BMJ 2017;358:j3179 doi: 10.1136/bmj.j3179 (Published 2017 July 06)

ANALYSIS

Cybersecurity and healthcare: how safe are we?

Rising cybersecurity threats to healthcare require policy makers to tackle fragmented governance, to develop and implement security standards, and to help organisations to improve their resilience, say **Guy Martin and colleague**s

Guy Martin *clinical research fellow*[1], Paul Martin *honorary principal research fellow*[2], Chris Hankin *director*[2], Ara Darzi *director of the Institute of Global Health Innovation*[1], James Kinross *senior lecturer in surgery*[1]

[1]Department of Surgery and Cancer, Imperial College London, 10th Floor QEQM Building, St. Mary's Hospital, Praed Street, London W2 1NY, UK; [2]Institute for Security Science and Technology, Level 2 Admin Office, Central Library, Imperial College London, South Kensington Campus, London, UK

Healthcare systems around the world have rightly identified the huge potential for digital technology to improve clinical outcomes and transform care delivery.[1] But the recent WannaCry malware attack has once again highlighted cybersecurity as a critical patient safety issue requiring urgent solutions.

Cybercrime—a universal challenge

Cyberattacks usually steal money, data, or intellectual property, but increasingly the aim is to cause overt disruption or political impact. They are often transnational and state sponsored; attributing them to individuals can be difficult. Many attacks are undetected or unreported, and only a small minority enter the public domain; among recent examples are the major breaches at TalkTalk, Mossack Fonseca, the US Democratic National Committee, and Yahoo. The global cost of cybercrime in 2014 was estimated to be $575bn (£440bn; €500bn).[2]

Cybercrime and healthcare

Healthcare faces even larger cyber risks than other sectors because of inherent weaknesses in its security posture. It is one of the most targeted sectors globally; 81% of 223 organisations surveyed, and >110 million patients in the US had their data compromised in 2015 alone.[3 4] Only half of these providers think that they are capable of defending themselves from cyberattack, and there has been a 300% increase in attacks in the past three years,[3 5] For those conducting cyberattacks the healthcare sector is an attractive target for two simple reasons: it is a rich source of valuable data, and it is a soft target. The current and emerging cyber risks to healthcare are outlined in box 1.

The healthcare sector is usually targeted for financial gain; cybersecurity aims to protect the confidentiality, integrity ,and availability of valuable healthcare data. Protecting confidentiality means ensuring that sensitive information, especially identifiable data, does not reach the wrong people. In 2015 criminals stole 80 million records from Anthem, a US health insurance company. Given that individual medical records are traded on the "dark web" for around $50, this breach had a market value of a billion dollars or more.[6] Medical records, especially those in the US, are worth much more on the black market than credit card details because they contain multiple permanent identifiers and financial information.[4] Unlike credit cards, these identifiers cannot be reset, and a person's records might contain enough information to open bank accounts, obtain loans, or acquire a passport. Protecting integrity means ensuring the accuracy and trustworthiness of data, and protecting availability means maintaining reliable access to the data and to the systems used to process and store the data.

The fallout from the global WannaCry ransomware attack in May 2017 is still settling; it reportedly affected around 200 000 systems in more than 150 countries.[7] Around 50 hospitals in the UK were directly affected, and many more pre-emptively shut down their computer systems causing considerable disruption—affecting care delivery, compromising patient safety, and potentially eroding trust. The attack used a prevalent type of malware known as ransomware; a malicious piece of software that encrypts the victim's data, blocks access to them, and threatens to publish or delete them unless a ransom is paid. The only way to regain access to the infected computer and data is to pay the ransom or to wipe the system and retrieve a backup.

The WannaCry attack, though hugely disruptive, did not specifically target the healthcare sector, but this has not always been the case. In 2016 a ransomware attack on the Hollywood Presbyterian Medical Center shut down its network for 10 days, preventing staff from accessing medical records or using medical equipment until the hospital paid the ransom (reportedly 40 Bitcoins, or about $17 000).[8] The infection is thought to have taken place through a "phishing" email. These are the

Correspondence to: J Kinross j.kinross@imperial.ac.uk

Box 1: Common and emerging cyber threats in healthcare

Data theftfor financial gain—stealing personal data for the purposes of monetary gain; for example, names, addresses, social security details, financial information

Data theft for impact—theft and public release of sensitive medical information; for example, celebrities, politicians, or other high profile people

Ransomware—using malware to block users from their data or systems or to delete data unless a fee is paid

Data corruption—deliberate corruption of data , such as altering test results, for political or personal gain

Denial of service attacks—disruption of a network or system by flooding it with superfluous requests, motivated by blackmail, revenge, or activism

