Department of Health & Social Care

NHS Improvement

NHS England

Lessons learned review of the WannaCry Ransomware Cyber Attack

February 2018

Title: Lessons learned review of the WannaCry Ransomware Cyber Attack
Author: William Smart - Chief Information Officer for Health and Social Care
Document Purpose: Independent Report
Publication date: 1 February 2018
Target audience: Public
Contact details: William Smart , Chief Information Officer for Health and Social Care Skipton House, 80 London Road, London, SE1 6LH Email: England.CIOReview@nhs.net

Published to gov.uk, in PDF format only.

www.gov.uk/dh

Lessons learned review of the WannaCry Ransomware Cyber Attack

Prepared by

William Smart, Chief Information Officer for the Health and Social Care System

Contents

Foreword

The Department of Health and Social Care's Data Security Leadership Board commissioned the Chief Information Officer for the health and social care system in England to carry out a review of May 2017's WannaCry cyber attack. The purpose of this report is to analyse the lessons learned, assess actions taken so far and make clear recommendations on what further measures are required to ensure the entire health and social care system is as robust as it can be in reducing the risk and impact of a future cyber attack.

For the first time, this review draws together key messages from the NHS's internal assessments and two national reviews[1] with key themes from lessons learned reports from local organisations.

On Friday 12 May 2017, a global ransomware attack, known as WannaCry, affected a wide range of countries and sectors. Although WannaCry impacted the provision of services to patients, the NHS was not a specific target.

The NHS responded well to what was an unprecedented incident, with no reports of harm to patients or of patient data being compromised or stolen. In total, 1% of NHS activity was directly affected by the WannaCry attack. 80[2] [3] out of 236 hospital trusts across England were affected[4], which means that services were impacted even if the organisation was not infected by the virus (for instance they took their email offline to reduce the risk of infection). 595 out of 7,454[5] GP practices (8%) and eight other NHS and related organisations were infected. This disruption to patient care has made it even clearer how dependent the NHS is on information technology and, as a result, the need for security improvements to be made across the service.

The incident also highlighted areas for improvement both within individual NHS organisations and across the system as a whole. Since the attack, urgent action has been taken to tackle these challenges, building on existing significant programmes of work that have been underway since 2010 to improve cyber resilience across the health and care system. These measures include support for local organisations to upgrade from Windows XP in 2010[6] and 2014[7], and the establishment of CareCERT by NHS Digital, one of only two sector-specific cyber support services in England.

Identified areas for improvement include the need for senior leadership and Board level accountability for cyber security in every health and care organisation. Local organisations must ensure effective management of their technology infrastructure, systems and services, including the adequate patching of devices and systems, ensure sufficient network security and replace unsupported software. Nationally, a new agreement with Microsoft has been signed, which includes patches for all its current Windows devices operating XP.

WannaCry has made clear the need for the NHS to step up efforts with cyber security so that every possible protection is taken to defend against a future attack.

---

[1] National Audit Office Investigation: WannaCry cyber attack and the NHS (October 2017) and National Cyber Security Centre 2017 Annual Review.

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

[3] Following publication of the NAO report on WannaCry, four NHS trusts contacted the NAO contesting their categorisation (as either "infected" or "affected") and have requested that the report be amended. The headline impact of this reclassification is to change the number of impacted trusts from 81 to 80.

[4] NHS England EPRR data; National Audit Office Investigation: WannaCry cyber attack and the NHS (October 2017)

[5] http://www.nhsconfed.org/resources/key-statistics-on-the-nhs

[6] NHS purchased rights for the NHS to use Windows 7 and all previous versions.

[7] Government funded an additional year of support for Windows XP.

As other industries have learned, no organisation can be completely immune from a cyber attack and there is no room for complacency. The occurrence of cyber attacks across the UK economy is increasing so, in the judgement of most industry experts, it is not a question of "if" but "when" the next cyber-attack strikes the health and social care system[8]. Data collected by the Information Commissioner's Office shows the healthcare sector accounted for the highest number of data security incidents in the third quarter of 2016, with 74 of the NHS's 239 reports related to cyber security incidents[9]. Although the majority of these were dealt with effectively, it is important that we take every measure to protect and defend health and care organisations against threats to their cyber security[10]. Our challenge is to change our mind-set to one that systematically evaluates and manages the threat to our services posed by cyber attacks.

All health and social care organisations can, and should, have strong cyber security measures in place, not least because the protection of our patients' confidential health and social care data is fundamental to delivering high quality and safe services. It is also clear that a one-size-fits-all approach will not work across health and social care. Our response needs to be proportionate to the scale and type of services being provided by each organisation, given the difference between a large acute hospital or major trauma centre and a small residential care home. Overall, it is critical that we maintain trust and confidence in the services we deliver, as information technology becomes ever more integral to the health and social care system.

Consequently, every organisation and individual working in health and social care needs to take stock of the actions that they are required to take to increase cyber resilience across the system; ensuring that the effectiveness of these actions is actively monitored and any short-falls rectified.

In July 2016, the National Data Guardian published 10 data security standards[11], which have been designed to address basic cyber vulnerabilities. Adherence to these standards by the health and care system could have significantly mitigated the impact of the WannaCry attack on our services. The NHS will now actively ensure that these standards are embedded across the service as part of a longer term improvement strategy.

Finally, as we saw during the WannaCry incident, people are at the heart of our defence against cyber attacks. I would again like to thank all staff involved during the incident for their resilience and extraordinary efforts in going the extra mile to keep our health and care services running for our patients. The dedication and hours put in by staff across all parts of the NHS during the incident may not have been widely known, but made a huge contribution to containing the disruption to patients, and so I wanted to take this opportunity to officially recognise and commend our staff publicly.

William Smart, Chief Information Officer – health and social care system

[8] Annual Review 2017 National Cyber Security Centre
[9] http://www.information-age.com/cyber-security-nhs-123464777/
[10] Annual Review 2017 National Cyber Security Centre
[11] https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

1. Introduction

Background

1.1. The Department of Health and Social Care's (DHSC) Data Security Leadership Board (DSLB) commissioned the Chief Information Officer (CIO) for the health and social care system in England to carry out a review of May 2017's WannaCry cyber attack.

1.2. The report sets out the events that occurred during the WannaCry cyber attack and describes the health and social care system's response to the incident. It also describes the immediate actions taken to recover, learn from and reduce the immediate risk of a future cyber attack. The report analyses lessons learned and provides recommendations on how the health and social care system can reduce the risk of a similar cyber attack in the future and improve responsiveness and action in the event of major incident.

Evidence and analysis

1.3. In reaching its conclusions, this review has synthesised key messages from reviews undertaken since the WannaCry attack[12], as well as local lessons learned reports received following a request from the CIO for the health and social care system to the CEOs of trusts and Clinical Commissioning Groups (CCGs).

1.4. The review team has met with stakeholders including the British Medical Association and General Practitioners Committee[13] and held steering review meetings with representatives from the National Cyber Security Centre (NCSC), Cabinet Office, DHSC, NHS Digital, NHS England, NHS Improvement, CIOs and the Local Government Association[14].

1.5. The review engaged with patients across England for their feedback on the impact on care via the DHSC sponsored voluntary and third sector community group network, the Health and Wellbeing Alliance, #NHS Citizen Twitter and NHS England's stakeholder forum for primary care digital transformation.

The scale of the health and social care sectors

1.6. The NHS cares for over 1 million patients every 24 hours in 236 trusts (comprising acute and specialist hospitals, community service providers and ambulance services) and 7,454 GP practices[15]. The NHS in England employs just over 1 million full-time equivalent staff (not including those working in general practice)[16]. Total health spending in England is nearly £124 billion in 2017/18, with around £110 billion spent on the day-to-day running of the NHS, with the remainder on public health initiatives, education, training, and infrastructure (including IT and buildings)[17].

1.7. There are 1.58 million people employed in adult social care in England[18], with around 20,000 organisations delivering a range of services that include residential care and nursing homes providing personal care and accommodation, as well as care provided in

[12] Including National Audit Office Investigation: WannaCry cyber attack and the NHS (October 2017); National Cyber Security Centre 2017 Annual Review, plus other internal NHS reviews and lessons learned documents.
[13] The body which represents all GPs in the UK. It deals with all matters affecting NHS GPs, whether or not they are BMA members.
[14] Refer to Appendix1
[15] http://www.nhsconfed.org/resources/key-statistics-on-the-nhs
[16] https://www.kingsfund.org.uk/projects/nhs-in-a-nutshell/nhs-staffing-numbers
[17] https://fullfact.org/health/spending-english-nhs/
[18] Skills for Care State of the Adult Social Care Sector and Workforce in England, 2017.

the community through domiciliary care services. Whilst local authorities have statutory responsibilities for wellbeing, care and support services, many social care providers operate as private and independent organisations. Over £20 billion of public funding is spent annually on social care services[19].

