The challenges of cybersecurity in health care: the UK National Health Service as a case study

As modern technology becomes indispensable in health care, the vulnerabilities to cyber-threats continue to increase, compromising the health information and safety of millions of people. This threat can happen in several ways: data can be stolen; data might be deleted or corrupted in a way that is not obvious until years later; and medical devices can be hacked, causing direct harm to patients.

In May, 2017, the WannaCry ransomware encrypted data and files on 230 000 computers in 150 countries, and impaired the functionality of the National Health Service (NHS) in England.[1] Key systems were blocked, preventing staff from accessing patient data and critical services. However, the WannaCry attack was not directly targeted at the NHS. Other major organisations were affected, including Telefonica, FedEx, Nissan, Russian Railways, and the Bank of China. However, the biggest effect was undoubtedly felt by the NHS.[2] While health systems worldwide watched, it became apparent how susceptible health care is to any cyber threat.

Today, at a global scale, the number of cyberattacks across all industries is rising, and the financial impact is accumulating: the average cost of a data breach globally is, according to a 2018 report[3] from IBM, US$3·86 million. Although health-care organisations might be less likely than financial services or public-sector bodies to be targets of cyberattack, the cost per capita for a data breach in health care was $408, nearly double that of financial services, which ranked second. Health-care organisations also take substantially longer than other industries to contain data breaches because of a lack of resources, both financial resources and trained personnel, and inefficient infrastructure.[3]

The problems seen in the NHS, a publicly funded nationalised health-care system, might help other countries to determine their security priorities going forward. In general, limited budgets and time-consuming

This online publication has been corrected. The corrected version first appeared at thelancet.com/digital-health on May 23, 2019

