BMJ 2018;361:k2381 doi: 10.1136/bmj.k2381 (Published 4 June 2018)

EDITORIALS

WannaCry—a year on

Investment is important, but a culture change is crucial

Guy Martin *clinical research fellow*[1], Saira Ghafur *senior policy fellow*[1], James Kinross *senior clinical lecturer*[1], Chris Hankin *professor*[2], Ara Darzi *professor*[1]

[1]Institute of Global Health Innovation, Imperial College London, UK; [2]Institute for Security Science and Technology, Imperial College London, UK

The disruption from last year's WannaCry malware attack affected 60 NHS trusts, 595 general practices, and thousands of patients.[1] The costs of the cybersecurity incident are not known. Worryingly, all 200 NHS hospitals inspected by the Care Quality Commission since the attack have fallen short of the UK government's Cyber Essentials Plus certification, a basic set of minimum organisational security standards.[2 3]

This sobering finding not only highlights the poor security and resilience in the NHS but also suggests that little real progress has been made in the past year. As we continue to rely evermore on technology, effective cybersecurity should be a fundamental part of the healthcare culture. Any breach, loss, or corruption of patient data can paralyse a hospital, harm individuals, and erode patients' trust in healthcare systems that are regularly under threat as they are a rich source of data and present a soft target.[4 5] The sophistication of cyberattacks continues to evolve, from amateur hackers or accidental compromise to complex state sponsored attacks. The risk is greater than ever.

Effect on patients

WannaCry was not targeted at the NHS but is now viewed as a warning shot. At a minimum, almost 7000 outpatient appointments were cancelled and an urgent cancer referral was delayed for at least 139 patients.[1] Operations were cancelled, and patients were in some cases diverted to alternative emergency facilities. Crucially, no data were collected on the number of cancelled GP appointments or the effect on social care providers.[1 6]

According to the report from the National Audit Office, no NHS organisations reported any harm to patients, although the evidence is limited.[6] How was harm quantified other than in terms of mortality? How long did the effect last beyond the initial event? What was the effect of lost imaging and cancelled appointments or procedures? And how were organisations able to track and report incidents when computer systems were down?

This incident highlights the fact that cybersecurity is not just an IT problem but a patient safety problem. Wrong site surgery is a serious error resulting in harm to a single patient, but a cyber incident may cause harm to every patient across a healthcare system. To protect the most vulnerable and critical elements of the health and social care system, it is crucial to develop and implement an agreed strategy for measuring the true effect of cybersecurity incidents and wider health IT failures.

National response

The Department of Health and Social Care, along with NHS England, NHS Digital, and NHS Improvement, has coordinated the response to the WannaCry attack, with each organisation taking on specific responsibilities. The government will invest £150m (€170m; $200m) over the next three years to improve the capabilities in the health service for preventing attacks, detecting threats, and mitigating harm.[1]

After WannaCry, £21m was channelled into tackling vulnerabilities in critical elements of the system—such as major trauma centres and ambulance trusts—and to overcome weaknesses in essential technology such as diagnostics.[1] A further £25m was made available to help NHS organisations that have identified weaknesses in their infrastructure to strengthen their systems.[1] The latest initiative aims to ensure that all NHS organisations upgrade their software to Microsoft Windows 10 to improve resilience.[7]

While progress is welcome, a systems approach and clear plan are required; systems should be secure by design, not default. Most health and social care providers are still likely to be highly vulnerable. Healthcare has, furthermore, lagged behind other critical infrastructure areas (power grid, water supply, etc) in terms of cybersecurity defences, with lower investment and national prioritisation. The government needs to make healthcare a priority for cybersecurity: the current lack of resilience may have far reaching consequences.[8 9]

Changing culture

Infrastructure investment is crucial for ensuring that IT systems and patient data are protected in the event of a cyberattack. Procedures to manage incidents need to be developed and tested, and business continuity planning improved. Concurrently,

Correspondence to: G Martin guy.martin@imperial.ac.uk

cybersecurity needs to be completely rethought and approached as a patient safety concern by raising awareness among healthcare staff and promoting strong leadership.