Business email compromise—creating fake personal communications for financial gain; for example, obtaining fraudulent payments or personal information

The unwitting insider—substantial disruption to systems or the loss of data owing to the unintentional actions of staff using outdated and at-risk systems

commonest means of delivering malware and are hard to defend against. Even in security conscious organisations, the click rate on a well crafted phishing email can be up to 30%.[4] Ransomware has affected other hospitals: one English hospital was forced to cancel all operations and transfer patients for two days in 2016,[9 10] and Boston Children's Hospital and hospitals in Germany have also been targeted.[11] Freedom of information requests in the UK found that in 2015-16 up to half of NHS trusts were hit by ransomware in the preceding year.[12] Despite these well publicised attacks and the availability of security patches, the warnings went largely unheeded resulting in the major disruption caused by WannaCry.

Although the healthcare sector is usually targeted for financial gain, other motives have also been reported. In 2016 1.28 million records from the Australian Red Cross Blood Service that contained large amounts of sensitive information, including donors' at-risk sexual behaviour, were posted on a public website for no clear motive but to expose security flaws.[9 13] Cyberattacks are also used for political impact—most notably in the recent attacks against the World Anti-Doping Agency, in which the medical records of prominent athletes were released.[14] Hackers linked to the militant group Islamic State have directly targeted NHS websites for propaganda purposes.[15] Other scenarios in which high profile people are targeted to damage their reputations are easy to imagine.

Why is healthcare so vulnerable?

The vulnerability of healthcare to cyberattack reflects a combination of factors, notably limited resources, fragmented governance, and cultural behaviours. Compared with other sectors, such as financial services, healthcare has chronically underinvested in information technology (IT) infrastructure. Many NHS organisations spend as little as 1-2% of their annual budget on IT, compared with 4-10% in other sectors,[16] and use many run-on legacy systems that are no longer supported. Indicative of this low level of investment many NHS trusts are still using Windows XP, an operating system that Microsoft stopped supporting in 2014.[17]

In addition, cybersecurity experts are in short supply, and cash strapped healthcare organisations cannot afford to pay the market rate for their services. Fragmented governance is another big problem, leading to a lack of clarity over who is responsible for securing systems and data. The UK healthcare sector comprises many thousands of distinct entities, and clear accountability and responsibility for cybersecurity at a national level are lacking. Finally, the culture of healthcare understandably focuses on caring for patients, even at the expense of security. One symptom of this patient first culture is the widespread sharing of passwords—a practice that makes sense but undermines security.

What does the future hold?

So far, attacks on healthcare have principally been for financial gain; the integrity of data has not been compromised. But we face the prospect that, intentionally or unwittingly, it will be. Consider the harm that could be caused by altering blood groups or test results.

Another worrying prospect is that of malicious cyberattacks on medical devices. In 2014 more than 300 medical devices were identified as being at risk.[4] In 2016 patients were warned of a vulnerability that could allow hackers to take control of the Animas OneTouch insulin pump.[18] Barnaby Jack, a well known hacker, has shown how to hack a Medtronic insulin pump to deliver a lethal insulin dose with a remote control.[19] Risks such as these seem set to rise with the rapid growth in consumer, wearable, and mobile technologies.[4-21]

Poor cybersecurity also has major financial and reputational risks for healthcare. Every European institution, including healthcare providers, should be thinking about the implications of the General Data Protection Regulation, which comes into effect in 2018. Among other things, the regulation makes it mandatory to report security breaches within 72 hours; non-compliance can result in a fine of up to €20m or 4% of annual global turnover.[22] The UK has had little central guidance or leadership on how organisations can meet these responsibilities. Another worry is that large scale compromises of patient data might undermine public confidence, making patients more reluctant to share their data with clinicians or researchers.[23 24]

What can the healthcare sector do?

Cybersecurity can never be 100% effective, and the threat to healthcare is an unavoidable new reality. But individuals and organisations can take practical steps to protect themselves and to reduce the effects of an attack.

An ultimate aim of cybersecurity should be to strengthen resilience. Resilient organisations are less likely to have their security breached and suffer less harm when breaches do occur. A simple approach to improving resilience is by maintaining secure and up-to-date backups so that an attack will not result in the permanent loss of data. In the case of a cyberattack on Papworth Hospital in 2016, a ransomware infection fortuitously happened just after the daily backup, so no data were lost.[25] More generally, good cybersecurity should be incorporated into the design of new IT projects from the outset and should be inherent in all healthcare systems. Security that is bolted on, or worse still, thought about only after a major incident is often more expensive and less effective.

