CYBER SECURITY AND HEALTHCARE: HOW SAFE ARE WE?

Journal:	*BMJ*
Manuscript ID	BMJ.2017.039662
Article Type:	Specialist Review
BMJ Journal:	BMJ
Date Submitted by the Author:	30-May-2017
Complete List of Authors:	Martin, Guy; Imperial College London, Departmemt of Surgery and Cancer Martin, Paul; Imperial College London, Institute for Security Science and Technology Hankin, Chris; Imperial College London, Institute for Security Science and Technology Darzi, Ara; Imperial College London, Kinross, James; Imperial College London, Division of Surgery
Keywords:	cyber security, patient safety, digital health, mobile health, electronic health records, data protection

CYBER SECURITY AND HEALTHCARE: HOW SAFE ARE WE?

Mr. Guy Martin[1] Clinical Research Fellow

Dr. Paul Martin[2] Honorary Principal Research Fellow

Prof. Chris Hankin[2] Director of the Institute for Security Science & Technology

Prof. Ara Darzi[1] Director of the Institute of Global Health Innovation

Mr. James Kinross[1] Senior Lecturer in Surgery

1. Department of Surgery and Cancer, Faculty of Medicine, 10th Floor, QEQM Building, St. Mary's Hospital, London W2 1NY
2. Institute for Security Science and Technology, Level 2 Admin Office, Central Library Imperial College London, South Kensington Campus, London SW7 2AZ

Corresponding Author: James Kinross

Senior Lecturer in Colorectal Surgery

Department of Surgery and Cancer,

Imperial College London,

10th Floor, QEQM Building, St. Mary's Hospital,

Praed Street,

London W2 1NY

+44(0) 7989 344238

j.kinross@imperial.ac.uk

Funders: No funding was provided for this work.

Word Count: 2,083

The advent of the digital era in healthcare holds great promise, but this could be undermined if weaknesses in cyber security are allowed to jeopardise patient safety and privacy.

INTRODUCTION

Healthcare systems around the world have rightly identified the vast potential for digital technology to improve clinical outcomes and transform the delivery of healthcare[1]. Some nations have made concerted attempts to legislate for healthcare cybersecurity [2], however, cyber risk has been largely underestimated and the majority of global health systems remain vulnerable to attack. The recent WannaCry malware attack, which disrupted significant parts of the National Health Service (NHS) in the UK, has once again highlighted cybersecurity as a critical patient safety issue. Patients, clinicians and institutions are now more integrated than ever before and increasingly dependent on shared health data. Here, the growing cyber security risks to healthcare are reviewed and future needs for effective cyber defence identified.

MAIN TEXT

Cyber crime – a universal challenge

Cyber attacks usually steal money, data or intellectual property, although increasingly the aim is to cause overt disruption or political impact. Cyber crimes are often transnational and attributing them to individuals can be difficult. Increasingly they are state sponsored and highly sophisticated. Many go 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 total cost of cyber crime globally in 2014 was estimated to be up to $575 billon[3].

Cyber crime and healthcare

Healthcare faces even larger cyber risks than other sectors because of inherent weaknesses in its security posture - *Figure 1* - and is one of the most targeted sectors globally; 81% of organisations surveyed and >110 million patients in the US had their data compromised in 2015 alone[4,5]. Only half of providers feel they are capable of defending themselves from cyberattack, and there has been a 300% increase in attacks in the past three years[4,6], For the criminals and foreign states who are 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 *Figure 2.*

Cyber security is intended to protect the Confidentiality, Integrity and Availability (CIA) of data. For healthcare, *Confidentiality* is about ensuring that sensitive information, especially identifiable data, does not reach the wrong people and that patient privacy is maintained. In 2015, for example, criminals stole 80 million personal records from the US health insurance company Anthem. Individual medical records are traded on the Dark Web for around $50, giving the breach a market value of a billion dollars or more[7]. 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[5]. Unlike credit cards, these identifiers cannot be reset, and an individual's health record may contain enough information to open bank accounts, obtain loans or acquire a passport. *Integrity* is about ensuring the accuracy and trustworthiness of data, whilst *Availability* is about maintaining reliable access to the data and the systems used to process and store it; these often come hand-in-hand as we seen in the recent WannaCry attack.

