The DSPT provides assurance on third party contracts. Organisations are asked to improve through continual assurance where the standards are not met. As part of the CSSM offering, NHS Digital also provides local organisations with access to the Cyber Operational Readiness Service to further help them achieve compliance with this recommendation.

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.

Progress update towards Recommendation 7

This recommendation has now been implemented and work will continue in this area through the Cyber Strategy.

A working group has been established to consider standards for the management and patching of diagnostic equipment. The guidance to manage the risks from use of medical devices was updated in October 2019. Additionally, the Medicines & Healthcare products Regulatory Agency have written into UK law two EU regulations relating to managing medical devices, which will come into effect when the UK leaves the EU.

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.

Progress update towards Recommendation 8

This recommendation has now been fully implemented.

The DSPT went live in April 2018 and full returns were submitted in March 2019. The DSPT provides assurance on local organisations' cyber incident response plans. Organisations are asked to improve through continual assurance where the standards are not met. The programme continues to provide support for regional exercises and to test local plans/responses, integrating national and local processes where necessary.

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).

Progress update towards Recommendation 9

This recommendation is partially implemented. Due to complete February 2020.

An interim CISO is in place while permanent recruitment continues. Three of five regional leads are in place. Recruitment for the remaining two regional leads will complete by February 2020.

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.

Progress update towards Recommendation 10

This recommendation has now been fully implemented.

An early warning system is now in place for incidents. Local organisations have been advised to join the Warning Advice and Reporting Point (WARP). In the North West region, WARP membership is centrally funded for all organisations.

Additional formal and informal alerting systems have been developed since the Wannacry attack, including the wider use of the GOV Notify SMS system, CIO/CISO/CCIO discussion networks, and the development of the Cyber Associates Network. The programme will continue to encourage regions to advocate joining their local WARP.

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.

Progress update towards Recommendation 11

For local implementation.

Sustainability and Transformation Partnerships continue to pool resources where applicable at a local level. NHS Digital regional leads can provide localised support for national services, infrastructure, systems and services.

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.

Progress update towards Recommendation 12

This recommendation has now been fully implemented.

A Cyber Associates Network was created in October 2018 which now has over 750 members from across 250+ organisations. The network is continuing to grow and provides members with access to relevant training and resources.

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.

Progress update towards Recommendation 13

This recommendation is partially implemented and work continues to March 2020.

The agreed GCHQ certified board training programme is being rolled out by NHS Digital nationally to all Trusts and Foundation Trusts. As of August 2019, over 80% of NHS Trusts have engaged in board level training; the remainder are targeted for March 2020.

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.

Progress update towards Recommendation 14

This recommendation has now been fully implemented.

A portfolio of relevant training has been agreed with input from local Health and Care organisations and also from the Cyber Associates Network. This includes work in partnership with Health Education England to ensure cyber security awareness training is included in their Building a Digital Ready Workforce programme. The training portfolio will continue to be refined based on user needs with local organisations deciding on appropriate timing of training for staff. Additionally, organisations are asked to ensure they have appropriate cyber and data security training as part of the DSPT assessment.

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.

Progress update towards Recommendation 15

This recommendation has now been fully implemented.

NHS Digital continue to promote CareCERT and maintain a view of the technology landscape. The roll out of Microsoft Windows Defender Advanced Threat Protection (ATP) enables the ability to isolate down to machine level. Improved monitoring and alerting of security incidents are now in place across the national networks.

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.

Progress update towards Recommendations 16,17 & 18

These recommendations have been implemented.

They have been incorporated into Emergency Planning and Rapid Response planning, the Data and Cyber Security Incident Joint Operational Handbook, and NHS Digital services.

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.

Progress update towards Recommendation 19

This recommendation has now been fully implemented.

A second national rehearsal was completed in May 2019, to be repeated annually alongside ongoing drills which test individual scenarios. NHS England continues to support local organisations to test their EPRR.

Recommendations 20, 21 & 22

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 disruption to standard channels.

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.

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.

Progress update towards Recommendations 20, 21 & 22

These recommendations have been implemented; we continue to improve implementation through CSU collaboration.

Published to GOV.UK in pdf format only.

NHSX/Cyber Security

www.gov.uk/dhsc