House of Commons

Committee of Public Accounts

Cyber-attack on the NHS

Thirty-Second Report of Session 2017–19

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 28 March 2018

HC 787
Published on 18 April 2018
by authority of the House of Commons

The Committee of Public Accounts

The Committee of Public Accounts is appointed by the House of Commons to examine "the accounts showing the appropriation of the sums granted by Parliament to meet the public expenditure, and of such other accounts laid before Parliament as the committee may think fit" (Standing Order No. 148).

Current membership

Meg Hillier MP (*Labour (Co-op), Hackney South and Shoreditch*) (Chair)

Bim Afolami MP (*Conservative, Hitchin and Harpenden*)

Sir Geoffrey Clifton-Brown MP (*Conservative, The Cotswolds*)

Martyn Day MP (*Scottish National Party, Linlithgow and East Falkirk*)

Chris Evans MP (*Labour (Co-op), Islwyn*)

Caroline Flint MP (*Labour, Don Valley*)

Luke Graham MP (*Conservative, Ochil and South Perthshire*)

Robert Jenrick MP (*Conservative, Newark*)

Gillian Keegan MP (*Conservative, Chichester*)

Shabana Mahmood MP (*Labour, Birmingham, Ladywood*)

Layla Moran MP (*Liberal Democrat, Oxford West and Abingdon*)

Stephen Morgan MP (*Labour, Portsmouth South*)

Anne Marie Morris MP (*Conservative, Newton Abbot*)

Bridget Phillipson MP (*Labour, Houghton and Sunderland South*)

Lee Rowley MP (*Conservative, North East Derbyshire*)

Gareth Snell MP (*Labour (Co-op), Stoke-on-Trent Central*)

Powers

Powers of the Committee of Public Accounts are set out in House of Commons Standing Orders, principally in SO No. 148. These are available on the Internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Richard Cooke (Clerk), Dominic Stockbridge (Second Clerk), Hannah Wentworth (Chair Support), Ruby Radley (Senior Committee Assistant), Carolyn Bowes and Kutumya Kibedi (Committee Assistants), and Tim Bowden (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Committee of Public Accounts, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 6593; the Committee's email address is pubaccom@parliament.uk.

Contents

Summary

The WannaCry cyber-attack on Friday 12 May 2017 was a wake-up call for the NHS. The attack caused widespread disruption to health services, with more than a third of NHS trusts affected. The NHS had to cancel almost 20,000 hospital appointments and operations, and patients were diverted from the five accident and emergency departments that were unable to treat them. Yet the NHS was lucky. If the attack had not happened on a Friday afternoon in the summer and the kill switch to stop the virus spreading had not been found relatively quickly, then the disruption could have been much worse. The Department of Health and Social Care (the Department) and its arm's-length bodies were unprepared for the relatively unsophisticated WannaCry attack; they had not shared and tested plans for responding to a cyber-attack, nor had any trust passed a cyber-security inspection. As the attack unfolded, people across the NHS did not know how best to communicate with the Department or other NHS organisations and had to resort to using improvised and haphazard ways to communicate. The Department still does not know what financial impact the WannaCry cyber-attack had on the NHS, which is hindering its ability to target its investment in cyber security. Although the Department and NHS bodies have learned lessons from WannaCry, they have a lot of work to do to improve cyber-security for when, and not if, there is another attack. The recent shocking use of a nerve agent to poison those on British soil has heightened concerns about the UK's ability to respond to international threats, and hammers home the risks from those hostile to the UK. A cyber-attack is a weapon which can have a huge impact on safety and security. It needs to be treated as a serious, critical threat. The rest of government could also learn important lessons from WannaCry.

Introduction

On Friday 12 May 2017 a global ransomware attack, known as WannaCry, affected more than 200,000 computers in at least 100 countries. Those affected by the cyber-attack faced a ransom demand to unlock their devices. In the UK, the NHS was particularly affected with about 80 of 236 NHS trusts across England suffering disruption, because they were either infected by the ransomware or had turned off their devices or systems as a precaution. WannaCry also infected another 603 NHS organisations including 595 GP practices. The NHS had to cancel almost 20,000 hospital appointments and operations, and five accident and emergency departments unable to treat some patients had to divert them to other hospitals. At 4pm on 12 May, NHS England declared the cyber-attack a major incident and implemented its emergency arrangements to maintain health and patient care. On the evening of 12 May a cyber-security researcher activated a kill-switch so that WannaCry stopped locking devices.

