National Audit Office

Report
by the Comptroller
and Auditor General

Department of Health

Investigation: WannaCry cyber attack and the NHS

HC 414 SESSION 2017–2019 27 OCTOBER 2017

What this investigation is about

1 On Friday 12 May 2017 a 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 4 pm 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 According to NHS England, the WannaCry ransomware affected at least 81 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.

3 Before the WannaCry attack the Department of Health (the Department) and its arm's-length bodies had work under way to strengthen cyber-security in the NHS. For example, NHS Digital was broadcasting alerts about cyber threats, providing a hotline for dealing with incidents, sharing best practice and carrying out on-site assessments to help protect against future cyber attacks; and NHS England had embedded the 10 Data Security Standards (recommended by the National Data Guardian) in the standard NHS contract for 2017-18 and was providing training to its Board and local teams to raise awareness of cyber threats. In light of the WannaCry attack, the Department announced further plans to strengthen NHS organisations' cyber-security.

4 Our investigation focuses on events immediately before 12 May 2017 and up until 30 September 2017. We only cover the effect the WannaCry attack had on the NHS in England. We do not cover how the WannaCry attack affected other countries or organisations outside the NHS. A cyber attack on either the health or social care sectors could cause disruption across the whole health and social care sector. For example, the Care Quality Commission (CQC) told us that, as some trusts were unable to communicate with social services, there could have been delays in the discharge of patients from hospital to social care, although the CQC relayed advice from NHS Digital and NHS England to social care providers to help manage any disruption. This investigation sets out the facts about:

- the ransomware attack's impact on the NHS and its patients;
- why some parts of the NHS were affected; and
- how the Department and NHS national bodies responded to the attack.

Summary

1 The WannaCry attack affected NHS services in the week from 12 May to 19 May 2017. The Department of Health (the Department) and NHS England worked with NHS Digital, NHS Improvement, the National Cyber Security Centre, the National Crime Agency and others to respond to the attack.

Key findings

The risk of a cyber attack affecting the NHS

2 WannaCry was the largest cyber attack to affect the NHS, although individual trusts had been attacked before 12 May 2017. For example, two of the trusts infected by WannaCry had been infected by previous cyber attacks. One of England's biggest trusts, Barts Health NHS Trust, had been infected before, and Northern Lincolnshire and Goole NHS Foundation Trust had been subject to a ransomware attack in October 2016, leading to the cancellation of 2,800 appointments (paragraph 3.7 and Figure 5).

3 The Department was warned about the risks of cyber attacks on the NHS a year before WannaCry and although it had work under way it did not formally respond with a written report until July 2017. The Secretary of State for Health asked the National Data Guardian and the Care Quality Commission (CQC) to undertake reviews of data security. These reports were published in July 2016 and warned the Department that cyber attacks could lead to patient information being lost or compromised and jeopardise access to critical patient record systems. They recommended that all health and care organisations needed to provide evidence that they were taking action to improve cyber-security, including moving off old operating systems. Although the Department and its arm's-length bodies had work under way to improve cyber-security in the NHS, the Department did not publish its formal response to the recommendations until July 2017 (paragraphs 3.6 and 3.11).

4 The Department and its arm's-length bodies did not know whether local NHS organisations were prepared for a cyber attack. Local healthcare organisations such as trusts and clinical commissioning groups are responsible for keeping the information they hold secure, and for having arrangements in place to respond to an incident or emergency, including a cyber attack. Local healthcare bodies are overseen by the Department and its arm's-length bodies. The Department and Cabinet Office wrote to trusts in 2014, saying it was essential they had "robust plans" to migrate away from old software, such as Windows XP, by April 2015. In March and April 2017, NHS Digital had issued critical alerts warning organisations to patch their systems to prevent WannaCry. However, before 12 May 2017, the Department had no formal mechanism for assessing whether NHS organisations had complied with its advice and guidance. Prior to the attack, NHS Digital had conducted an on-site cyber-security assessment for 88 out of 236 trusts, and none had passed. However, NHS Digital cannot mandate a local body to take remedial action even if it has concerns about the vulnerability of an organisation (paragraphs 2.5, 2.7, 2.10 to 2.12 and 3.2, and Figure 4).