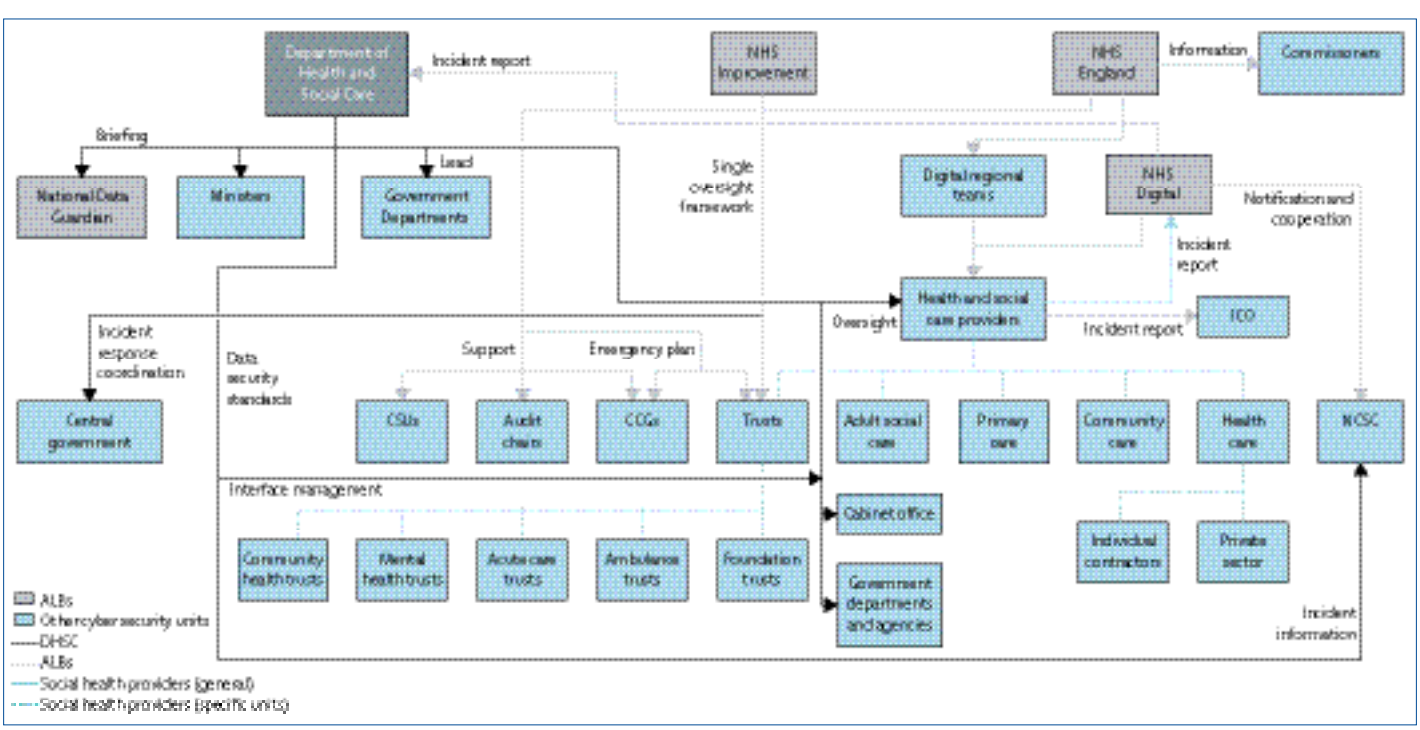


Figure: **National accountabilities for cyber security of the UK Department of Health and Social Care and Arm's Length Bodies**
This figure is based on discussions with representatives from National Health Service (NHS) England, NHS Digital, and the Department of Health and Social Care (DHSC). The figure was verified by the Department of Health and Social Care. ALB=Arm's Length Body. CCG=Clinical Commissioning Group. CSU=Commissioning Support Unit. ICO=Information Commissioner's Office. NCSC=National Cyber Security Centre.

approval processes are attenuating the NHS's ability to adapt to evolving technological challenges. Since the WannaCry attack, the NHS has taken several steps to increase its cyber resilience, and accountabilities have been assigned to the Department of Health and Social Care and Arm's Length Bodies (ALBs), as shown in the figure. The figure highlights the substantial complexity of NHS organisational structures because of the large number of ALBs and sovereign organisations. A new ALB, NHS X, will be launched in July, 2019, with the remit of overseeing digital transformation in the NHS, including setting cyber security standards. How this will alter the above accountabilities remains to be seen. Uncoordinated processes and overlapping competencies result in higher costs, inefficiency, and wasted resources. This problem is not new and, despite the complexity of doing so, most NHS services are delivered in a joined-up way, which, has not been the case for cybersecurity functions. One of the biggest problems for cybersecurity has been navigating accountability, making it difficult for frontline organisations to seek appropriate resources and help. Furthermore, the information technology (IT) landscape within the NHS is highly heterogeneous and inconsistent. To date, to our knowledge, no catalogue exists to systematically list all software and hardware deployed within the NHS, leading to a severe lack of awareness of vulnerabilities.

Although cyber incidents are required to be reported and registered in the NHS, the data are not systematically processed and assessed, resulting in missed opportunities to understand risks and threats. Risks and vulnerabilities are not measured at a local level, making it difficult to assess the effect of a cyberattack on NHS IT infrastructure, data, and patients in advance.

Health care is the only industry globally for which the biggest threat to data breaches comes from internal sources.[4] In 2017, 46% of breaches were due to employee behaviour (eg, by clicking on infected links in e-mails, employee negligence, or abusing access to data).[5] Currently, online training is mandatory for all NHS staff members, although evidence from 2018 shows that only 12% of NHS Trusts have reached this mark.[6] Given the risk human error presents to data breaches in health care, instructions and training on cybersecurity for all employees need to be given greater precedence.

There has been chronic underinvestment in health-care IT, especially compared with other market sectors; this investment can be as little as 1–2% of the annual budget on IT compared with 4–10% in other sectors.[7] To embed a security culture, progressive investment needs to be made in IT and an economic impact assessment to understand what is working.

Since the WannaCry attack, substantial capital has been invested to upgrade systems and to improve cybersecurity capabilities across the NHS.[1] However, with limited budgets, health systems are faced with difficult choices in allocating resources and cybersecurity investment is often not a priority. This choice of resource allocation is often seen as a trade-off in all sectors, although the potential consequences for health-care—both patient safety and economic—could be staggering if not addressed. What will be the tipping point before cultural and organisational changes are made across the board? Our case study highlights issues that are clearly relevant and applicable to health systems globally. Yet we should ask what lessons can disparate health systems learn from each other, and how can we scale and spread this learning to ensure we can minimise the effect of any future cyberattacks.