The fallout from the WannaCry ransomware attack is still settling, although it has so far reportedly affected around 200,000 systems in more than 150 countries[8]. Around 50 hospitals in the UK were directly affected, and many more pre-emptively shut down their computer systems resulting in significant disruption - affecting care delivery, compromising patient safety, and potentially eroding trust. The attack used a prevalent type of malware

known as ransomware, which creates encrypted copies of data before deleting the originals. The only way to regain access to the infected computer and the data is to pay the Bitcoin ransom, or wipe the system and retrieve a backup copy. The WannaCry attack, though hugely disruptive, did not specifically target the healthcare sector; however, this has not always been the case. In 2016 a ransomeware attack on the Hollywood Presbyterian Medical Center in Los Angeles shut down its network for 10 days, preventing staff from accessing medical records or using medical equipment until the hospital paid the ransom (reportedly a mere 40 Bitcoins, or about $17,000)[10]. It is thought that the infection took place when an employee clicked on an attachment to a 'phishing' email and unwittingly downloaded the ransomware. Phishing emails are the commonest means of delivering malware and hard to defend against. Even in security conscious organisations, the click rate on well-crafted phishing emails can be up to 30%[5]. Ransomware has previously affected other hospitals: one English hospital was forced to cancel all operations and transfer patients for two days following an attack in 2016[11,12], whilst Boston Children's Hospital and hospitals in Germany have also been targeted[13]. Two Freedom of Information (FOI) requests in the UK found that in 2015-16 up to half of NHS Trusts were hit by ransomware the preceding year[10]. It is telling that despite these well publicised attacks, and the availability of security patches for known vulnerabilities, the warnings went largely unheeded, resulting in the significant disruption caused by WannaCry.

Healthcare data is usually stolen or ransomed for money. However, some incidents have no obvious financial motive. In 2016, the Australian Red Cross Blood Service suffered a major breach in which 1.28 million records containing large amounts of sensitive information, including donors' high-risk sexual activity were dumped on a public website[11]. Cyberattacks may also be used to create overt political impact – most notably in the recent attacks against the World Anti-Doping Agency (WADA), in which the medical records of prominent athletes were release[14]. More recently ISIL-linked hackers have directly targeted

NHS websites for propaganda purposes[15]. It is easy to imagine other scenarios in which high-profile individuals are targeted in order to damage reputations or potentially worse.

Why is healthcare so vulnerable?

The vulnerability of the healthcare sector to cyberattack reflects a combination of factors, notably limited resource, fragmented governance and culture[16]. Compared with other sectors such as financial services, healthcare has chronically under-invested in IT infrastructure. Many NHS organisations spend as little as 1-2% of their annual budget on IT, compared to 4-10% in other critical sectors[17], and many run on multiple legacy systems that are no longer supported with security updates. Indicative of this low level of investment, in the UK, the majority of NHS trusts are still, to some extent, using Windows XP, an operating system that Microsoft ceased to support in 2014[18].

It is not only the outdated infrastructure that creates vulnerabilities: cyber security experts are in very 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, ranging from national organisations to individual GP surgeries, all of which have their own governance structures. In the UK, at least, there is a lack of clear accountability and responsibility for cyber security at a national level, for what is evidently a national problem. Finally, the culture of healthcare understandably focuses on the core mission of caring for patients, even at the expense of security. One symptom of this patient-first culture is the widespread sharing of passwords and IT credentials – a practice that undermines security, but nonetheless makes sense.

What does the future hold?

So far, attacks on healthcare have principally been for the purpose of financial gain, and there have been no significant cases in which the integrity of healthcare data is known to

have been compromised. However, we face the real prospect that, intentionally or unwittingly, the integrity of healthcare data will be compromised. Consider, for example, the harm that could be caused by altering blood groups, test results or imaging reports.