How the WannaCry attack affected the NHS

5 The attack led to disruption in at least 34% of trusts in England although the Department and NHS England do not know the full extent of the disruption (Figure 1). On 12 May, NHS England initially identified 45 NHS organisations including 37 trusts that had been infected by the WannaCry ransomware. Over the following days, more organisations reported they had been affected. In total, at least 81 out of 236 trusts across England were affected. The trusts included:

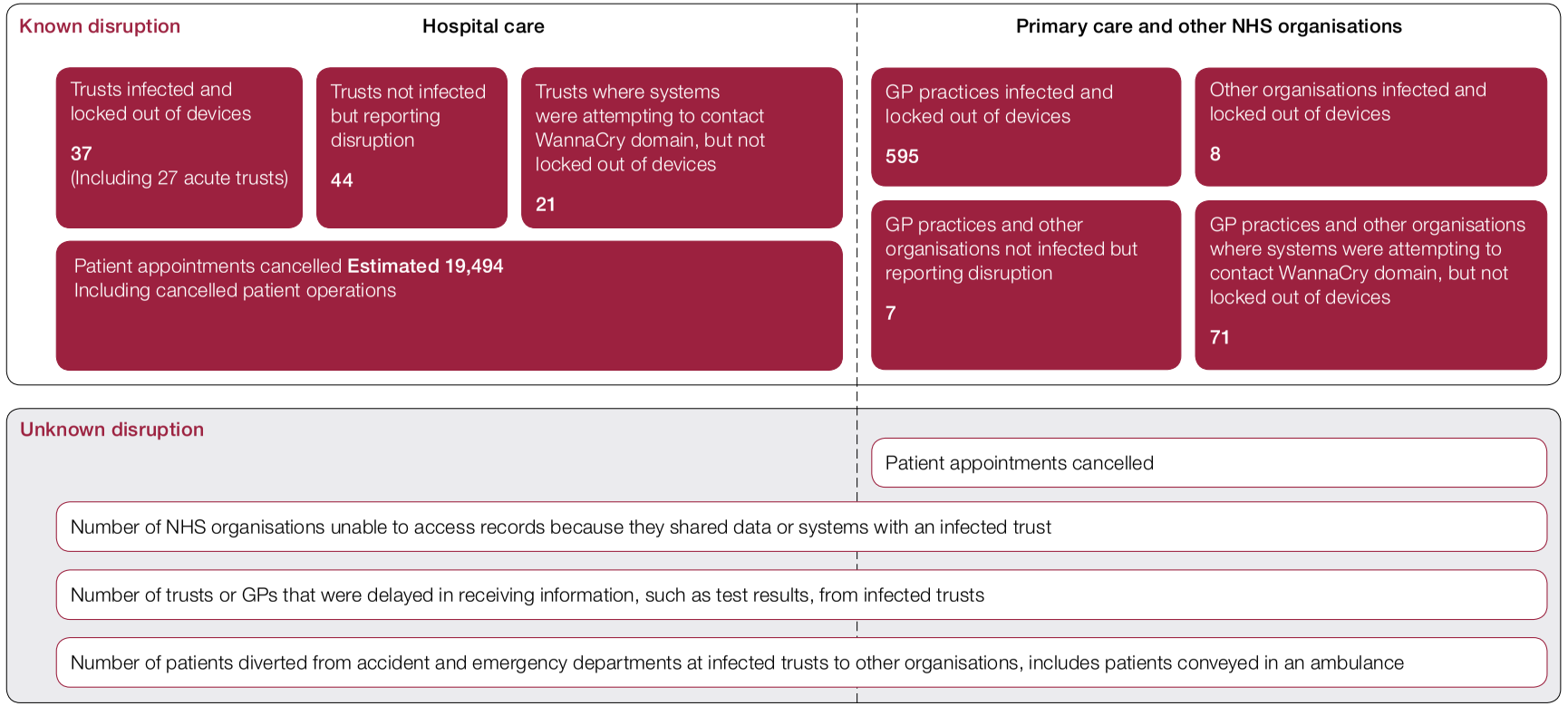
- 37 infected and locked out of devices (of which, 27 were acute trusts); and
- 44 not infected but reporting disruption. For example, these trusts shut down their email and other systems as a precaution and on their own initiative, as they had not received central advice early enough on 12 May to inform their decisions on what to do. This meant, for example, that they had to use pen and paper for activities usually performed electronically.