The WannaCry attack

1.8. Although it was not directly aimed at the NHS, the WannaCry cyber attack highlighted vulnerabilities within the NHS in England. It exposed a need to improve across all parts of the NHS, including improved discipline and accountability around cyber security at senior leadership and Board level, the importance of swift and effective patching of systems when new security updates are released, and historic underinvestment in network security and up to date software.

- None[20] of the 80 NHS organisations affected by WannaCry had applied the Microsoft update patch[21] advised[22]by NHS Digital's CareCERT bulletin on 25 April 2017 following the receipt of intelligence of a specific threat from BT on 24 April 2017.
- Whether organisations had patched their systems or not, taking action to increase the security of their network firewalls facing the N3 network would have guarded organisations against infection[23].
- This was an attack using a specific Microsoft Windows vulnerability, not an attack on unsupported software. The majority of NHS devices infected were running the supported, but unpatched, Microsoft Windows 7 operating system. Unsupported devices (those on XP) were in the minority of infected devices[24] and the number of these devices has decreased in the last 18 months from 18% to 1.8% in January 2018.
- NHS organisations and staff in every GP Practice, hospital and clinic are connected by N3, a private national broadband network built and managed by BT. In addition, many local authorities have N3 network access to facilitate information sharing between health and social care organisations. The N3 network is currently being replaced by the Health and Social Care Network (HSCN), which will provide an opportunity to facilitate greater connectivity between the NHS, local authorities and social care providers.
- Healthcare is a complex environment with many connected systems. Some critical medical devices/equipment still use Microsoft XP software supplied by third parties and were affected, including for example, MRI scanners and blood test analysis devices[25]. This meant that, in some cases, even if a specific diagnostic device was working normally, the software being used to, for example, view X-rays or access blood test results, may not have been available because it was on an infected device or one that had been quarantined because it operated using unsupported software.

---

[19] Health and social care funding explained, The Health Foundation: http://www.health.org.uk/node/10302

[20] NHS Digital reported to the National Audit Office Investigation: WannaCry cyber attack and the NHS (October 2017, p.16) that all NHS organisations infected by WannaCry had unpatched, or unsupported, Windows operating systems.

[21] Microsoft issued a patch to address this vulnerability on 14 March 2017
[22] Note, organisations were advised not instructed. NHS Digital has no powers to mandate organisations.
[23] National Audit Office Investigation Report into WannaCry and the NHS, October 2017.
[24] Ibid, p.10.
[25] NHS England EPRR Cyber Incident Facilitated Debrief, June 2017.

1.9. During the incident, national bodies worked together to coordinate advice and support to NHS organisations in restoring services and addressing vulnerabilities to the malware attack. NHS England instituted its major incident protocol and coordinated the response through the same team that would deal with any other national major incident. This created a robust framework through which to manage the incident. Lessons have been learned about how a cyber incident differs from other types of major incident.

2. The WannaCry attack

2.1. The WannaCry cyber attack began on the morning of Friday 12 May 2017 and, within a day, was reported by Europol to have infected more than 230,000 computers in at least 150 countries[26] [27]. This global attack quickly became a matter of public concern, with the UK's national media paying particular attention to the impact and the response of the NHS in England.

2.2. The cybersecurity firm Avast identified WannaCry as one of the broadest and most damaging cyber attacks in history[28]. The majority of the attacks targeted Russia, Ukraine and Taiwan but Chinese universities, Spanish Telefonica, Russia's Interior Ministry and global firms like FedEx also reported that they had been impacted alongside the NHS[29]. Nissan Motor Manufacturing UK in Tyne and Wear halted production after the ransomware infected some of their systems and Renault stopped production at several sites in an attempt to stop the spread of the ransomware.

2.3. The WannaCry ransomware cryptoworm targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payment in the Bitcoin cryptocurrency. The initial infection was likely through an exposed vulnerable internet-facing Server Message Block (SMB) port[30], rather than email phishing as initially assumed[31].

2.4. The work of a cybersecurity researcher, who activated a 'kill-switch'[32] on the evening of Friday 12 May, had the effect of stopping WannaCry infecting further devices. Without this intervention, it is likely that the impact that WannaCry had on services would have been even greater.

Incident chronology

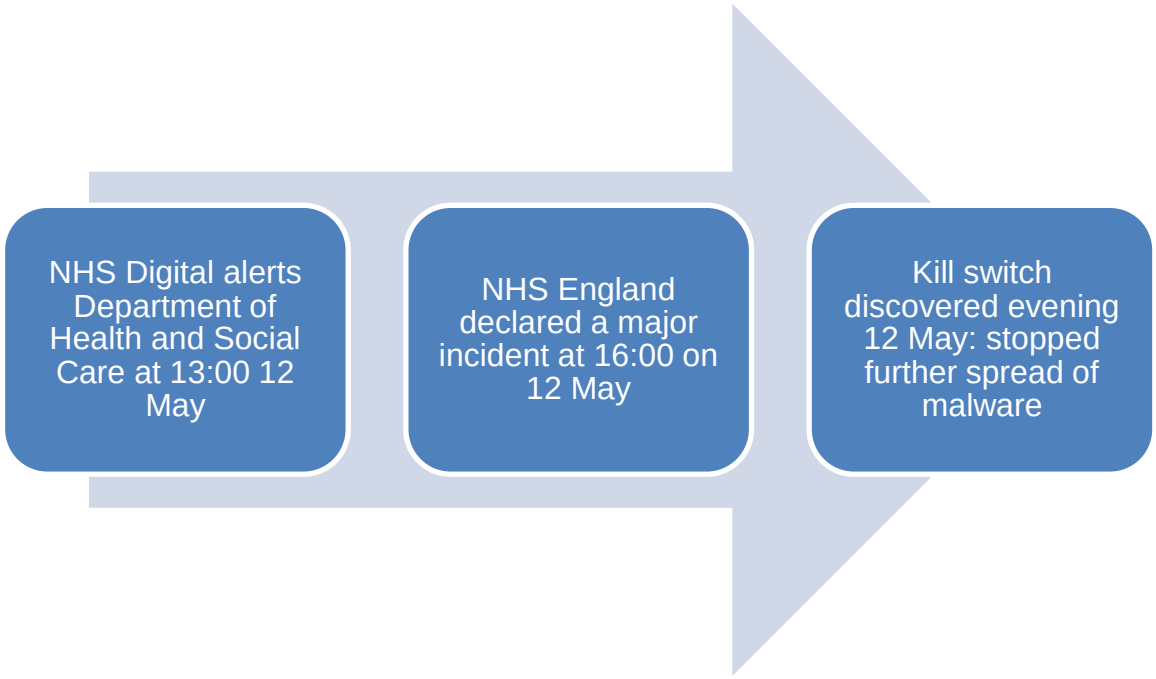
2.5. NHS Digital's CareCERT service alerted the DHSC just after 13:00 on 12 May 2017 following reports from four NHS trusts of ransomware attacks impacting multiple NHS organisations. This had increased to 16 trusts by 16:00. At this point, NHS England declared a major incident and initiated its existing Emergency, Preparedness, Resilience and Response (EPRR) plans and acted as the single point of coordination for incident management with support from NHS Digital and NHS Improvement.

2.6. The NHS response to the attack had three phases:

- Securing the emergency care pathway – Friday to Sunday (12 to14 May 2017);
- Assuring primary care was operationally stable – Saturday evening to Monday morning (13 to 15 May 2017);
- Ongoing remediation, wider system actions and the anti-virus update.

[26] Cyber-attack: Europol says it was unprecedented in scale". BBC News. 13 May 2017.
[27] Unprecedented cyber-attack hits 200,000 in at least 150 countries, and the threat is escalating. CNBC. 14 May 2017.
[28] https://blog.avast.com/wannacry-update-the-worst-ransomware-outbreak-in-history
[29] http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/
[30] Dan Goodin. An NSA-derived ransomware worm is shutting down computers worldwide. ARS Technical. 14 May 2017
[31] Bill Brenner. WannaCry: the ransomware worm that didn't arrive on a phishing hook. Naked Security. Sophos. 18 May 2017.
[32] A 'kill-switch' is a mechanism that is incorporated into software to shut down that software, or the device on which it sits, in an emergency situation in which it cannot be shut down in the usual manner: National Audit Office Investigation: WannaCry cyber attack and the NHS (October 2017).