Another worrying prospect is that of malicious cyberattacks on medical devices. As long ago as 2014, more than 300 medical devices were identified as being at risk [5]. In 2016 Johnson & Johnson warned patients of a vulnerability that could allow hackers to take control of the Animas OneTouch insulin pump [19], whilst Barnaby Jack, a well-known hacker, demonstrated how he could remotely control a Medtronic insulin pump to deliver a lethal insulin dose[20]. Risks such as these seem set to increase with the rapid growth in consumer, wearable and mobile technologies[5,21,22].

In addition to patient safety, there are significant financial and reputational risks for healthcare arising from poor cyber security. Every European institution, including healthcare providers, should be thinking about the implications of the General Data Protection Regulation (GDPR) which comes into effect in 2018. Among other things, GDPR makes it mandatory to report security breaches within 72 hours, and non-compliance can result in a fine of up to €20 million or 4% of annual global turnover[23]. In the UK to date there has been little guidance or leadership on how organisations can meet these responsibilities in practice. Another worry, beyond fines and legal action, is that large-scale compromises of patient data might undermine public confidence, making patients more reluctant to share their data with clinicians or researchers[24,25].

What can the healthcare sector do?

Cyber security can never be 100% effective, and the threat to healthcare is an unavoidable new reality. However, there are many practical steps that individuals and organisations can take to protect themselves and reduce the likelihood or impact of an attack.

An ultimate aim of cyber security 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, up-to-date and retrievable backups, so that an attack will not result in the permanent loss of data. In the case of a cyberattack on Papworth Hospital in the UK in 2016, a ransomware infection fortuitously happened just after the daily backup and so no data was lost[26]. More generally, good cyber security should be designed-in from the outset of new IT projects. Security that is bolted-on at the end is often more expensive and less effective. Systems can also be designed to make them inherently more secure –, for example, by assembling the 'full picture' only when it is needed for direct care.[27]. Security should be inherent in healthcare systems, not retrofitted or, worse still, thought about for the first time only after a major incident.

Another mechanism for enhancing resilience is insurance. Cyber security insurance is a rapidly growing business with global sales of $2.75 billion in 2015[28]. The rising cost of cyberattacks might cause insurance companies to tread with more caution in future. Nonetheless, the right insurance regime can drive improvements in cyber security 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 enormous costs of cyberattacks, in much the same way as they do with clinical negligence costs. Cyber security can be further bolstered by nationally driven support for incident management, organisational preparedness, threat advice and the dissemination of best practice. The mechanisms for providing such support are beginning to emerge – for example the CareCERT initiative the UK [29].

In addition to strengthening resilience, there is a need to develop common security standards that are relevant to the healthcare sector. There is a plethora of general standards for cyber security, such as the CIS Critical Controls[30], NIST 800-53[31] and ISO27001[32]. The UK

National Cyber Security Centre (NCSC) offers expert advice and guidance on how organisations can protect themselves and grow resilience; the elements of their *"10 Steps to Cyber Security"* that are most relevant to healthcare are seen in *Figure 3*. These principles are linked to the UK Government's Cyber Essentials Scheme, which provides guidance, together with an entry level assurance framework to help mitigate common risks[33].

Standards are only helpful if they are relevant and they are used. Currently, none of the standards are specifically designed for the unique context of healthcare and none are routinely or consistently applied across the sector. Fragmented governance, huge inter-connectivity, the requirement for widespread access, the lack of regulatory pressure on security, and lack of resource all suggest a need for a healthcare-specific standard for cyber security. Identifying effective cyber security as a fundamental patient safety issue, and applying consistent standards of regulation and assurance, could greatly improve the protection of patients and their data.