NHS England and NHS Digital identified a further 21 trusts that were attempting to contact the WannaCry domain, but were not locked out of their devices. There are two possible reasons for this. Trusts may have become infected after the kill-switch had been activated, and were therefore not locked out of their devices. Alternatively, they may have contacted the WannaCry domain as part of their cyber-security activity.

A further 603 primary care and other NHS organisations were infected by WannaCry, including 595 GP practices. However, the Department does not know how many NHS organisations could not access records or receive information, because they shared data or systems with an infected trust. NHS Digital told us that it believes no patient data were compromised or stolen (paragraphs 1.2 to 1.5 and 1.9, and Figure 1).

Figure 1
The impact of WannaCry on the NHS

The NHS experienced a wide range of disruption as a consequence of the WannaCry cyber attack



Notes

1 'Other organisations' include clinical commissioning groups, 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.

2 The numbers shown are based on organisations self-reporting problems to national bodies, and NHS England and NHS Digital's analysis of internet activity, and may be higher if some organisations did not report the problems they experienced in a timely or accurate way.

3 Some of the trusts identified as not infected but reporting disruption did have a small number of devices infected. However, they did not report themselves to NHS England as infected, and NHS England did not recategorise them as being infected after the WannaCry attack was over.

4 Some trusts, GP practices and other organisations were identified as having systems that attempted to contact the WannaCry domain, but were not locked out of their devices. There are two possible explanations for this: they could have become infected after the kill-switch had been activated. Or, they could have avoided infection but contacted the WannaCry domain as part of their cyber-security activity. NHS England does not know which organisations fall into each category.

Source: National Audit Office analysis of NHS England data

6 **Thousands of appointments and operations were cancelled and in five areas patients had to travel further to accident and emergency departments.** Between 12 May and 18 May, NHS England collected some information on cancelled appointments, to help it manage the incident, but this did not include all types of appointment. NHS England identified 6,912 appointments had been cancelled, and estimated more than 19,000 appointments would have been cancelled in total, based on the normal rate of follow-up appointments to first appointments. NHS England told us it does not plan to identify the actual number because it is focusing its efforts on responding appropriately to the lessons learned from WannaCry. As data were not collected during the incident, neither the Department nor NHS England know how many GP appointments were cancelled, or how many ambulances and patients were diverted from the five accident and emergency departments that were unable to treat some patients (paragraphs 1.7, 1.8 and 1.10, and Figure 1).

7 **The Department, NHS England and the National Crime Agency told us that no NHS organisation paid the ransom, but the Department does not know how much the disruption to services cost the NHS.** The Department, NHS England and the National Crime Agency told us no NHS organisation paid the ransom. NHS Digital told us it advised the trusts it spoke to not to pay the ransom, and wrote to all trusts on 14 May advising against the payment of ransoms. The Department does not know the cost of the disruption to services. Costs include: cancelled appointments; additional IT support provided by local NHS bodies, or IT consultants; or the cost of restoring data and systems affected by the attack. National and local NHS staff worked overtime including over the weekend of 13-14 May to resolve problems and to prevent a fresh wave of organisations being affected by WannaCry on Monday 15 May (paragraphs 1.11 and 1.12).

8 **The cyber attack could have caused more disruption if it had not been stopped by a cyber researcher activating a 'kill-switch'.** On the evening of 12 May a cyber-security researcher activated a 'kill-switch' so that WannaCry stopped locking devices. This meant that some NHS organisations had been infected by the WannaCry ransomware, but because of the researcher's actions, they were not locked out of their devices and systems. Between 15 May and mid-September NHS Digital and NHS England identified a further 92 organisations, including 21 trusts, as contacting the WannaCry domain, although some of these may have been contacting the domain as part of their cyber-security activity. Of the 37 trusts infected and locked out of devices, 32 were located in the North NHS region and the Midlands and East NHS region. NHS England believes more organisations were infected in these regions because they were hit early on 12 May before the WannaCry 'kill-switch' was activated (paragraphs 1.14 and 2.2, and Figure 3).