Conclusions and recommendations

1. **The NHS was not prepared for WannaCry and there is a long way to go before agreed, prioritised and costed plans for improving cyber security are in place across the NHS.** As far back as April 2014 the Department had written to NHS trusts warning them to migrate from old software such as Windows XP. Yet at the time of WannaCry, 5% of the NHS IT estate was still using Windows XP. There were further warnings in 2016 and, even in March and April 2017, just before the attack, NHS Digital had issued warnings to trusts to secure their Windows operating systems. Yet at the time of WannaCry, patching had only taken place in around two-thirds of trusts and none of 88 trusts had passed NHS Digital's assessments of their cyber security arrangements. Following WannaCry, the Department and the NHS recognised that things needed to change. In February 2018, the Department, NHS England and NHS Improvement published a Lessons Learned review with 22 recommendations for strengthening the NHS's cyber security. However, implementation plans have yet to be agreed, and the Department does not know exactly how much the recommendations will cost or when they will be implemented. Some NHS organisations still have a lot to do to improve their cyber security including Barts Health NHS Trust, one of the largest NHS trusts affected by WannaCry.

   Recommendation: ***The Department and its national bodies should urgently consider and agree implementation plans arising from the recommendations within their Lessons Learned document, prioritising and costing actions, setting a clear timetable, and ensuring national and local roles, responsibilities and oversight arrangements are clear. They should provide an update on progress to the Committee by the end of June 2018.***

2. **Communications during the cyber-attack were not co-ordinated and there were no alternative communication methods when email was switched off.** Local NHS organisations reported the WannaCry attack to different national bodies within and outside the health sector, including to their local police forces, as they did not know where responsibilities lay and who they should contact during a cyber-attack. Communication was also hindered during the cyber-attack as trusts were unable to access email, either because they were infected or because they had closed down their systems as a precaution. As local NHS organisations did not know how to communicate with the Department or other NHS organisations they resorted to using WhatsApp or personal mobile phones to communicate with each other. Although NHS England's emergency team were able to communicate with each other during the attack, the Department now accepts that it needed a wider network of contacts to manage the cyber-attack. Since the attack, a cyber handbook has been produced to describe the approach and actions to be taken by NHS organisations in the event of a cyber-attack.

   Recommendation: ***The Department and national bodies should set out clear roles and responsibilities for national and local NHS organisation so that communications are co-ordinated during a cyber-attack. They should also work together to identify and develop secure alternative communication channels when email, for example, is unavailable.***

3. **The Department and its national bodies know more about NHS preparedness for a cyber-attack now, but still have much more to do to support trusts to meet required cyber security standards and to respond to a cyber-attack.** Before 12 May 2017, the Department and its national bodies did not know whether every NHS organisation was prepared for a cyber-attack and relied too much on local organisations' own assessments of their preparedness. NHS England assures us that since WannaCry it now has better visibility of trusts' preparedness and which trusts it needs to be most worried about. At the time of our evidence session NHS Digital had completed on-site assessments to test cyber security and identify vulnerabilities at 200 trusts, although all trusts had failed the assessment. We are told that this was because a high bar had been set for NHS providers to meet the required standard, but some of the trusts had failed the assessment purely because they had still not patched their systems—the main reason the NHS had been vulnerable to WannaCry. There is also the risk that those organisations not infected by WannaCry, a relatively unsophisticated attack, become complacent and do not keep on top of their cyber security risks. The Department and its arm's-length bodies still have limited central information on trusts' IT and digital assets such as anti-virus software and IP addresses which would help them to target their support during a cyber-attack.

   Recommendation: ***The Department and its arm's length bodies should support local organisations to improve cyber security and be ready for a cyber-attack by developing a full understanding of the cyber security arrangements and IT estate of all local NHS organisations.***

4. **Without an understanding of the costs of WannaCry national and local organisations cannot target investment in cyber security.** Neither the Department nor its arm's-length bodies, have estimated the financial impact of the WannaCry attack on the NHS. Their focus at the time of the attack was on collecting data to ensure patient safety and continuity of care rather than assessing financial impact. However, financial data is likely to be available locally and NHS national bodies collected some information on cancelled appointments and operations. The Department agreed to look again at what it could do. Immediately following the WannaCry attack, the Department reprioritised £21 million of capital funding to address key vulnerabilities in Major Trauma Centres and Ambulance Trusts, while a further £25 million of capital funding has been made available in 2017–18 to support organisations most vulnerable to cyber security risks. A better understanding of the costs and impact would help both local and central NHS bodies make the best cyber-security investment decisions.