FIGURE 1: MALWARE DISCOVERY TO INTERCEPTION



2.7. The incident lasted a week. It was formally "stood up" at 16:00 on Friday 12 May 2017 and "stood down" at 17:30 on Friday 19 May 2017. Over the course of the evening of the 12 May, the incident management gained pace with:

- A national EPRR conference call taking place at 16:00. Further national calls would continue into the evening;
- At 16.55, NHS Digital released an NHS-wide CareCERT cyber bulletin with a technical description of the ransomware and remediation advice;
- At 17:00, NHS England took part in an incident briefing with the Secretary of State for Health;
- From 17:00, regional incident coordination centres in NHS England began to coordinate positive assurance around CareCERT communications and actions with local organisations.

2.8. Throughout Friday 12 May, local organisations worked to resolve, and in many cases, prevent infection. Informal leadership networks shared information across local and national organisations, supporting the formal EPRR processes.

2.9. That same evening, a ‘kill switch’ was discovered by a UK malware researcher which stopped the malware spreading further.

2.10. Over the weekend of 13 and 14 May, NHS England’s EPRR team worked with the DHSC, NHS Digital, NHS Improvement and the NCSC to coordinate the NHS’s response to the incident, including the provision of incident coordination, information, advice and guidance to local NHS organisations as they restored services and addressed their vulnerabilities to the malware attack. The initial focus of this activity was on securing and protecting emergency care services. During the weekend, local NHS trusts, partner organisations and regional NHS teams initiated conference calls, collaborating together across sectors of care to share knowledge, resources and information to support the response and resolution.

2.11. On 13 May, five acute trusts were operating some diverts from their A&E departments and a number of trusts were experiencing issues with diagnostic services (e.g. MRI and Computed Tomography (CT) scanning). The diverts were lifted on 16 May, although some elective appointments and procedures continued to be cancelled.

2.12. On 14 May, the NHS Digital CareCERT team released a number of NHS-wide guidance documents, including patching guidance with an accompanying letter, frequently asked questions and a Wannacry alert broadcast with further technical advice.

2.13. As a result of reports of the widespread impact of the virus on diagnostic devices, an information request was sent out to all trusts on 14 May requesting information on the types and numbers of diagnostic devices that had been infected by WannaCry. Coordinated action to engage with device manufacturers to manage the production and implementation of patches for infected devices was also implemented.

2.14. From this point, Commissioning Support Units (CSUs) and other IT delivery partners worked with NHS England and NHS Digital to re-install and patch systems in primary care. 95% of infected practices were re-installed and patched by 17 May, with the remaining 5% completed by Friday 19 May when the incident was "stood down". These numbers included 595 infected practices that needed to have machines rebuilt before they were patched. A large number of practices would have required a physical visit to deploy the patch where remote patch management arrangements were either not in place or not possible in this instance[33].

2.15. During the week and up to 19 May, additional IT engineering support resource was deployed to trusts and CSUs where requested by NHS Digital and through Local Government Association networks, coordinated by NHS England's regional teams. NHS England continued work to address issues in pharmacy and dental practices, and on ensuring the stability of primary care services.

2.16. NHS Digital issued a further CareCERT alert to CareCERT subscribers[34] on 16 May requesting that they patch and fully deploy antivirus software[35]. NHS England requested confirmation on 17 May that all organisations had received this CareCERT alert, that anti-virus updates had been implemented and that rollout had been completed across all organisations.

2.17. Immediate action was taken following the incident to improve recovery and resilience of the NHS. Additionally, the DHSC-led cross system Data Security Leadership Board (DSLB) reviewed the system response to WannaCry at its 8 June meeting and agreed immediate a comprehensive set of actions as part of a single coordinated programme to improve resilience.

[33] Many practices didn't commence patching until Monday 16 May. Source: NHS England EPRR.

[34] Not the NHS, only NHS organisations which subscribe to the CareCERT bulletins.

[35] NHS Digital had previously issued a CareCERT alert on 16 March 2017 and on 25 April 2017 as an 'all hands broadcast' following notification by BT Advanced Threat Intelligence of a specific threat. NHS Digital also issued a High Severity CareCERT alert on 12 May and guidance online, and sentvia CareCERT, on 14 May.

CASE STUDY 1: Extraordinary efforts were taken across Yorkshire and Humber in dealing with the WannaCry cyber-attack:

- On Friday afternoon, via a number of communication channels, local management contacted all staff in Yorkshire and Humber and instructed to power down all devices.
- Throughout Friday afternoon and over the following weekend the IT teams worked with staff, NHS England, IT security, anti-virus and infrastructure suppliers to address all vulnerabilities that the virus had exploited – this included but was not limited to replacing or rebuilding infected devices, as well as an estate wide patch and anti-virus refresh.
- Operational teams were in post early on Monday morning to manage what we expected to be an exceptionally high level of demand from concerned end users.
- Throughout the week, the major incident Team has remained in post, systematically working around the estate to resolve any further issues identified.
- Across the entire Yorkshire and Humber estate, 5% of all GP surgeries were impacted.
- 250 infected end user devices have been replaced or rebuilt.

Impact on patient care

2.18. The attack led to disruption in one third of hospital trusts in England[36]. NHS England data shows that at least[37] 80 out of 236 trusts were affected – with 34 infected and locked out of devices (of which 27 were acute trusts), and 46 not infected but reporting disruption. A further 603 primary care and other NHS organisations[38] were infected by WannaCry, including 8% of GP practices[39] (595 out of 7,454). During the incident, devices in an additional 21 NHS organisations made calls to the WannaCry 'kill switch'. Whilst this may indicate the presence of infected devices within those organisations, it may also have been the result of routine cyber security maintenance activities.

2.19. As part of its incident response the NHS enacted its "mutual aid" processes in some parts of the country. This meant that where one A&E could no longer take patients, nearby A&Es stepped up to take their demand. During the incident, some patients from five hospitals travelled further for emergency treatment than normal[40].

2.20. 1.2 % (6,912) first appointments were cancelled and re-arranged between 12 and 18 May. NHS England's EPRR review identified at least 139 patients who had an urgent

[36] National Audit Office Investigation: WannaCry cyber attack and the NHS (October 2017)
[37] Numbers are based on organisations self-reporting problems to national bodies and NHS England / NHS Digital analysis of internet activity and may be higher if some organisations did not report problems experienced in a timely or accurate way: National Audit Office Investigation: WannaCry cyber attack and the NHS.
[38] "Other organisations" include CCGs, Commissioning Support Units, an NHS 111 provider, and non-NHS bodies that provide NHS care such as a hospice, social enterprise and community interest companies.
[39] Ibid
[40] Barts Health NHS Trust (Royal London Hospital); Mid Essex Hospital Services NHS Trust (Broomfield Hospital); East and North Hertfordshire NHS Trust (Lister Hospital); Hampshire Hospitals NHS Foundation Trust (Basingstoke Hospital); and North Cumbria University Hospitals NHS Trust (West Cumberland Hospital).

appointment for potential cancer cancelled between 12 and 18 May[41], representing approximately 0.4% of urgent cancer referrals

2.21. The disruption to secondary care had a knock on effect for primary care, for example on access to test results. Third party systems were also impacted, for example DocMan[42], impacting the electronic flow of clinical information from secondary care to primary care services.

2.22. During and after the attack, evening and weekend clinics in GP practices were impacted due to the lack of availability of electronic patient records and clinical systems[43]. NHS England did not collect data during the incident on how many GP appointments were cancelled or how many ambulances and patients were diverted from the accident and emergency departments that were unable to treat patients[44]. Current systems do not allow for the collection of standardised appointment data across GPs but work is underway to address this.

Impact on social care

2.23. Based on a 100% return from local authorities to COBR in the aftermath of WannaCry, no local authorities reported having been infected[45]. However, a number of local authorities switched off their link to the NHS N3 network as a precaution against infection and, in some cases, quarantined emails being sent from nhs.net. This meant that business continuity arrangements needed to be implemented.

2.24. There is no evidence to confirm whether, and how many, social care providers were infected. There is, however, anecdotal evidence that both councils and care providers may have been affected by delays in NHS care with business continuity arrangements needing to be put in place between health and care organisations in some local areas. A comprehensive assessment of all social care providers is needed to identify key cyber vulnerabilities for targeted action[46].

NHS equipment

2.25. 1,220 (1%) pieces of diagnostic equipment across the NHS were affected by WannaCry. This figure does not include diagnostic devices which were disconnected to prevent further infection. As a result, there were, for example, delays in test processing and communication of diagnostic results. There is no figure available for affected equipment in general practices as this data is not centrally collected.