Security is about people and the workplace culture. The most common sources of ransomware are inadvertently opened malicious emails, and one of the biggest risks to data therefore comes from people inside the organisation.[10] Since it is easy to access large amounts of sensitive personal information, the risk of unintentional or deliberate compromise by staff must be tackled. Organisations must also be trusted by patients to secure their data and use them appropriately. Education programmes, including the NHS Digital Academy, provide excellent opportunities to improve awareness and educate digital healthcare leaders.

Clarity is needed about where responsibility, accountability, and authority lie. Good leadership, both nationally and locally, is key to ensure a consistent message is delivered and effective change delivered.[11] Lack of robust leadership was undoubtedly a contributing factor to the WannaCry attack and to the weak security of the health and social care system.[11]

All organisations must comply with the Data Protection Act, which includes compliance with the General Data Protection Regulation, and Directive of Security of Network and Information Systems. The impact of these has been hugely underestimated, and substantial doubts remain about how prepared the system is.[12] Investing in infrastructure and people, educating staff, delivering effective governance through strong leadership, and identifying the cyberthreat as a fundamental threat to patient safety are therefore pressing concerns.

A year on from WannaCry, we must not be complacent that there has not been another large cybersecurity incident in the NHS or social care. One thing is certain: it is a question of when—and not if—it happens again. The threat and potential effects are increasing, and security can never be completely effective. In addition to much needed investment, a fundamental cultural change is essential: effective healthcare cybersecurity must be a pillar of patient safety.

Competing interests: The authors have read and understood BMJ policy on declaration of interests and have no relevant interests to declare.

Provenance and peer review: Not commissioned, not externally peer reviewed.

1 Lessons learned review of the WannaCry Ransomware Cyber Attack. Department of Health and Social Care, 2018. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf
2 Public Accounts Committee. Cyberattack on the NHS Inquiry. 2018. https://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/inquiries/parliament-2017/nhs-cyber-attack-17-19/
3 Hughes O. NHS trusts fail post-WannaCry cyber security checks. *Digital Health* 2018 Feb 7. https://www.digitalhealth.net/2018/02/nhs-trusts-fail-post-wannacry-cybersecurity/
4 Brendan P. Anthem to pay record $115 million to settle US lawsuits over data breach. Reuters 2017 Jun 23. https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML
5 Yadron D. Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers. *Guardian* 2016 Feb 17. https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center
6 National Audit Office. Investigation: WannaCry cyber attack and the NHS. National Audit Office, 2017. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
7 Dearden L. NHS to spend £150m on cyber security to bolster defences after WannaCry attack. *Independent* 2018 Apr 28. https://www.independent.co.uk/news/health/cyber-attacks-nhs-wannacry-security-investment-microsoft-a8327091.html
8 Hughes O. Cybersecurity forecast 2018: threats and trends for the year ahead. *Digital Health* 2017 Dec 28. https://www.digitalhealth.net/2017/12/cybersecurity-2018-predictions/
9 Levenathall R. Report: healthcare way behind other major sectors in proper cybersecurity protocols. *Healthcare Informatics* 2018 Feb 14. https://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-way-behind-other-major-sectors-proper-cybersecurity
10 Mukherjee SY. Why is health care cybersecurity so bad? Blame the insiders, New Verizon report says. *Fortune*, 2018 Mar 2. http://fortune.com/2018/03/02/healthcare-cybersecurity-verizon-report/
11 Cyber-attack. “Fix is about leadership not money.” BBC Newsnight 2017 May 16. http://www.bbc.co.uk/news/av/technology-39933577/cyber-attack-fix-is-about-leadership-not-money
12 McCall B. What does the GDPR mean for the medical community?*Lancet* 2018;391:1249-50. 10.1016/S0140-6736(18)30739-6 29619949