   Recommendation: ***The Department should provide an update to the Committee by the end of June 2018 with its national estimate of the cost to the NHS of WannaCry and with its national bodies agree with local organisations how to target investment appropriately in line with service and financial risks.***

5. **Not all local bodies have the means to update and protect systems without disrupting the ongoing delivery of patient care.** In the weeks immediately before the attack, NHS Digital had warned trusts to apply a patch that would have prevented WannaCry, but most of the organisations subsequently affected did not do so. Trusts find it difficult to apply patches without disrupting other parts of IT systems or the operation of equipment vital to patient care. There are also difficulties with medical

equipment and systems that can only be updated by external suppliers, where the NHS needs to be proactive in ensuring suppliers are protecting systems properly. But there are ways to mitigate and manage these difficulties if you have the requisite skills. All NHS organisations face a challenge in attracting and retaining the right staff, and even NHS Digital itself has only 18 to 20 suitably skilled cyber security staff.

Recommendation: ***The Department and its arm's-length bodies should:***

- ***set out how local systems can be updated whilst minimising disruption to services, and provide guidance and support to do this;***
- ***ensure that all IT suppliers and suppliers of medical equipment to the NHS are accredited and that local and national contracts include standard terms to maintain and protect NHS devices and systems from cyber-attack; and***
- ***ensure that local and national workforce plans include a focus on IT and cyber skills.***

6. **While the NHS needs to recognise cyber security is essential for patient safety, there are also lessons from WannaCry for the whole of government.** WannaCry could have had a more serious impact on the NHS if it had not happened in the summer, or on a Friday, or if the kill switch not been discovered so soon by a cyber security researcher. While WannaCry was a relatively unsophisticated and financially motivated attack, future attacks could be more sophisticated and malicious in intent, and involve the theft or compromise of patient data. The Department accepts that cyber-attacks are now a fact of life and that the NHS will never be completely safe from them. The whole of government is at risk of a cyber-attack and, while the Department and NHS bodies are learning lessons from WannaCry, the whole of government must also learn lessons from the cyber-attack. The Department and in particular, NHS Digital, worked closely with the National Cyber Security Centre, during and after the WannaCry cyber-attack. In the Department's view government having a single organisation to work with at the centre on cyber-security was helpful.

Recommendation: ***The Department and its national bodies need to make cyber security a priority, and work with wider government, including the Cabinet Office and the National Cyber Security Centre, to share lessons and promote best practice.***

1 NHS readiness for WannaCry and for future cyber-attacks

1. On the basis of a report by the Comptroller and Auditor General, we took evidence from the Department of Health and Social Care (the Department), NHS England, NHS Improvement, and NHS Digital about the WannaCry cyber-attack.[1]

2. On Friday 12 May 2017 the global ransomware attack, known as WannaCry, affected more than 200,000 computers in at least 100 countries. In the UK, the attack particularly affected the NHS, although it was not the specific target. At 4pm on 12 May, NHS England declared the cyber-attack a major incident and implemented its emergency arrangements to maintain health and patient care. On the evening of 12 May a cyber-security researcher activated a kill-switch so that WannaCry stopped locking devices.[2]

3. According to NHS England, the WannaCry ransomware affected some 80 out of the 236 trusts across England, because they were either infected by the ransomware or turned off their devices or systems as a precaution. A further 603 primary care and other NHS organisations were also infected, including 595 GP practices. The attack led to the NHS cancelling almost 20,000 hospital appointments and operations. However, neither the Department nor NHS England know how many GP appointments were cancelled, or how many ambulances and patients were diverted from five accident and emergency departments that were unable to treat some patients.[3]