Financial impact

2.26. No NHS organisations paid the ransom, as standing advice not to do so was re-circulated by the NCSC during the incident and repeated by NHS Digital[47].

---

[41] This number may be higher if trusts identified cancellations after 18 May when the major incident was stood down.
[42] In situations where local file servers, for which certain versions of DocMan is reliant, were affected
[43] Feedback from GP IT Committee with RCGP and BMA representatives
[44] Ibid
[45] Based on LA responses to Cobra in the aftermath of WannaCry, LAs were asked to rate Y/N if infected. No LAs reported infection but some LAs reported taking precaution i.e. switching off their access to the N3 network.
[46] National Audit Office Investigation: WannaCry cyber attack and the NHS
[47] Ibid

3. What we have done since WannaCry

3.1. Whilst this report sets out a set of recommendations to strengthen the resilience and ability of local organisations to respond to the cyber threat, since the WannaCry attack in May, significant progress has been made across the system in improving preparedness and our ability to respond, as set out below.

3.2. In parallel with the actions set out from the 8 June DSLB (listed in section 3.3), a number of additional activities have been taken to strengthen the resilience and response of the health and care system as set out below.

- Following the WannaCry attack, a "Cyber Handbook" has been produced to describe the approach and actions to be taken by NHS England, NHS Digital and NHS Improvement in the event of a cyber attack affecting the NHS.
- The principles of the "Cyber Handbook" state that when a major incident is called, DHSC will be the lead with NHS England responsible for coordinating the system response through the national EPRR team and that the EPRR protocol will be followed. This route will be followed for formal communication to local CCGs and providers and supportive information may be sent by NHS Digital and NHS Improvement. The "Cyber Handbook" does not detail local cyber response activities in any depth and should be tested alongside local and scaled approaches to cyber response including testing the mechanisms for communication between the wider system and local CIOs.
- To date, 190 independent on-site cyber assessments of NHS Trusts have been undertaken. Whilst the wider cyber security programme is looking at addressing some of the shortfalls, these assessments have identified that most NHS trusts also need capital investment in areas such as addressing weaknesses in their infrastructure to secure networks by upgrading firewalls, improving network resilience and segmentation to minimise the risk to medical, improving device security through device replacement and automation of patch management, and improving anti-virus protection.
- Immediately following the WannaCry attack, the Digital Delivery Board (the governing board for the Personalised Health and Care 2020 programme) reprioritised £21m capital to address key vulnerabilities in Major Trauma Centres and Ambulance Trusts. This funding has been released on the basis of an independent assessment of target organisations' cyber preparedness, and a bid from sites setting out their key priorities reviewed and approved by NHS Digital, with 32 organisations receiving funding.
- In addition, 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.
- In parallel, 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, including ensuring that these are operating on supported versions of software.

- The CareCert suite of services has been further developed by NHS Digital to provide local support and national oversight around cyber resilience and incidents. To ensure a proactive approach to cyber resilience, NHS Digital has launched CareCERT Collect, an online self-service platform for local organisations to register technical compliance and technical information to assist mitigation activities. The 2017/18 Data Security and Protection Requirements published in October 2017 sets out the responsibility for organisations to confirm, via CareCERT Collect, within 48 hours that plans are in place to act on High Severity CareCERT advisories. NHS Digital will regularly monitor and evaluate the effectiveness of the CareCERT service reporting findings into the CIO for health and social care.
- NHS England, NHS Improvement and NHS Digital have been working with providers of care since WannaCry to achieve sign up to the CareCERT Collect portal and to ensure that plans are in place to apply critical and high impact CareCERT advisories.
- NHS Digital has produced and is testing the alpha version of the redesigned Information Governance Toolkit, as recommended by last year's CQC and NDG data security reviews, centred on assuring local implementation of the NDG's data security standards, which are at the heart of the overall data and cyber security programme.
- Procurement has been initiated by NHS Digital for investment in a new Security Operations Centre (SOC). This will enhance the existing data security services provided by CareCERT and the Data Security Centre.
- As a result of learning from WannaCry, the NHS Digital Data Security helpline has now been made available 24/7. A full service operates 9:00 to 17:00 with a national service desk handling out of hours calls, supported by an expert data security on call team.
- Local NHS and care organisations have commissioned additional external support to audit systems and processes locally in response to the WannaCry. NHS Digital have also continued to provide on-site data security assessments to NHS organisations since WannaCry.
- NHS Digital currently publishes a set of technical "Good Practice Guides" on its website. These guidelines are high level and require further development. NHS Digital is working with local organisations and relevant expert networks to further develop these guides to ensure that they provide the necessary information to local organisations. The use of the "Good Practice Guides" should be regularly monitored and evaluated, reporting the findings to the office of the CIO for health and social care.

3.3. At the DHSC-led DSLB meeting held on 8 June 2017, a number of immediate next steps were agreed, which were grouped into the areas of incident response, resilience, leadership and medium term actions. These next steps are set out below along with the current status of the action.

Incident response

- Create and disseminate national, regional and local incident handling plans – NHS England *(complete)*.
- Update DHSC incident handling plan to include all Arm's Length Bodies, the NCSC and the Local Government Association – DHSC *(complete)*.
- Agree media plan, agreed in advance, including plans for advance briefings with i.e. BBC on handling in the event of another cyber incident – DHSC with NHS England, NHS Digital and NHS Improvement *(in progress).*
- Ensure that provider digitisation programme supports cyber security – NHS England with NHS Digital *(in progress)*.
- Build on existing GP IT work with CCGs and CSUs, and work with GP Systems of Choice (GPSoC) principle suppliers to make GP systems more secure *(in progress)*.
- Dialogue involving local organisations / NHS Digital to explore central framework vs. identifying suitable NCSC accredited suppliers local organisations can contract with ability to increase scope of call-off contracts to remedy major incidents – NHS England and NHS Improvement *(in progress)*.
- Involve providers on what will be required to implement the data security standards – NHS Improvement and NHS England *(in progress)*.
- Target interventions to protect priority patient care pathways that are reliant on technology (e.g. diagnostics, major trauma) – NHS England with input from NHS Digital, Public Health England, NHS Blood and Transplant and MHRA *(in progress, subject to identification of additional investment for cyber)*.
- Plan to remove or isolate unsupported software in the NHS – including XP (by April 18) and Windows 7 (Jan 2020) – DHSC, with input from CIO for health and social care and NHS Digital *(in progress)*.
- Deliver text alerts to NHS CEOs and CIOs when email is unavailable – NHS Digital with input from NHS England and NHS Improvement *(in place)*.
- Target immediate capital support for strategically important trusts with risky infrastructure – CIO with input from NHS Digital *(complete, with £21m prioritised)*.
- Review funding and prioritisation within Personalised Health and Care 2020 to support data security – DHSC, NHS Digital and NHS England, via Digital Delivery Board *(in progress)*.

Resilience

- Provide assurance that critical CareCERT alerts have been acted on, via new CareCERT Collect Portal – NHS Digital, with NHS Improvement and NHS England following up exceptions, from summer 2017 *(complete)*.
- Provide CareCERT Assure on site assessments for all trusts, prioritising those affected by ransomware incident – NHS Digital *(in progress)*.
- Ensure that all CareCERT alerts are being distributed to all Local Authorities

- Boost capacity within NHS Digital to support cyber assessments – NHS Digital *(in progress)*.
- Issue NHS Standard Contract guidance on the NDG standards and implementation in 2017/18 (in future years, this will be the same as the "statement of requirements", setting out the measures/metrics, facilitated by the redesigned IG toolkit) – NHS England, summer 2017 *(complete)*.
- Ensure effective processes agreed for audit against the data security standards ("statement of requirements" via new metrics) – NHS England and NHS Improvement, with DHSC, NHS Digital and Care Quality Commission, from summer 2017 *(complete)*.
- Work between NHS England, NHS Improvement and NHS Digital around confirming cyber readiness across provider and commissioning organisations *(ongoing)*.