The NHS response to the attack

9 **The Department had developed a plan, which included roles and responsibilities of national and local organisations for responding to an attack, but had not tested the plan at a local level.** This meant the NHS was not clear what actions it should take when affected by WannaCry. NHS England found that responding to WannaCry was different from dealing with other incidents, such as a major transport accident. Because WannaCry was different it took more time to determine the cause of the problem, the scale of the problem and the number of organisations and people affected (paragraph 3.3 and Figure 2).

10 **As the NHS had not rehearsed for a national cyber attack it was not immediately clear who should lead the response and there were problems with communications.** The WannaCry attack began on the morning of 12 May. At 4 pm NHS England declared the cyber attack a major incident and at 6:45 pm initiated its existing Emergency, Preparedness, Resilience and Response plans to act as the single point of coordination for incident management, with support from NHS Digital and NHS Improvement. In the absence of clear guidelines on responding to a national cyber attack, local organisations reported the attack to different organisations within and outside the health sector, including local police. Communication was difficult in the early stages of the attack as many local organisations could not communicate with national NHS bodies by email as they had been infected by WannaCry or had shut down their email systems as a precaution, although NHS Improvement did communicate with trusts' chief executive officers by telephone. Locally, NHS staff shared information through personal mobile devices, including using the encrypted WhatsApp application. Although not an official communication channel, national bodies and trusts told us it worked well during this incident (paragraphs 3.3 to 3.5 and Figure 2).

11 **In line with its existing procedures for managing a major incident, NHS England initially focused on maintaining emergency care.** Since the attack occurred on a Friday this caused minimal disruption to primary care services, which tend to be closed over the weekend. Twenty-two of the 27 infected acute trusts managed to continue treating urgent and emergency patients throughout the weekend. However, five – in London, Essex, Hertfordshire, Hampshire and Cumbria – had to divert patients to other accident and emergency departments, and a further two needed outside help to continue treating patients. By 16 May only two hospitals were still diverting patients. The recovery was helped by the work of the cyber-security researcher that stopped WannaCry spreading (paragraphs 1.7, 1.13 and 1.14).

Lessons learned

12 NHS Digital told us that all organisations infected by WannaCry shared the same vulnerability and could have taken relatively simple action to protect themselves. All NHS organisations infected by WannaCry had unpatched or unsupported Windows operating systems so were susceptible to the ransomware. However, whether organisations had patched their systems or not, taking action to manage their firewalls facing the internet would have guarded organisations against infection. NHS Digital told us that the majority of NHS devices infected were unpatched but on supported Microsoft Windows 7 operating systems. Unsupported devices (those on XP) were in the minority of identified issues. NHS Digital has also confirmed that the ransomware spread via the internet, including through the N3 network (the broadband network connecting all NHS sites in England), but that there were no instances of the ransomware spreading via NHSmail (the NHS email system) (paragraphs 1.2, 1.6 and 2.4 to 2.6).

13 There was no clear relationship between vulnerability to the WannaCry attack and leadership in trusts. We found no clear relationship between trusts infected by WannaCry and the quality of their leadership, as rated by the Care Quality Commission (paragraph 2.8).

14 The NHS has accepted that there are lessons to learn from WannaCry and is taking action. Lessons identified by the Department and NHS national bodies include the need to:

- develop a response plan setting out what the NHS should do in the event of a cyber attack and establish the roles and responsibilities of local and national NHS bodies and the Department;
- ensure organisations implement critical CareCERT alerts (emails sent by NHS Digital providing information or requiring action), including applying software patches and keeping anti-virus software up to date;
- ensure essential communications are getting through during an attack when systems are down; and
- ensure that organisations, boards and their staff are taking the cyber threat seriously, understand the direct risks to front-line services and are working proactively to maximise their resilience and minimise impacts on patient care.

Since WannaCry, NHS England and NHS Improvement have written to every trust, clinical commissioning group and commissioning support unit asking boards to ensure that they have implemented all 39 CareCERT alerts issued by NHS Digital between March and May 2017 and taken essential action to secure local firewalls (paragraphs 3.8 and 3.9).