4. Local organisations such as NHS trusts, NHS foundation trusts, clinical commissioning groups and GP practices are responsible for their own cyber security arrangements, which are overseen and supported by NHS England, NHS Digital, NHS Improvement and the Care Quality Commission. For example: NHS Digital shares alerts about cyber threats, provides a hotline for dealing with incidents, shares best practice and carries out on-site assessments of organisations' cyber security; and NHS England requires trusts to comply with the data security standards set out in the standard NHS contract for 2017–18.[4]

NHS readiness for the WannaCry cyber-attack

5. The Department and the Cabinet Office wrote to NHS trusts in 2014, warning them it was essential they had "robust plans" to migrate away from old software, such as Windows XP, by April 2015.[5] A further warning came from the National Data Guardian and Care Quality Commission (CQC) in July 2016 that cyber-attacks could lead to patient information being lost or compromised and jeopardise access to patient record systems.[6]

1 Report by the Comptroller and Auditor General, Investigation: WannaCry cyber attack and the NHS, Session 2017–19, HC 414, 27 October 2017
2 C&AG's Report, para 1
3 C&AG's Report, para 1, 5–6, Figure 1
4 Qq 7–8, 28; C&AG's Report, para 3, Figure 4
5 C&AG's Report, Summary para 4
6 National Data Guardian for Health and Care, Review of Data Security, Consent and Opt-Outs (June 2016), para 2.1.9; Care Quality Commission, Safe data, safe care (June 2016), pp. 11–12

In March and April 2017, just before the WannaCry attack, NHS Digital had issued critical alerts warning NHS organisations to patch their systems, and NHS Digital told us that patching had taken place in more than two-thirds of trusts when the attack occurred.[7]

6. In response to these warnings, the Department told us that at the time of the WannaCry cyber-attack, a major programme of work was underway to improve cyber security across the NHS for the first time. However, local NHS organisations' responses to the warnings on improving their cyber security since 2014 had been mixed. In 2015, about 18% of NHS systems had used XP; this was down to 4.7% at the time of the WannaCry attack, and according to the Department is now down to 1.8 %.[8] Some NHS organisations still have a lot to do to improve their cyber security including Barts Health NHS Trust, one of the largest NHS trusts affected by WannaCry.[9]

7. The Department and NHS England told us that that they had a lot to learn from the WannaCry attack and that a "whole series of things needed to change".[10] In February 2018, just a few days before our evidence session, the Department, NHS England and NHS Improvement published a Lessons Learned review which included 22 recommendations to strengthen cyber security in the NHS. However, neither the Department nor NHS England could provide us with details on the costs and timescale for implementing the recommendations and did not expect to have a much clearer plan and timetable for a few weeks or months. We asked the Department and NHS England to provide six-monthly updates on progress with the plan to the National Audit Office, which the Department agreed would be completely appropriate.[11]

Communication during the cyber-attack

8. The Department and its arm's-length bodies had developed a plan for responding to a cyber-attack, but it had not been tested with local organisations. NHS England therefore initiated its emergency response plan, although not until three hours after the attack had been declared a major incident, which it agreed was too slow. NHS England also told us that, although it considered that its emergency plan had worked well, cyber-attacks were different to other types of major incidents, and NHS organisations needed more specific guidance. In particular when the WannaCry attack began, local bodies did not know who to contact and what actions they should take. Trusts reported the attack to different organisations within and outside the health sector, including local police services. Similarly, communications from national bodies to local organisations and to the public also came from a number of sources, including NHS England, NHS Digital and the National Cyber Security Centre.[12]

9. Some NHS trusts could not access email because they had been infected by WannaCry or had disconnected from the NHS network as a precautionary measure. Therefore front-line NHS staff used WhatsApp and mobile phones to communicate.[13] The Department told us that NHS England's emergency response team had been able to communicate with each other during the attack, but acknowledged WannaCry showed that a wider network

7 Q 11, C&AG's Report, para 2.5
8 Q 4
9 Qq 54, 56
10 Qq 11, 22, 25
11 Qq 65–66
12 Qq 32–38, 61–62; C&AG's Report, para 3.3, 3.4
13 Qq 35; C&AG's Report, para 3.4–3.5; NHS Providers (WCA0003), para 6–8

of contacts was required to manage a cyber-attack.[14] NHS England told us that, since the WannaCry attack, it had developed an IT-specific response plan (a cyber handbook) for use in the event of another cyber-attack. This plan requires local organisations to contact NHS Digital's data security operation centre if they suspected a cyber-attack was underway.[15] They also told us that NHS Digital and the Chief Information Officers of local organisations have created new communication channels, including a text message service allowing NHS Digital to communicate with key personnel across the NHS, such as Chief Information Officers. There were also now local text message services allowing Chief Information Officers and Chief Clinical Information Officers to communicate with each other.[16]