Leadership

- Publish Government response to the NDG Review and associated data security standards – DHSC *(complete)*.
- Communicate the importance of cyber security to trust leaders and Boards – NHS Improvement to trusts and NHS England to CCGs *(ongoing)*.
- Set out annual statement of requirements, for Boards to respond with a letter of assurance, as the same measures and metrics underpinning the NHS Standard Contract, facilitated by the redesigned IG toolkit – NHS Improvement with NHS Digital and NHS England *(complete)*.
- Set expectation for every NHS Board to have an Executive Director as data security lead – NHS Improvement to trusts and NHS England to CCGs *(ongoing)*.
- Delivery of cyber security awareness for NHS leaders/board level leadership teams (NCSC accredited) – Health Education England and NHS Digital *(in progress)*.
- Provide regional support through NHS England regional cyber champions, proactively picking up critical CareCERT alerts, agreeing whether these can also support NHS Improvement – NHS England and NHS Improvement *(in place)*.
- Use Global Digital Exemplars to show what good cyber preparedness/practice looks like – NHS England and CIO for health and social care *(in progress)*.
- Produce an introduction to cyber security for social care providers – NHS Digital and Care Provider Alliance and supported by Local Government Association and Skills for Care *(complete)*.
- Tailored messaging for GP practices via Royal College of GPs / British Medical Association – NHS England *(in progress)*.
- Tailored messaging for social care providers – DHSC with Care Provider Alliance, Local Government Association and NHS Digital *(in progress)*.

Medium term actions

- Ensure that Care Quality Commission inspections are based on robust assurance – Care Quality Commission with NHS Digital: framework published in June; inspections from September 2017 *(in progress)*.
- Issue replacement for IG toolkit – NHS Digital, April 2018 *(in progress)*.
- Enforce new NIS Directive, which creates a regulatory framework for standards, audit, plus fining – DHSC with NHS Digital, from May 2018 *(in progress)*.
- Consider data security as part of segmentation under the Single Oversight Framework and as part of decision making on special measures, as part of standard NHS Improvement framework – NHS Improvement, from summer 2018 *(in progress)*.

4. Recommendations: Preparedness

4.1. It is not a question of “if” but “when” the next cyber attack occurs. Our challenge is to ensure that the health and care system nationally, regionally and locally is equipped to withstand and respond to cyber attacks in an effective manner which minimises disruption to services and, most importantly, impact on our patients. This section sets out lessons learned and additional recommendations that, together, will strengthen the resilience and preparedness of the health and social care system against future cyber attacks.

National and local accountability for cyber security

4.2. Every part of the health and social care system is accountable for securing itself against a potential cyber attack. The leadership of every organisation are accountable for providing assurance that they have taken the necessary actions to put in place appropriate resilience measures against attacks, and have robust disaster recovery and business continuity processes in place to recover in the event of an attack.

4.3. From a broader system perspective, and to create clarity of accountability, responsibility for cyber security, accountability is vested as follows:

- DHSC Permanent Secretary – business owner and accountable for cyber security across the health and social care system and sets cyber strategy;
- CIO for the health and social care system – on behalf of the health and care system, commissions projects and services required to increase cyber resilience;
- CEO NHS Digital – accountable for securing national digital infrastructure and services, as well as the provision of cyber support to national and local organisations, including providing alerts in relation to new and emerging threats, providing technical expertise, resources, monitoring and management services during an incident.

4.4. The accountabilities of health and care organisations are:

- **Department of Health and Social Care**
  - Lead Government Department and leads the health and care system, including overseeing cyber security resilience and incident responses.
  - Manages the interface between health and social care with the Cabinet Office, other government departments and agencies.
  - During a cyber incident coordinates briefings to Ministers and the National Data Guardian.
  - Coordinates involvement in central government responses to incidents.
  - Contributes to cross Government briefings when responding to a major incident, including when a COBR response is called.
  - Coordinates public communications in agreement with other organisations.

- **National Data Guardian**
  - Provides independent advice on data sharing and security.
  - Must be informed about all cyber security incidents at the same time as Ministers.

- **NHS England**
  - Provides information about cyber security to commissioners.

- Works with CCGs, CSUs, and audit chairs at a leadership level to support board ownership of cyber security and overall response when cyber incidents occur.
- Responsible for helping to embed cyber security standards in the health sector, e.g. through the NHS Standard Contract and through the inclusion of requirements for services it commission, such as IT for GPs.
- Responsible for ensuring CCGs and providers (e.g. trusts) have appropriate emergency preparedness plans in place to respond to an incident or emergency.
- Lead the system response when major incident called. Coordinates the control of an incident through its Emergency Preparedness, Resilience and Response (EPRR) structures where appropriate.
- Communicates to the healthcare system about the practical and clinical steps to be taken in response to an incident when required.
- Does this through digital teams at regional level. These teams coordinate with NHS England's central cyber team and with NHS Digital.

- **NHS Improvement**
  - Communicates information about cyber security to trusts and other healthcare.
  - Works with trusts at a leadership level to support board ownership of cyber security and overall response to cyber incidents.
  - Works with senior healthcare leaders to ensure recommended actions for cyber resilience are implemented, and acts as an escalation point when cyber incidents occur.
  - Attains assurance that follow up actions to increase resilience have been implemented by healthcare providers.
  - Considers data security during its oversight of trusts, through the Single Oversight Framework and as part of its decision making on trusts who are in special measures.
  - Works with NHS England to communicate to the healthcare system during a cyber incident, in particular through the CIO for the health and care system (who works across NHS Improvement and NHS England).

- **Care Quality Commission**
  - Assesses and regulates the safety of patient care.
  - Assesses the adequacy of leadership including in ensuring data security.
  - Takes account of data security in reaching judgements on well led organisations.

- **NHS Digital**
  - Works with local healthcare to understand and advise on their cyber security requirements.
  - Communicates its role in managing cyber security and incidents to other healthcare organisations.
  - Maintains key IT systems used by healthcare organisations, such as N3 and SPINE.
  - Provides advice to the health and social care system about how to protect against, or respond to, a cyber incident.
  - Provides advice and support to health organisations during a cyber incident, through 'CareCERT React'.

- Works to understand and respond to cyber incidents on national systems or on healthcare IT networks.
- Notifies and works with the National Cyber Security Centre to respond to cyber incidents.

- **Clinical Commissioning Groups (CCGs)**
  - CCGs are accountable for the commissioning of services from GP IT Delivery Partners.
  - CCGs will ensure this includes ensuring that GP IT Delivery Partners act upon CareCERT Advisories within required timescales with CCG holding accountability through exception reporting.
  - CCGs will ensure their commissioned GP IT Delivery Partner has allocated equivalent senior level responsibility for data and cyber security within their organisation.
    - Digital systems purchased by the practice or the CCG outside the GP Systems of Choice (GPSoC) framework and which store or process patient identifiable data or which connect to the GP IT managed infrastructure should be reviewed for compliance with the 10 NDG security standards – the responsibility for this rests with the contract holder i.e. the GP or CCG.
    - In addition, each general practice is accountable for ensuring data security incidents and near misses are reported in accordance with national reporting guidance and legal requirements. This including maintaining a business continuity plan.

- **NHS Trusts and Foundation Trusts**
  - Responsible for following standards set by the DHSC and its Arm's Length Bodies, for protecting data the data they hold, according to the Data Protection Act 1998, and for having arrangements in place to respond to an incident or emergency, under the Civil Contingencies Act 2004.

National Data Guardian data security standards

4.5. The data security standards developed by the National Data Guardian (NDG) in July 2016 provide a robust basis for health and social care organisations to reduce their vulnerability to cyber attacks. These security standards are aimed at addressing vulnerabilities so that health and care organisations can improve their ability to defend against basic threats and build upon this capability as part of a longer term improvement strategy. In summary, these standards are focused on ensuring that:

- Staff are equipped through training and standards, to be able to handle personal confidential data confidently. Leaders must take data security seriously and support their staff in reaching these levels of competence.
- Those in leadership positions take responsibility for proactively preventing data security breaches and for responding appropriately to incidents or near misses, by making sure that processes support data security.
- Secure and up-to-date technology is in place through effective lifecycle management of the technology within the organisation.

4.6. The NDG data security standards provide all health and care providers with a framework that is proportionate, enabling smaller providers, including charitable organisations, to achieve compliance. For larger providers and services, a wealth of industry best practice

is available and should be followed where appropriate. For smaller organisations, partnerships with more established providers with mature IT capability are encouraged.

4.7. It is recommended that all NHS organisations develop local action plans to move to compliance with the Cyber Essentials Plus standard by June 2021, as recommended by the NCSC. This should be the minimum bar that all health and social care organisations must meet. These plans are to be provided to the Chief Information Officer for health and care by 30 June 2018.

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 3*0 June *2018. NHS Digital should produce a framework to support organisations, drawing on security assessments undertaken to-date.*

4.8. NHS Digital has been commissioned to deliver on-site data security assessments aligned to Cyber Essentials Plus standards. Funding is in place to 2018/19. NHS providers who have not undertaken an assessment should commission on-site assessments and act on recommendations from the subsequent findings reports and address any shortfalls in compliance. Provision of funding for this service beyond 2018/19 will be assessed in the light of the take-up and impact of these reviews on cyber resilience in the service.