CONCLUSION

The healthcare sector is complex, fragmented and chronically short of human and financial resources, yet it holds large amounts of sensitive and valuable data in systems that are increasingly critical for the safe provision of patient care. Cyber security is not just about protecting data; it is fundamental to the safety and privacy of patients, and to maintaining their trust. Cyber security must become an integral part of any digital transformation policy, a pillar of healthcare regulation, and the subject of future patient safety research strategies. There is a pressing need to develop practical standards that are specific to the healthcare sector, agree clear lines of responsibility and governance, and commit appropriate resources to the provision of adequate security. Cyber threats are an unavoidable reality and the risk is increasing. It is imperative that these threats are identified, monitored and tackled as part of a coordinated global response.

KEY MESSAGES

- The threat from cyberattacks on healthcare is real and growing
- Good security means more than just protecting data. We now face the potential for large scale disruption to the delivery care, making cyber security a fundamental aspect of patient safety
- Cyber security in healthcare is a huge challenge, but there are practical steps that organisations and individuals can take to protect themselves and their patients
- There is a pressing need for healthcare specific standards and best practice, backed by firm regulation, sufficient resources and clear lines of responsibility

CONTRIBUTORS AND SOURCES

James Kinross, the corresponding author is the guarantor of the article.

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 & Technology at Imperial College London and adviser to Context Information Security. Chris Hankin is the Director of the Institute for Security Science & Technology and Professor of Computing Science at Imperial College London. Ara Darzi is the Paul Hamlyn Chair of Surgery at Imperial College London.

CONFLICTS OF INTEREST

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

LICENCE

I "*James Kinross",* The Corresponding Author of this article contained within the original manuscript which includes any diagrams & photographs within and any related or stand-alone film submitted (the Contribution") has the right to grant on behalf of all authors and does grant on behalf of all authors, a licence to the BMJ Publishing Group Ltd and its licencees, to permit this Contribution (if accepted) to be published in the BMJ and any other BMJ Group products and to exploit all subsidiary rights, as set out in our licence set out at: http://www.bmj.com/about-bmj/resources-authors/forms-policies-and-checklists/copyright-open-access-and-permission-reuse."

I am one author signing on behalf of all co-owners of the Contribution.

The Contribution has been made in the course of my employment and I am signing as authorised by my employer.

REFERENCES

1 Institute of Medicine. *Crossing the Quality Chasm: A New Health System for the 21st Century.* National Academies Press, Washington 2001.

2 Luna R, Rhine E, Myhra M, *et al.* Cyber threats to health information systems: a systematic review. *Technol Heal Care* 2016;**24**:1–9. doi:10.3233/THC-151102

3 Center for Strategic and International Studies. The global cost of cybercrome: economic impact of cybercrime II. 2014.

4 KPMG. Health care and cyber security: imcreasing threats require increased capabilities. 2015. https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf

5 Institute for Critical Infrastructure Technology. Hacking healthcare in 2016: lessons the healthcare industry can learn from the OPM breach. 2016.

6 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

7 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

8 Scott M, Wingfield N. Hacking attack has security experts scarmbling to contain fallout. New York Times. 2017.

9 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

10 Mansfield-Devin S. Ransomware: taking buisnesses hostage. *Netw Secur* 2016;:8–17.

11 Mansfield-Devin S. In brief. *Comput Fraud Secur* 2016;:4.

12 Evenstad L. No NHS trust recovers after cyber attack. Comput. Wkly.

2016.http://www.computerweekly.com/news/450402278/NHS-trust-recovers-after-cyber-attack (accessed 21 Dec2016).

13 Cyber Security Intelligence. Easy:hackers taken down a hospital. 2016.https://www.cybersecurityintelligence.com/blog/easy-hackers-take-down-a-hospital-1566.html (accessed 1 Jun2016).

14 BBC. Wiggns and Froome medical recrds released by 'Russian hackers'. 2016.http://www.bbc.co.uk/news/world-37369705 (accessed 21 Dec2016).

15 Sengupta K. Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images. Indep. 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 Kruse C, Frederick B, Jacobson T, *et al.* Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Heal Care* 2017;**25**:1–10. doi:10.3233/THC-161263

17 Mai H, Speyer B. Banking & technology snapshot: digital economy and structural change. 2012. https://www.dbresearch.com/PROD/DBR_INTERNET_ENPROD/PROD0000000000299039.pdf

18 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 (accessed 21 Dec2016).