Local organisations readiness for a future cyber-attack

10. Before 12 May 2017, the Department and its national bodies did not know whether every NHS organisation was prepared for a cyber-attack and relied too much on local organisations' own assessment of their information governance.[17] Since WannaCry, the Department, NHS England and NHS Digital told us that they have improved their understanding of local organisations' readiness for another cyber-attack. For example, NHS Digital has now assessed cyber security at 200 trusts to identify vulnerabilities, compared to the 88 assessed before WannaCry.[18]

11. Although none of the 200 trusts had passed NHS Digital's cyber security assessment, the Department and NHS England and NHS Improvement told us that at least they now know which organisations they are most worried about, and have plans to improve cyber security at a number of organisations. The Department and NHS Digital told us that trusts had not passed the test, not because they had not done anything on cyber security, but rather that the Cyber Essentials Plus standard against which they are assessed is a high bar. However, some trusts had failed the assessment solely because they had not patched their systems—the main reason the NHS had been vulnerable to WannaCry.[19] NHS England told us that it is also concerned that trusts that were not infected by WannaCry could become complacent over cyber security and not keep on top of their cyber security risks.[20]

12. NHS Digital told us it was a priority for it to understand what cyber security arrangements were in place at a local level so it had the information and could provide targeted advice and support during any future cyber-attack.[21] However, NHS Digital still did not have some of the key information it needed to manage any future national attack on the NHS, such as on the use of anti-virus software and IP addresses, and whether the boards of local organisations' include cyber security on their risk registers.[22]

14 Qq 34, 37, 61–62
15 Qq 33, 35–38
16 Qq 35–37; NHS Digital (WCA0004), section 3.3
17 Qq 40, 54, 63; C&AG's Report, para 2.10–2.12
18 Qq 5–6
19 Qq 5–7, 54–56
20 Q 56
21 Qq 50–52
22 Qq 63–64; C&AG's Report, para 2.12

2 The impact of WannaCry and lessons learned

The financial cost of the WannaCry cyber-attack

13. The Department for Health and Social Care (the Department) told us that neither it, nor its arm's-length bodies, had estimated the national financial cost of the WannaCry attack to the NHS. However, they did assure us that no NHS organisations had paid the ransom.[23] National bodies had collected some data from local organisations during the attack such as on cancelled appointments and operations. The data had been collected to help the NHS manage, and recover from, the cyber-attack and not to assess the cost of the attack. The Department felt that a retrospective collection of data to assess the financial impact would be too burdensome on local organisations and the Department and its arm's-length bodies saw little benefit in doing this since the national case for change, and for investment, in cyber security had already been made.[24]

14. We recognise that at the time of the attack the focus would have been on patient care rather than working out what WannaCry was costing the NHS. However, an understanding of the financial impact on the NHS is also important to assess the seriousness of the attack and likely to be relevant to informing future investment decisions in cyber security. We pressed the witnesses on the importance of also understanding the financial cost of the attack and the Department agreed to look again at whether it could provide a global estimate of the financial cost of WannaCry, without an overly burdensome additional data collection from local organisations. The Department and arm's-length bodies added that many NHS staff undertook unpaid overtime to manage the WannaCry attack.[25]

15. The Department is investing more in cyber-security following the WannaCry attack. Between 2015 and 2020, the Department had originally allocated £4.2 billion to IT programmes, including £50 million for cyber security. Immediately following the WannaCry attack, the Department reprioritised £21 million of capital funding to address key vulnerabilities in Major Trauma Centres and Ambulance Trusts, while a further £25 million of capital funding was made available in 2017–18 to support organisations most vulnerable to cyber security risks. The Department told us that at least a further £150 million will be invested in local infrastructure as well as national systems and services to improve monitoring, resilience and response in 2018–19 and 2019–20. This means since WannaCry the Department has allocated an additional £196 million for cyber-security up to 2020. The Department explained that it is difficult to be precise on expenditure on cyber security because expenditure on general upgrades to IT systems often improve cyber security and local organisations also invest in their own cyber security.[26]