4.9. However, all reviews of the WannaCry attack have noted that the vulnerabilities that were exploited could have been addressed through good IT management control.

4.10. NHS IT environments are complex and, as shown by this incident, integral to the operational running of the NHS. Health and care organisations must invest in appropriate IT infrastructure, tools and resources. As a result, it is recommended that the CIO for health and social care convene an expert panel in the first quarter of 2018/2019 financial year. The panel should include service CIOs, Chief Clinical Information Officers (CCIOs) and NHS Digital to define and consult on a set of IT infrastructure, application and service management guidelines for organisations hosting clinical systems and patient data. The aim should be to define proportionate guidelines that use existing best practice standards including, for example ISO27001, an internationally recognised standard for Information Security, and the IT Infrastructure Library (ITIL) for IT management processes.

Recommendation 2: *In the first quarter of 2018/2019 financial year, the* CIO *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.*

4.11. IT estates need to be run by competent and qualified staff and resourced to an appropriate level. Boards should consider whether these services could be more effectively provided by third party organisations and should regularly assess their organisations' IT management, cyber capability and capacity.

4.12. In the case of GP IT, services should only be commissioned by CCGs from organisations compliant with the following applicable industry standards:

- ISO 27001 for Information Security Management;
- Demonstration of satisfactory compliance as defined in the NHS Information Governance Toolkit (or any successor framework);
- Commissioned GP IT services should work closely with commissioned IG services for GPs to ensure a joined up approach to information security.

Information Governance Toolkit and new Data Protection Security Toolkit

4.13. All providers who deliver services under the NHS Standard Contract are expected to comply with the current Information Governance Version 14.1 Toolkit during the financial year 2017/18.

4.14. The Information Governance Toolkit will be replaced by a new Data Security Protection Toolkit (DSPT) from 2018/19 and will be available from April 2018. Completion of the DSPT will be mandatory for all NHS organisations. For Local Authorities, the new DPST should be completed from April 2018 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.

4.15. The DSPT will help:

- All health and social care organisations audit their own systems and practices against the NDG data security standards.
- Demonstrate compliance against CQC's Key Line of Enquiry (KLOE) under the Governance and Management section of the Well Led inspection area. The KLOE assesses providers ability to operate within a framework that demonstrates robust arrangements around the security, availability, sharing and integrity of confidential data, records and data management standards.
- Organisations understand how the forthcoming General Data Protection Regulations (GDPR) will impact on them from 25 May 2018, which will replace the Data Protection Act 1998. Broadly, GDPR aims to bring together privacy laws across Europe and to give greater protection and rights to individuals. The legislation is currently being considered by Parliament and will not be known in full detail until the proposed legislation receives the royal assent.

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* CIO *for health and social care details of their position against the DSPT. This will help audit compliance against the NDG's 10 security standards and CQC's well-led* 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.*

Cyber resilience of social care

4.16. To address the current lack of insight on the cyber resilience of all types of social care providers, research should be prioritised to provide a comprehensive assessment of social care providers to identify key cyber vulnerabilities for targeted action. This should be based on an understanding of how data flows across social care and the interaction with other organisations, such as local government, and highlight risks. This research will be used to identify where additional support to the sector can be most effective.

Recommendation 4: *Research will be commissioned by the* CIO *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.*

Leadership

4.17. The NDG Review made clear the role of board leadership to the success of this agenda. It recommends that a Senior Information Risk Owner (SIRO) be charged, on behalf of their board, to ensure that the 10 information security standards are followed throughout their organisation. This includes, for example, ensuring that CareCERT alerts are actioned, patches are implemented when required and that regular review of firewall configuration and password controls are undertaken.

4.18. Feedback from local organisations to this review has been clear about the importance of such leadership to ensure basic security measures are followed and resources prioritised, whilst minimising impact on clinical services during system downtime for maintenance.

4.19. Over half of local NHS organisations reported they had not patched systems when required due to concerns about the impact of the necessary downtime on clinical services. Balancing the clinical and cyber/technology risk requires a proactive dialogue between clinical and technical staff facilitated by visible leadership of technology and cyber security at board level, and a better understanding of the balance between clinical and technology risk within organisations. It is therefore important that, where operational clinical risk needs to be balanced against data security risk, that a board-level executive director, in partnership with the organisation's medical director, CIO and CCIO, has the authority to mandate the regular maintenance of critical systems and equipment.

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.*

4.20. When commissioning new IT systems, and as part of change control to existing systems, local organisations must factor in and budget for adequate controls and resources to maintain updates and security patches. Business cases should reflect consideration for the impact on cyber security.

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.*

Business continuity and management of third parties

4.21. A key challenge identified during the WannaCry attack was the NHS's reliance on third party suppliers for the management and support of systems and equipment, in particular diagnostic equipment. As a starting point, 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 adequate.

4.22. WannaCry highlighted the need for improved technical and contractual management of diagnostic equipment. 1% of diagnostic devices were impacted by the WannaCry attack, with many local organisations reporting slow and inadequate responses from device vendors. During the first quarter of the 2018/19 financial year, a working group will be established by the CIO for health and social care to define standards around the operational management and patching of diagnostic equipment.

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.*

4.23. WannaCry exposed the fundamentally interconnected nature of health and social care provision and the impact of decisions taken on others. Local organisations' business continuity and disaster recovery plans need to include both the necessary detail about their response to cyber incidents and 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) and set 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.

4.24. The business continuity and disaster recovery plans should be regularly tested, reviewed, updated locally and have board level oversight. Testing of business continuity plans should be proportional to the service impact and desk based exercises should be undertaken for key patient facing and support services at least on an annual basis. It is important to note that given services are not delivered in isolation; plans should be considered and tested across a local area between the NHS and its partners and within

organisations. Boards should consider annual internal audit review of business continuity and disaster recovery plans in relation to the increasing and changing cyber threat posed.

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.*

Capability and resources

4.25. It is recommended that NHS Digital appoint a Chief Information and Security Officer (CISO) reporting to the CIO for health and social care, by the end of the first quarter of the 2018/19 financial year. The role will work alongside the DHSC, NHS England, NHS Improvement and NHS Digital to lead on the cyber and security agenda nationally. The role will lead national cyber working groups, help inform policy and drive improvements and standardisation. 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). This cyber security lead will work closely with the national CISO, NHS Digital and local heads of cyber and information security.

4.26. One of the key lessons of attack was the interconnected nature of health and social care organisations in England, whereby the actions taken by one organisation have a direct impact on others. It is therefore recommended that each Sustainability and Transformation Partnership (STP) and Accountable Care System (ACS) area identify a cyber and information security lead from across the organisations in their locality to ensure the coordination of cyber security issues across their STP. This post will work with local boards and leaders to drive professionalism and lead on local recovery and response plans. Post holders must hold a recognised professional cyber/information security certification.

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*)*.

4.27. We recommend that NHS providers join and collaborate with local Warning, Advice and Reporting Point (WARP) groups, where these exist. 'WARPs' are local / sub-regional public sector community forums set up to share trusted, up-to-date advice on information security, cyber threats, incidents and solutions. These bring together public sector organisations within local areas to share intelligence and support coordination.

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.*

4.28. The WannaCry incident highlighted successful, local STP approaches of sharing technical expert resources between providers to improve recovery time and share local knowledge. 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 STP or ACS wide continuity plans in relation to system-wide cyber attacks. Consideration should also be given to the footprints of wider computer networks, where a threat could be interconnected across many local areas. The forthcoming procurements for Health and Social Care Network (HSCN) infrastructure, to replace the N3 network, present a local opportunity to collaborate and ensure that IT is secure by design across a number of partners, including local government and social care providers where these are applicable.

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 STP or ACS wide continuity plans in relation to system wide cyber-attacks.*

4.29. As well as local collaborations, we recommend and support the development of professional community network models for cyber and information security across the health and social care system, working in conjunction with organisations such as NHS Digital, The British Computer Society, Health Education England and the NHS Digital Academy.

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.*

Training and development

4.30. At the heart of cyber security are people. Consequently, this review recognises the importance of training and development as a countermeasure against the cyber threat.

4.31. The boards of health and social care organisations set the standard for wider organisation culture. In addition to having an executive fulfil the role of the SIRO, it is recommended that boards undertake annual board cyber awareness training. Through our national cyber expert working groups, we will define standards and expectations for board training during 2018. This is in addition to the mandatory and statutory information governance (IG) training that individual board members will be required to complete.

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 CIO 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.*

4.32. In addition, organisations should ensure that their staff receive regular and targeted IG 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.