Another mechanism for enhancing resilience is insurance—a rapidly growing business with global sales of $2.75bn in 2015.[26]

The rising costs might cause insurance companies to tread with caution in future, but the right insurance regime can drive improvements by providing financial incentives for organisations to take better care of themselves. Healthcare providers need to find cost effective ways to protect themselves against the potentially crippling costs of cyberattacks, in much the same way as they do with the costs of clinical negligence. Cybersecurity can be further bolstered by national support for incident management, organisational preparedness, and threat advice. The mechanisms for providing such support are beginning to emerge—for example, the CareCERT initiative the UK.[27]

In addition to strengthening resilience, we need to develop common security standards that are relevant to the healthcare sector. Many general standards exist for cybersecurity, such as the CIS Critical Controls,[28] NIST 800-53,[29] and ISO27001.[30] The UK National Cyber Security Centre offers expert guidance on how organisations can protect themselves and grow resilience, including their "10 steps to cybersecurity" (box 2).[31]

These principles are linked to the UK government's Cyber Essentials Scheme, which provides guidance and an entry level assurance framework to help mitigate common risks.[32] Standards are only helpful if they are relevant and are used. Currently, no standards are specifically designed for the healthcare sector and none is routinely or consistently applied. Fragmented governance, huge interconnectivity, widespread access, the lack of regulatory pressure on security, and limited resources indicate a need for healthcare specific cybersecurity standards and solutions.

US Congress recently established a task force to assess how the healthcare sector can protect itself from cyberattack, streamline its leadership and create incentives for organisations to update their networks.[33] For the NHS to apply these lessons, NHS Digital must take ownership and responsibility, deploying practices well established in other industries, such as penetration testing, and developing sector specific standards so that local resilience can be objectively measured, assessed, and benchmarked. Moreover, it must develop a national prevention strategy, consider introducing a centralised "cash for clunkers" programme to provide organisations with additional funding or incentives to replace outdated hardware and systems, and be empowered to create and mandate local and national response plans for cyber major incidents. Cybersecurity preparedness and resilience must also be integrated into local and national quality metrics—for example, through the Care Quality Commission, to drive improvements and to explicitly hold local and national leaders to account.

Conclusions

The healthcare sector is complex, fragmented, and chronically short of resources, yet it holds large amounts of sensitive and valuable data in vulnerable systems. Cybersecurity is not just about protecting data; it is fundamental for maintaining the safety, privacy, and trust of patients. Effective cybersecurity must become an integral part of healthcare systems, a pillar of regulation, and the subject of future research strategies. We must urgently develop practical standards and solutions that are specific to the healthcare sector, agree clear lines of responsibility and governance, and commit appropriate resources to the provision of adequate security.

Contributors and sources: Guy Martin is a surgeon and clinical research fellow in the department of surgery at Imperial College London. James Kinross is a surgeon and senior lecturer in the department of surgery at Imperial College. Paul Martin is honorary principal research fellow at the Institute for Security Science and Technology at Imperial College London and adviser to Context Information Security. Chris Hankin is the director of the Institute for Security Science and Technology and professor of computing science at Imperial College London. Ara Darzi is the Paul Hamlyn chair of surgery at Imperial College London. James Kinross, the corresponding author is the guarantor of the article.