23 Qq 2, 17; C&AG's Report, para 1.11–1.12
24 Qq 18–19, 21–26, 50; C&AG's Report, para 1.8
25 Qq 21–26, 50
26 Qq 27–28, 54

Updating and protecting systems without disrupting patient care

16. Most NHS organisations could have prevented WannaCry by applying a patch released by Microsoft for Windows 7 (more than 90% of devices in the NHS use the Windows 7 operating system). NHS Digital had issued CareCERT alerts in March 2017 and April 2017 asking them to apply this patch. Despite this, many organisations did not apply the patch; the majority of organisations infected by WannaCry were using Windows 7 and could therefore have prevented the infection.[27] NHS England and NHS Digital told us that the complexity and size of trusts' IT estates meant they find patching their systems difficult—for example the Royal Free London NHS Foundation Trust, which had more than 10,000 computers and devices. Patching can disrupt the use of medical equipment and present a clinical risk to patients, and applying a patch in one part of an IT system can cause disruption elsewhere in that system.[28] In addition, medical devices provided by external suppliers need to be updated by that supplier, rather than by the trust. Some major IT suppliers cannot just patch one system in isolation, but need to patch across their entire estate, which can take time. The NHS needs to be proactive in ensuring its suppliers are patching, or at least understand where it might be vulnerable and take action accordingly.[29]

17. NHS Digital and NHS England told us that there were a number of potential mitigations for these challenges, based on having layers of cyber security in place to protect organisations rather than just one type of protection.[30] For example, NHS organisations could have prevented WannaCry, even without patching their systems, had they taken action to manage their firewalls.[31] Organisations can also protect themselves by segmenting their networks (so that not all IT devices on the network can connect with all other devices) and, in particular, by isolating medical devices from their networks. NHS Digital told us it has developed guidance for trusts about isolating medical devices from their network. NHS England also told us that the NHS could work more closely with suppliers of medical devices to make sure those devices can be updated when patches are available.[32]

18. A further challenge faced by local NHS organisations in maintaining cyber security is having a sufficiently skilled workforce. NHS organisations, including local organisations, struggle to recruit and retain skilled cyber security staff, as there is a national shortage of this type of expertise and they are competing in a market where there are three jobs for every expert, and private sector organisations can pay more for cyber security experts than the NHS can. NHS Digital itself told us that it has only 18 to 20 "deeply technically skilled people", though it is doing work to develop a future workforce by developing graduate schemes alongside universities. NHS Digital told us that one way it was seeking to address this challenge was by working with the National Cyber Security Centre and Crown Commercial Service to engage trusted suppliers from outside the NHS who can support the NHS during a cyber-attack.[33]

27 Qq 11–12; C&AG's Report, para 2.5
28 Qq 11–12
29 Qq 12–14
30 Q 50
31 Q 11; C&AG's Report, para 2.4
32 Qq 11–14
33 Q 67

Wider lessons for government

19. The WannaCry attack disrupted a third of trusts but could have had an even more serious impact on the NHS if it had not happened in the summer, or on a Friday, or had the kill switch not been discovered so soon by a cyber security researcher.[34] WannaCry was a financially motivated ransomware attack, and as such relatively unsophisticated (it locked devices but did not seek to alter or steal data). However, future attacks could be more sophisticated and malicious in intent, resulting in the theft or compromise of patient data.[35] The Department and its arm's-length bodies accept that cyber-attacks are now a fact of life and that the NHS will never be completely safe from them.[36] They also acknowledge that they need to learn lessons and make changes in response to WannaCry.[37]

20. This Committee's report Protecting information across government recognised cyber-attack as a risk for the whole of government, and the whole of government can take lessons from the WannaCry attack.[38] The Department, and in particular NHS Digital, worked closely with the National Cyber Security Centre, during and after the WannaCry cyber-attack. The Department told us that having a single organisation at the centre of government to work on cyber-security was very helpful.[39]

34 Qq 1, 20, 44; C&AG's Report, para 1, 1.13–1.14;
35 Qq 9, 11, 45; NHS Digital (WCA0004); Martyn Thomas (WCA0001), para 1–6
36 Qq 2, 11
37 Qq 4, 11, 22, 25, 37, 45; 48
38 Committee of Public Accounts, Thirty-eighth Report of Session 2016–17, Protecting information across government, HC 769
39 Q 58

Formal minutes

Wednesday 28 March 2018

Members present:

Meg Hillier, in the Chair

Bim Afolami	Layla Moran
Sir Geoffrey Clifton-Brown	Anne Marie Morris
Chris Evans	Lee Rowley
Gillian Keegan	Gareth Snell
Shabana Mahmood	

Draft Report (*Cyber-attack on the NHS*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 20 read and agreed to.

