Public Accounts Committee inquiry: Cyber-attack on the NHS

Submission by NHS Providers, January 2018

NHS Providers is the membership organisation and trade association for the NHS acute, ambulance, community and mental health services that treat patients and service users in the NHS. We represent 99% of all NHS foundation NHS trusts and NHS trusts, who collectively account for £74 billion of annual expenditure and employ more than one million staff.

Key messages

- A large majority of the affected NHS trusts managed to carry on treating urgent and emergency patients through the weekend, and a few days after the attack only two were still diverting patients. This demonstrates the high levels of commitment, resilience and resourcefulness of staff working under difficult conditions.

- We agree with the National Audit Office (NAO) report that there is significant work to be done but it is important to remember that this cyber attack was not focused on the NHS alone; it was a global attack which affected many organisations including multiple large multinationals. The NHS is taking steps at national and local level to prepare for the next attack. Part of this is to ensure that NHS trusts apply software patches and keep anti-virus software up to date. Capital investment is vital to upgrade the complex digital infrastructure in NHS trusts.

- There are lessons to be learned around communication. There was a lack of leadership and coordination from NHS England and NHS Digital on the day of the attack. This was frustrating not only for those NHS trusts affected by the attack but also for those seeking to prevent the spread of the virus.

Introduction

1. The WannaCry cyber attack in May 2017 brought significant disruption to the NHS in England with 37 NHS trusts directly affected and disruption to a further 44 NHS trusts. The report by the NAO into the cyber attack on the NHS gives us a valuable opportunity to look at what the service needs to do to minimise the risk of future cyber attacks.

2. The NAO rightly acknowledges the important contribution of NHS staff who worked overtime to stop or minimise the impact of the attack on patients. Our submission focuses on the complexity of infrastructure across the NHS, the need for capital investment and more effective communications during the attack. We have included feedback we have received from NHS trusts.

Complexity of infrastructure

3. Within the NHS, there are hundreds of separate entities each with their own complex infrastructures. For example, there are 231 NHS trusts in England, each with their own IT infrastructure running multiple technologies and activities across a variety of operating systems. NHS trusts have over a million devices, which range from PCs and laptops to MRI and CT scanners.

4. Despite the complex nature of NHS technology, business continuity and disaster recovery plans kicked in during the attack where appropriate. This varied from closing down potentially

comprised systems in some NHS trusts to activating a "silver command" response in others. Many of the affected NHS trusts reverted to paper records which meant they could continue seeing patients.

5. The NAO report highlights that there had been a failure to patch and update systems as well as a reliance on old software. There are a number of factors which make it very difficult to schedule and complete any software upgrade, and to avoid delaying patient care:
   - Equipment may be needed 24 hours a day throughout the year.
   - Many medical devices also run on embedded versions of software. As the NAO also notes, in some cases, upgrades to these devices need to be carried out by the supplier, rather than the trust. For example, MRI scanners are connected to both a trust and the equipment supplier's network and the specific software for the scanner needs to be updated in close collaboration with the supplier.
   - In some cases the equipment used by NHS trusts can be costly to replace but is sufficiently old that it cannot be upgraded as the third party suppliers no longer exist.
   - A number of NHS trusts were still in the process of converting from XP. However it is worth noting that there is not a direct correlation between using XP and being impacted by the attack and NHS trusts outperform the commercial sector in moving away from XP.
     - 52% of businesses are still using XP in their companies and it's still installed on 14% of business computers.
     - In Dec 2015, 1 in 5 NHS trusts were using XP; in June 2017 it had fallen to 1 in 20.
     - 20% of NHS trusts were affected by the malware but less than 5% were using XP.

Communications

6. NHS trusts are clear that while the national and local communications within the NHS, and with the public, should be reviewed and lessons learnt for future incidents, nevertheless the NHS handled the response well given the scale of the attack.

7. The difficulty of mass communication – both from the national bodies to the frontline, and within local NHS bodies – without email was a challenge faced across the NHS and other corporations subject to the attack. This was a particular issue as the national bodies led the response, and continued to use NHS email to communicate during an incident that involved NHS email. This meant that central messages were often missed due to incoming emails being blocked.