The most recent well publicised cyber-attack on health care was in Singapore in 2018, in which the health data of 1·5 million Singaporeans, including the country's Prime Minister, was stolen.[8] A Committee of Inquiry was subsequently appointed and some of the major recommendations included the review of all systems and networks fully and regularly by Singapore's Ministry of Health; the training of all staff in cybersecurity practices; the requirement of enhanced security checks on critical systems; and regulation of responses to attacks to prevent damage.[8]

A so-called cyber-siege, in 2007, led the Estonian government to create its cybersecurity strategy, which has built many aspects of cybersecurity into the country's law.[9] The Estonian Information System Authority publishes an annual cybersecurity report, which found that nearly 11 000 cybersecurity incidents occurred in 2018, although only 122 of all these cases, ten of which were in health care, directly affected the functionality of the systems.[9] To combat cybersecurity threats in health care, Estonia introduced blockchain technology to securely manage electronic patient records creating a time-stamped record of anyone coming in contact with it, and adding or omitting information. Estonia is a digitally advanced society,

where patients use electronic identification cards to access their health information and decide with who this information can be shared with.[9]

The USA has had some of the most highly publicised cyberattacks on health care; in 2015, criminals stole 80 million records from Anthem, a US health insurance company.[7] Federal regulations for protecting patient health information are covered under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009.[10] The most recent development has been the launch of the US National Institute of Standards and Technology cybersecurity framework[11] in 2018, which represents a collaboration between the US government and private entities to improve cyber infrastructures throughout the country. This framework, which is voluntary, is used across crucial sectors and is the most frequently used to improve cyber-resilience in health care in the USA.[11]

Although these three examples hail from different contexts, they highlight common cyber security problems and subsequent principles of best practice that are universal to improve cyber resilience in health care.

Because of the NHS's complex structure, there is a lack of clearly defined responsibilities and security preparedness in the face of a cyberattack, making it near impossible to assess the NHS's resilience and the potential effect an event would have on the health and social care system. The available NHS response and mechanism of accountability are not clear. Addressing this issue requires a concerted effort, not only to clarify frameworks but also to promote and instil a single understanding of cybersecurity. The alternative is to face substantial reputational and financial loss, and, most importantly, risk patients' safety.

*Saira Ghafur, Emilia Grass, Nick R Jennings, Ara Darzi
Institute of Global Health Innovation and National Institute for Health Research Patient Safety Translational Research Centre, Imperial College London, London SW7 2AZ, UK (SG, EG, AD); and Department of Computing and Department of Electrical and Electronic Engineering, Imperial College London, London, UK (NRJ)
saira.ghafur13@imperial.ac.uk

We declare no competing interests.

This work was supported by the National Institute for Health Research Imperial Patient Safety Translation Research Centre. Infrastructure support was provided by the National Institute for Health Research Imperial Biomedical Research Centre. The views expressed are those of the author(s) and not necessarily those of the National Health Service, the National Institute for Health Research, or the Department of Health. EG was also supported by the Fritz Thyssen Foundation in Germany.

Copyright © 2019 The Author(s). Published by Elsevier Ltd. This is an Open Access article under the CC BY 4.0 license.

1 Smart W. Lessons learned review of the WannaCry ransomware cyber attack. London: Department of Health & Social Care, 2018. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf (accessed Feb 12, 2019).

2 Ghosh A, Ashok I. WannaCry: list of major companies and networks hit by ransomware around the globe. *International Business Times* May 16, 2017. https://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hit-by-deadly-ransomware-around-globe-1621587 (accessed Feb 12, 2019).

3 IBM. 2018 cost of a data breach study: global overview. 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN& (accessed Feb 12, 2019).

4 Verizon. 2018 Data Breach Investigations Report. 2018. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf (accessed Feb 12, 2019).

5 Infoguard Cyber Security. 5 industries that top the hit list of cyber criminals in 2017. 2017. http://www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/ (accessed Feb 12, 2019).

6 REDSCAN. REDSCAN reveals a large disparity in cybersecurity skills and spending across NHS. 2018. https://www.redscan.com/news/nhs-cybersecurity-skills-survey/ (accessed Feb 12, 2019).

7 Cybersecurity and healthcare: how safe are we? *BMJ* 2017; **358:** j3179.

8 Kwang K. SingHealth cyberattack: Committee of Inquiry appointed, report due end-2018. *Channel NewsAsia* July 24, 2018. https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-committee-of-inquiry-appointed-report-due-10557724 (accessed Feb 12, 2019).

9 e-Estonia. Cyber security report 2018: investing in the security of information systems to secure digital lifestyle. 2018. https://e-estonia.com/cyber-security-report-2018/ (accessed Feb 12, 2019).

10 Jalali MS and Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. *J Med Internet Res* 2018; **20:** e10059.

11 National Institute of Standards and Technology. Cybersecurity framework. 2018. https://www.nist.gov/industry-impacts/cybersecurity (accessed Feb 12, 2019).