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.*

4.33. The NHS Digital Academy has been commissioned by NHS England to develop current and future health care digital leaders and drive professionalism. The Academy will provide a yearlong world class digital health training course to CIOs, CCIOs and aspiring digital leaders from clinical and non-clinical, backgrounds. Cyber and information security will be a key and critical component of the curriculum. This will ensure that

digital leaders within health and social care can provide leadership across their organisations and local communities.

Role of NHS Digital in supporting the service before incident

4.34. There is a specific need for all parts of the health and care system to understand the role and criticality of NHS Digital's CareCERT service in assessing and communicating the cyber threat environment and to act on intelligence provided. To achieve this, NHS Digital must more proactively publish guidance to the service, and local organisations must more actively seek advice.

4.35. NHS Digital has a critical role in providing national cyber security services. Their security operations centre will provide enhanced monitoring of national services across health and care and will also enable NHS Digital to offer specific advice and guidance to local NHS organisations, including:

- A monitoring service and sharing of guidance, advice, threat intelligence and remediation to relevant contacts across health and care organisations;
- Specialist support for NHS organisations affected by a cyber security incident;
- Ongoing monitoring of NHS Digital national systems and services.

4.36. NHS Digital needs to maintain a clear and consistent view of the technology landscape across the service. This should include data on areas such as the status of patching across national and local organisations, the scale of obsolete technology and the ability to monitor network traffic passing across national infrastructure. In addition, in exceptional circumstances and in consultation with local and national leadership, NHS Digital should have the ability to isolate organisations, parts of the country or particular services (such as term off external communications) in order to contain the spread of a virus during an incident.

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.*

5. Recommendations: Response

5.1. During the incident, national bodies worked together to coordinate advice and support to NHS organisations in restoring services and addressing vulnerabilities to the malware attack. NHS England instituted their major incident protocol and coordinated the response through the same team that would deal with any other national major incident. This created a robust framework through which to manage the incident, although there are a number of lessons that have been learned that need to be brought to bear in the event of a future cyber attack.

Incident management

5.2. Managing the incident through the formal EPRR model was success. As the owners of the statutory EPRR process, NHS England now needs to take a number of actions to update its standard operating procedure for NHS England's national and regional incident coordination centres. Working with colleagues across DHSC, NHS Digital and NHS Improvement, these changes have been developed into a "Cyber Handbook" that sets out the roles and responsibilities of national bodies, ensuring the clarity of ownership of each part of the system and the responsibilities of the relevant organisations such as NHS Digital, NHS Improvement, NHS England, the NHS's regions, CCGs, CSUs, etc.

5.3. This Handbook includes ensuring that there is alignment between NHS England and NHS Improvement and to ensure that there is clarity and capacity to manage an incident across the provider sector. NHS Digital needs to enhance its procedures to support regional 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.

Recommendation 16: *It is recommended that NHS Digital enhance its procedures to support regional 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.*

5.4. During the incident, processes had to be created and implemented to address important issues that were at one step removed from hospitals, social care and GP practice IT systems. This included diagnostic equipment, NHS suppliers and logistic firms, high street pharmacies, dentists, care homes and private providers. All of these processes also need to be described for a local cyber attack where the incident is being managed through regional EPRR teams.

Recommendation 17: *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.*

5.5. NHS England needs to develop scenarios to ensure that, with its partners, it can manage a coordinated or multiple attacks whereby, for instance, a terrorist bombing attack was combined with a cyber attack.

Recommendation 18: *It is recommended that NHS England, working with its partners, develop scenarios to ensure that it can manage a coordinated or multiple attack whereby, for instance, a terrorist bombing attack is combined with a cyber attack.*

5.6. In December 2017, a cyber incident rehearsal was held bringing together representatives from DHSC, NHS England, NHS Improvement and NHS Digital to test response protocols. These lessons are being documented and revisions will be made to the EPRR processes and "Cyber Handbook" as necessary.

5.7. It is recommended that an annual national cyber rehearsal is undertaken, and that regional and local organisations similarly undertake regular tests of their EPRR plans in the event of a cyber incident.

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.*

Managing communication during an incident

5.8. Communications during the incident could have been more coordinated. Local lessons learned reports highlight the difficulty of managing communications between local organisations during the incident.

5.9. During the WannaCry incident, secondary care providers tended to turn to NHS Improvement for information and support. In parallel, NHS England were asking for information through standard EPRR reporting mechanisms and NHS Digital were also asking for information from their contacts. The purpose of the incident room during an incident is to ensure that communication channels are clear and well managed.

5.10. This lack of coordination, especially early on in the incident, meant that the reporting burden on local organisations was significantly higher than necessary initially, with providers responding to the same information via multiple requests.

5.11. National organisations must be joined up to ensure clear and consistent communications to local organisations to minimise local reporting burden and support faster local response. This includes the need for regular planned updates to local organisations during incidents to ensure they have the most up-to-date view of the incident status and the latest advice and guidance.

5.12. The NHS relies on email for much of its communication across the service. As a result of the attack, a number of organisations cut their external network links or took down their email, which presented challenges to communication. Some trusts used social media platforms successfully to communicate during the incident as an alternative mode of communication. Local organisations' lessons learned reports favoured agreement in advance of alternative communications mechanisms.

5.13. The availability and testing of alternative communication channels is required to ensure that multiples communication routes are available to support incident response in the eventuality that an attack disrupts email communications. Since the attack, both the National CIO/CCIO Network and NHS Digital have launched alternative communications mechanisms to alert subscribers during an incident.

Data collection during the incident

5.14. NHS England's EPRR review identified the challenge of capturing situation data during a live incident. The particular challenges around WannaCry were partly due to the rapid development of the incident, the frequency and turnaround time requirements for information requests and a lack of quality assurance processes to check the returns. As a result of experience gained from the WannaCry attack, there is now an established set of standard data requests by NHS England that will be implemented in the event of a future attack that should reduce reporting burden.

5.15. This should both reduce the burden of data collection during a live incident, but also improve the quality, accuracy and completeness of data to support the management of the incident.

5.16. NHS England's EPRR team are planning to deploy a standard incident management solution during 2018/19. NHS Digital will need to ensure they have access to and are able to use the system. Paper processes need to exist and be implemented in the event that the incident management system is impacted by a cyber attack.

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 communicate channels in the event of distribution to standard channels.*

Role of NHS Digital in supporting the service during an incident

5.17. NHS Digital had alerted the service to the WannaCry vulnerability prior to the attack via their CareCert service. Had this advice been acted on in a timely manner, the scale and impact of the attack could have been much reduced.

5.18. NHS Digital needs to develop their on-call and major incident operating guidelines to ensure that the right expertise and seniority of decision making is available in the event

of a national incident. In addition, NHS Digital's contact centre needs to be able to be sufficiently resourced during a live incident to address information requests.

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.*

Availability of resource to manage incident

5.19. The traditional nature of major incidents has been that they are either very intense, but are over within a number of hours (such as a major traffic incident or physical terror attack) or they are long lasting but slow moving (such as strike action). Cyber attacks create the potential for a long running, highly intense incident. NHS England needs to ensure that it has the capacity to rotate its incident coordination centre and senior leadership to effectively manage the response.

5.20. The commitment and long hours put in by staff was recognised in all lessons learned reports.

5.21. Within local organisations, during the incident technical, clinical and administrative staff were very stretched in addressing the consequences of the attack. Many of these staff were required to work extended hours, including weekends and a number cancelled annual leave to support recovery. Action is required to ensure that sufficient IT staff are in post to support the IT infrastructure and systems with local organisations, and mechanisms in place to support the pooling of resources in localities in the event of an incident, which should be identified as part of organisations' business continuity and recovery plans.

5.22. Many of the staff[48] involved in the WannaCry incident had not experienced a major cyber incident before, nor had they had any preparatory training for such an event. Organisations noted that the technical security team, directors and associate directors needed training in cyber incident response, and that there should be ongoing user training for all staff to encourage good security behaviours as well as the reporting of suspicious emails and other threats.

Primary care

5.23. For primary care, local business continuity plans are already a core and mandated requirement outlined in the GP IT operating model for both GP IT delivery providers commissioned by CCGs, either from CSUs other IT delivery partners. The quality of these plans must be assured to ensure they are fit for purpose to address a future cyber attack. For primary care, roles and accountabilities are set out in the GP IT operating model[49].

[48] Although knowledge required by different staff groups will be different, local lessons learned reports did not differentiate when referring to staff in general as not having experienced a cyber attack before.