8. Significant thought needs to be given to what future communications channels are used within NHS trusts, throughout local health and care systems and nationally, to ensure communication is still possible during any future attacks. For some NHS trusts and organisations email was down for a considerable length of time, and adopting alternative communications channels will be key in the future. This seems likely to be via mobile, personal email or instant messaging services for communications such as WhatsApp. We know that some regional communications networks – working across providers, commissioners and regional offices of the central bodies – have now set up WhatsApp groups but it is important that no sensitive data is shared in these groups. There is a need to have secure instant messaging solutions within the NHS in the future as whilst WhatsApp has end to end encryption it doesn't meet the NHS information governance requirements.

Role of national bodies

9. NHS Digital was the official lead organisation for the national NHS response to the attack, but NHS England in particular also took on a public facing role. There were several examples of NHS trusts receiving constructive support from communications teams in the national and regional offices of NHS England and NHS Improvement. However, overall we have heard from NHS trusts that, during the attack there was confusion about the role of the different bodies, with greater clarity needed over which one was leading and NHS trusts receiving multiple information requests.

10. Many NHS trusts also said they would have liked NHS Digital to be more proactive in providing updated messages across traditional media and social media channels as the situation developed. NHS trusts also found that there was limited central guidance or information updates from NHS Digital meaning that they had to rely on wider networks and industry contacts for information. Some NHS trusts were told not to release any messages to the public even though they wanted to reassure the public that their A&E was still open. This had repercussions for NHS trusts and their relationships with their local media and patients.

11. We would recommend greater clarity about NHS Digital's role in handling future incidents, as well as a more joined up and visible response from the national bodies. More could have been done to set out what steps the NHS was taking to protect patients and service users an it would have been helpful to frontline staff if there had been greater public awareness that WannaCry was not just an attack on the NHS, as some media were implying, but in fact a global attack which affected 200,000 victims in 150 different countries.

Capital investment

12. There needs to be proper investment in NHS infrastructure - NHS buildings, NHS medical equipment and NHS IT – to enable the NHS to function effectively. For the past five years the NHS capital budget has been used to cover day to day operating costs, with £1.2bn taken from the capital budget in 2016-17[1]. That inevitably brings risk, but this has not always been sufficiently associated with the knock-on impact of ageing IT infrastructure. There are also misperceptions about the scale of the task – it is not as simple as upgrading software in those NHS trusts still running Windows XP. Underinvestment in technology is a much wider issue with more complex ramifications.

13. We welcome the commitment from NHS England and NHS Improvement as set out in the NAO's report to reprioritise £21 million in capital funding from existing IT budgets to improve cyber-security in major trauma centres. We hope this is the beginning of a far greater national understanding of and investment in capital, and recognition of the resilience that this imbues in day-to-day operations.

Conclusion

14. Any major incident, whatever the cause, gives an opportunity to look at what can be improved in the future. Cyber crime is not new, but it is developing at an alarming rate and is therefore an extraordinarily difficult risk to mitigate. NHS trusts can continue to ensure they do all they can to prevent cyber attacks, through security measures and staff awareness, but the risk will remain.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/629984/DH_annual_accounts_2016_2017_web_version.pdf

We need significant capital investment to ensure we can deal with the threat of cyber crime in the future.

15. Business continuity and disaster recovery plans were initiated and escalated to the appropriate level. Some NHS trusts also had specific cyber security response plans, which proved invaluable as they were able to invoke this plan as soon as they were alerted. There is now an opportunity to evaluate them and be better prepared in the event of a future attack.

16. Despite the multitude of issues faced, the staff involved went above and beyond to ensure that patient safety and patient care were never compromised. Clinical and support staff worked closely to minimise the impact on patients and restore IT systems.

17. NHS Providers will do everything it can to ensure that NHS trusts share good practice, and we've seen examples of this already happening. We will continue to make the case for significant investment in IT infrastructure.