Introduction agreed to.

Conclusions and recommendations agreed to.

Summary agreed to.

Resolved, That the Report be the Thirty-second of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Wednesday 18 April 2018 at 2.00pm

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Monday 5 February 2018	*Question number*
Simon Stevens, Chief Executive, NHS England, **Sir Chris Wormald**, Permanent Secretary, Department of Health, **Rob Shaw**, Deputy Chief Executive, NHS Digital, **Jim Mackey**, former Chief Executive, NHS Improvement, and **Will Smart**, Chief Information Officer, NHS England and NHS Improvement	Q1–67

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

WCA numbers are generated by the evidence processing system and so may not be complete.

1 Dr Martyn Thomas (WCA0001)

2 NHS Digital (WCA0004)

3 NHS Providers (WCA0003)

4 Professor Harold Thimbleby (WCA0002)

List of Reports from the Committee during the current session

All publications from the Committee are available on the publications page of the Committee's website. The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2017–19

First Report	Tackling online VAT fraud and error	HC 312 (Cm 9549)
Second Report	Brexit and the future of Customs	HC 401 (Cm 9565)
Third Report	Hinkley Point C	HC 393 (Cm 9565)
Fourth Report	Clinical correspondence handling at NHS Shared Business Services	HC 396 (Cm 9575)
Fifth Report	Managing the costs of clinical negligence in hospital trusts	HC 397 (Cm 9575)
Sixth Report	The growing threat of online fraud	HC 399 (Cm 9575)
Seventh Report	Brexit and the UK border	HC 558 (Cm 9575)
Eighth Report	Mental health in prisons	HC 400 (Cm 9575) (Cm 9596)
Ninth Report	Sheffield to Rotherham tram-trains	HC 453 (Cm 9575)
Tenth Report	High Speed 2 Annual Report and Accounts	HC 454 (Cm 9575)
Eleventh Report	Homeless households	HC 462 (Cm 9575)
Twelfth Report	HMRC's Performance in 2016–17	HC 456 (Cm 9596)
Thirteenth Report	NHS continuing healthcare funding	HC 455 (Cm 9596)
Fourteenth Report	Delivering Carrier Strike	HC 394 (Cm 9596)
Fifteenth Report	Offender-monitoring tags	HC 458 (Cm 9596)
Sixteenth Report	Government borrowing and the Whole of Government Accounts	HC 463 (Cm 9596)
Seventeenth Report	Retaining and developing the teaching workforce	HC 460 (Cm 9596)
Eighteenth Report	Exiting the European Union	HC 467 (Cm 9596)

Nineteenth Report	Excess Votes 2016–17	HC 806 (Cm 9596)
Twentieth Report	Update on the Thameslink Programme	HC 466
Twenty-First Report	The Nuclear Decommissioning Authority's Magnox	HC 461
Twenty-Second Report	The monitoring, inspection and funding of Learndirect Ltd.	HC 875
Twenty-Third Report	Alternative Higher Education Providers	HC 736
Twenty-Fourth Report	Care Quality Commission: regulating health and social care	HC 468
Twenty-Fifth Report	The sale of the Green Investment Bank	HC 468
Twenty-Sixth Report	Governance and departmental oversight of the Greater Cambridge Greater Peterborough Local Enterprise Partnership	HC 896
Twenty-Seventh Report	Government contracts for Community Rehabilitation Companies	HC 897
Twenty-Eighth Report	Ministry of Defence: Acquisition and support of defence equipment	HC 724
Twenty-Ninth Report	Sustainability and transformation in the NHS	HC 793
Thirtieth Report	Academy schools' finances	HC 760
Thirty-First Report	The future of the National Lottery	HC 898
First Special Report	Chair of the Public Accounts Committee's Second Annual Report	HC 347