[49] Securing Excellence in GP IT Services, 2016-18 Operating Model, 3rd Edition (NHSE, May 2016) https://www.england.nhs.uk/digitaltechnology/info-revolution/digital-primary-care/gp-it-operating-model-2016-18/

5.24. Although alerting mechanisms between commissioners and providers made it easier for NHS England's EPRR teams to contact IT suppliers for pharmacy, the absence of a consistent approach for contacting GPs out of hours made it more challenging to communicate with primary care, particularly GPs. There were also instances of inappropriate communication with GPs by, for example, asking individual GP practices to update on patching/state of IT when they are not directly responsible for this and the contact should have been via CCGs, with locally commissioned GP IT delivery partners.

5.25. As outlined by the GP IT operating model[50], responsibility for assurance and contractual oversight is devolved to CCGs as the accountable commissioner of GP IT services. Around a third of CCGs currently source GP IT services outside of the Lead Provider Framework (LPF) through third party organisations such as NHS trusts, local health informatics services (HIS) or private sector suppliers for which NHS England has no central contractual oversight or formal communication routes.

5.26. Much of the lessons learned feedback received from GP IT service providers centred on having clear communication streams at both regional and national levels and standard procedures in respect of response and reporting requirements. Additional feedback included:

- A need to update contact details i.e. the mechanism to contact GPs;
- Imperfect national understanding of which IT providers delivered services in which CCG area;
- Formal response mechanisms should be established as responses relied on pre-existing networks and relationships;
- There were different reporting and response requirements across different patches causing extra work, which should be standardised;
- Access to some GP premises was difficult;
- Small third-party suppliers contracted by CCGs were slow to react and respond to instructions and some clinical suppliers were also quite slow in responding.

5.27. The performance of CSUs and the other IT support organisations in ensuring GP systems had been kept up-to-data and were tested and cleaned over the weekend was impressive. However, GP practices that did not use a CSU for IT support were harder to contact and assure.

5.28. CSUs must be cyber accredited[51] and responsible for coordinating a cyber response across primary care and CCGs, either by themselves or through locally contracted third party providers. All parts of the country will be covered by a CSU and all GP practices and CCGs must receive IT support from cyber accredited suppliers. All approved suppliers must comply with a national response protocol to be drawn up by NHS Digital to ensure 24/7 on call care and linkages to CSUs.

5.29. Finally, CSUs need a developed and tested emergency response capability that dovetails with NHS England's EPRR procedures.

[50] https://www.england.nhs.uk/gp/gpfv/infrastructure/gp-it-operating-model/

51 Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM).

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.*

Appendix 1

CIO Review Steering Group Membership

William Smart

Chief Information Officer for Health and Social Care

George Lucas

Business Manager for Will Smart, Chief Information Officer for Health and Social Care

Paul Fleming

Regional Head Digital Technology (Midlands & East)

NHS England

Anthony Brown

Senior Project Manager for Cyber Response Report

NHS England

Samantha Pryke

Cyber Security Policy Lead

Department of Health and Social Care

Indi Singh

Head of Architecture and Cyber Security

NHS England

Dan Taylor

Head of the Data Security Centre

NHS Digital

Mark Golledge

Programme Manager – Health and Care Digital Lead

Local Government Association

Masood Nazir
National Clinical Lead – Primary Care Digital Transformation
NHS England

Dan Harte
Cyber Security Consultant
National Cyber Security Centre

John Noble
Director of Incident Management
National Cyber Security Centre

Joe McDonald
Chair, Chief Clinical Information Officers Network
Chief Clinical Information Officer
Northumberland Tyne & Wear NHS Foundation Trust

Steven Dobson
Chief Digital Officer
Greater Manchester Health and Social Care Partnership

Steven Chilton
Chief Information Officer
Heart of England NHS Foundation Trust

Appendix 2

Terms of Reference for the Review

Introduction

These are the terms of reference for a Lessons Learned review, commissioned by the Department of Health and Social Care Data Security Leadership Board, following the WannaCry cyber attack on 12 May 2017. They take account of the NCSC and NHSE reviews which are also running in parallel, in addition to the CQC and NDG reviews published in July 2016, and the existing cross-system cyber security programme.

Purpose

The purpose of this review is to:

- Undertake an analysis of the key lessons learned from the WannaCry cyber attack on 12 May 2017;
- Provide an assessment of what actions are required to mitigate the risk and impact of a future cyber attack on the NHS and social care, looking in particular at infrastructure, incident response, and resilience; and
- Ensure that this learning is widely shared across all parts of the healthcare system.

Scope and objectives

The scope of this review includes:

- The existence, availability and content of policy, advice and guidance on cyber security to NHS and social care organisations nationally, regionally and locally;
- The adherence of organisations to this guidance, including the assurance that was available as to the state of preparedness across the system;
- The advice and support available, as well as actions taken by key actors, during the attack and as part of service restoration;
- The readiness of the system in the event of a future attack, including organisational culture, leadership, capability and capacity to address this agenda;
- Clinical engagement in the planning for, and management of, cyber attacks;
- Critical vulnerabilities, including an assessment of the impact of aged infrastructure (e.g. Windows XP) on the scale and impact of the attack on services, including the time to recovery; and
- The existing funding allocated to hospital digitisation, cyber security and improving technology.

Appendix 3

Timeline of Data and Cyber Security measures before WannaCry

2010: NHS offered free upgrade from Windows XP as NHS Microsoft Enterprise Agreement ended in May 2010.

2014: SofS established National Data Guardian (NDG) role.

2014: Support for Windows XP ended. Government funded an additional year of support for public services to move away from Windows XP.

October 2015: CareCERT established – 1 of only 2 sector-specific national cyber support services in country. Comprehensive suite of broadcasting alerts, best practice, incident response & on site assessments/support.

September 2015: SofS commissioned Dame Fiona Caldicott's NDG & CQC Reviews. Announced via speech at NHSE Expo on 2 September

25 November 2015: Spending Review - £4.2bn for technology – an increase of £900m revenue & £1.3bn capital for technology transformation projects. Central IT spend protected & over £50m available for CareCERT (£15m revenue/£36m capital).

December 2015: 15-18% of systems on Windows XP (currently down to 4.7%).

1 May 2016: NDG & CQC wrote to NHS trusts outlining key data security steps to take before new standards published.

11 May 2016: NDG & CQC wrote to service providers highlighting the need for them to act to mitigate cyber risks.

6 July 2016: NDG & CQC wrote to SofS outlining recommendations of NDG and CQC Reviews & published on same day.

6 July 2016: DH & NHSD NEDs wrote to DH ALBs emphasising local leaders' responsibility for data and cyber security and highlighting proposed NDG security standards.

7 September 2016: Wachter review published – outlined recommendations to inform health and care system's approach to IT implementation and endorsed NDG Review's recommendations.

27 October 2016: DH & ALBs NEDs attended training on importance of leadership in organisations' strong cyber resilience.

November 2016: Chancellor launched UK's new National Cyber Security Strategy & provided nearly £2bn public funding for transformational investment over next 5 years.

November 2016: NHS Standard Contract 2017/18 published including new requirements on implementing Caldicott recommendations.

14 February 2017: Queen opened National Cyber Security Council to provide cyber security nationally.

1 April 2017: Caldicott recommendations included in NHS Standard Contract 2017/18

Appendix 4

Glossary

ACS – Accountable Care System

CareCERT – suite of services and support provided by NHS Digital to health and care system

CCG(s) - Clinical Commissioning Group(s)

CCIO(s) – Chief Clinical Information Officer(s)

CIO(s) – Chief Information Officer(s)

CISO – Chief Information and Security Officer

CT – Computed Tomography

CSU(s) – Commissioning Support Unit(s)

DHSC – Department of Health and Social Care

DSLB – Data & Cyber Security Leadership Board

DSPT – Data security Protection Toolkit

EPRR – NHS England Emergency Preparedness, Resilience and Response

GDS - Government Data Service

GDPR – General Data Protection Regulations

GP – General Practioner

GP IT - General Practice IT

HSCN – Health and Social Care Network

HIS – Health Informatics Services

IGSOC –information governance statement of compliance

ISO - Information Security Officer

ITIL – IT Infrastructure Library

IT – Information technology

KLOE – Key Line of Enquiry

MRI – Magnetic Resonance Imaging

N3 – Secure national broadband service built and managed by British Telecoms for NHS

NCSC – National Cyber Security Centre

NDG – National Data Guardian

PCs – Personal computers

PSN CoCo – Public Services Network Code of Connection

SIRO – Senior Information Risk Officer

SMB – Server Message Block

SOC – Security Operations Centre

STP – Sustainability and Transformation Partnership

WARP – Warning, Advice & Reporting Point