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

1 Institute of Medicine. *Crossing the Quality Chasm: A New Health System for the 21st Century*. National Academies Press, 2001.
2 Center for Strategic and International Studies and McAfee. The global cost of cybercrime: economic impact of cybercrime II. 2014. https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf
3 KPMG. Health care and cyber security: increasing threats require increased capabilities. 2015. https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf
4 Institute for Critical Infrastructure Technology. Hacking healthcare in 2016: lessons the healthcare industry can learn from the OPM breach. 2016. http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf.
5 TrapX Security Inc. Health care cyber breach research report for 2016. 2017. http://deceive.trapx.com/rs/929-JEW-675/images/Research_Paper_TrapX_Health_Care.pdf
6 Abelson R, Goldstein M. Anthem hacking points to security vulnerabilities of healthcare industry. *New York Times* 2015.http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0
7 Scott M, Wingfield N. Hacking attack has security experts scrambling to contain fallout. *New York Times* 2017. https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html.
8 Winton R. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. *Los Angeles Times* 2016.http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
9 Mansfield-Devine S. In brief. *Comput Fraud Secur* 2016;358:4doi:10.1016/S1361-3723(16)30097-5.
10 Evenstad L. No NHS trust recovers after cyber attack. *Comput Wkly* 2016.http://www.computerweekly.com/news/450402278/NHS-trust-recovers-after-cyber-attack.
11 Cyber Security Intelligence. Easy: hackers taken down a hospital. 2016.https://www.cybersecurityintelligence.com/blog/easy-hackers-take-down-a-hospital-1566.html.
12 Mansfield-Devine S. Ransomware: taking businesses hostage. *Netw Secur* 2016;358:8-17.
13 Australian Red Cross Blood Service. Press Release 2016. http://www.donateblood.com.au/media/news/blood-service-apologises-donor-data-leak
14 BBC. Wiggns and Froome medical recrds released by "Russian hackers." 2016.http://www.bbc.co.uk/news/world-37369705.
15 Sengupta K. Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images. *Independent* 2017.http://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html
16 Mai H, Speyer B. Banking and technology snapshot: digital economy and structural change. 2012. https://www.dbresearch.com/PROD/DBR_INTERNET_ENPROD/PROD0000000000299039.pdf
17 Millman R. Nine in 10 NHS trusts still use Windows XP. *ITPro* 2016.http://www.itpro.co.uk/public-sector/27740/nine-in-10-nhs-trusts-still-use-windows-xp
18 Finkle J. Johnson and Johnson letter on cyber bug in insluin pump. *Reuters* 2016.http://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-t-idUKKCN12414G.
19 Parmar A. Hacker shows off vulnerabilities of wireless insulin pumps. MedCity News. 2012.http://medcitynews.com/2012/03/hacker-shows-off-vulnerabilities-of-wireless-insulin-pumps/.
20 Food and Drug Administration. Cybersecurity. 2016.http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm
21 Finkle J. New rules for avoiding cyber bugs in medical devices. *Sci Am* 2016.https://www.scientificamerican.com/article/new-rules-for-avoiding-cyber-bugs-in-medical-devices/
22 Information Commissioner's Office. Overview of the General Data Protection Regulation (GDPR). 2017. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.
23 Papoutsi C, Reed JE, Marston C, Lewis R, Majeed A, Bell D. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. *BMC Med Inform Decis Mak* 2015;358:86.. doi:10.1186/s12911-015-0202-2 pmid:26466787.
24 National Data Guardian. Review of data security, consent and opt-outs. 2016. https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs
25 Muncaster P. NHS Trust suspends operations after major cyber incident. Infosecurity. 2016.http://www.infosecurity-magazine.com/news/nhs-trust-suspends-operations/ .
26 PriceWaterhouseCoopers. Insurance 2020: reaping the dividends of cyber resiliance. 2016. http://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html
27 Mansfield-Devine S. New NHS security services. *Comput Fraud Secur* 2016;358:3doi:10.1016/S1361-3723(16)30067-7.
28 Centre for Internet Security. Critical Security Controls version6.1. 2017. https://www.cisecurity.org/controls/
29 National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity. 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
30 International Organisation for Standardisation. ISO 27001:2013. 2013. https://www.iso.org/standard/54534.html
31 National Cyber Security Centre. 10 steps to cyber security. 2016. https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
32 Her Majesty's Goverment (HMG). Cyber essentials. 2015. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
33 Healthcare Industry Cybersecurity Task Force. Improving cybersecurity in the healthcare industry. 2017. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf?mod=djemCybersecruityPro&tpl=cy

Box 2: Key steps to improving cybersecurity and resilience[31]

Set up a risk management regime—Assess the risks to your organisation as you would for financial, clinical, or operational risks. Embed cybersecurity in risk management processes across the organisation

Network security—Defend your networks and filter out unauthorised access or malicious content; for example, through use of firewalls and intrusion detection systems

Malware prevention—Establish effective anti-malware defences

User education and awareness—Produce a cybersecurity policy and ensure that it corresponds with staff training. Cybersecurity and risk awareness should be mandatory in the same way as for information governance, fire safety, and child protection training

Removable media controls—Control or limit access to removable media (such as memory sticks) and scan all media for malware before allowing access to systems. Consider whether there is a need to allow any access; for example by blocking ports

Secure configuration—ensure all relevant patches and updates are applied and that hardware and software are regularly updated

Home and mobile working—Develop a secure mobile working policy and train staff to follow it. Remember that data need to be protected both in transit and off site, and special consideration must be given to patients and staff accessing medical records remotely

Incident management—Establish a robust incident response and disaster recovery capability to ensure safe care can be delivered in the event of an attack. Report all incidents to the relevant authorities

Monitoring—Continuously monitor all systems and networks and look for unusual activity that may indicate an attack is in process

User privileges—Control access and limit user privileges to essential systems whenever practical and ensure that regular activity log audits are made

Key messages

The threat of cyberattacks on healthcare is real and growing

Good security means more than just protecting data. We face the potential for large scale disruption to the delivery of care, making cybersecurity a fundamental patient safety consideration

Cybersecurity in healthcare is a huge challenge, but organisations and individuals can take practical steps to protect themselves and their patients

We urgently need healthcare specific standards and best practice, backed by firm regulation, sufficient resources, and clear lines of responsibility