19 Finkle J. Johnson & Johnson letter on cyber bug in insluin pump. Reuters. 2016.http://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-t-idUKKCN12414G (accessed 21 Dec2016).

20 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/ (accessed 26 Jan2017).

21 Food and Drug Administration. Cybersecurity.

2016.http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm (accessed 6 Jan2017).

22 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/

23 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/ (accessed 22 May2017).

24 Caldicott F. Review of Data Security, Consent and Opt-Outs National Data Guardian. 2016.

25 Papoutsi C, Reed J, Marston C, *et al.* 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;**15**:86. doi:10.1186/s12911-015-0202-2

26 Muncaster P. NHS Trust suspends operations after major cyber incident. Infosecurity. 2016.http://www.infosecurity-magazine.com/news/nhs-trust-suspends-operations/ (accessed 21 Dec2016).

27 Kocabas O, Soyata T. Medical data analytics in the cloud using homomorphic encryption. In: Raj P, Deka G, eds. *Handbook of Reserach on Cloud Infrastructure for Big Data Analytics*. IGI Global 2014.

28 PriceWaterhouseCoopers. Insurance 2020: reaping the dividends of cyber resiliance. 2016.

29 Mansfield-Devin S. New NHS security services. *Comput Fraud Secur* 2016;:3.

30 Centre for Internet Security. Critical Security Controlvs V6.1. 2017.

31 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

32 International Organisation for Standardisation. ISO 27001:2013. 2013.

33 Her Majesty's Goverment (HMG). Cyber Essentials. 2015.

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

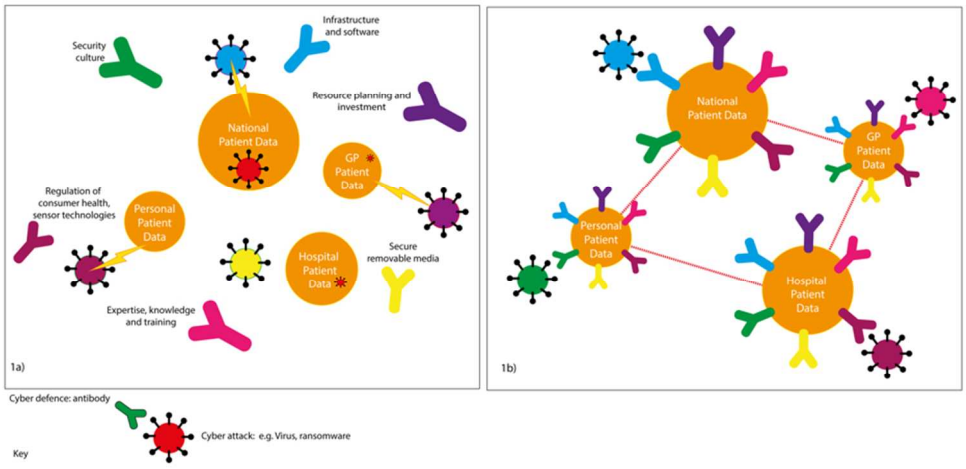

Figure 1 – current weaknesses and future solutions for effective cyber security in healthcare are analogous to the immune system. Current threats are varied and diverse and inevitably lead to infections. An effective response requires in-built resilience, a coordinated defence with clear responsibilities and expert assistance.

Data theft for financial gain– stealing of personal data for the purposes of monetary gain (e.g. names, addresses, social security details, financial information)
Data theft for impact – theft and public release of sensitive medical information (e.g. celebrities, politicians or other high profile individuals)
Ransomware – using malware to block users from their data or systems or delete data unless a fee is paid
Data corruption – deliberate corruption of data (e.g. altering of 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 (e.g. obtaining fraudulent payments or personal information)
The unwitting insider – significant disruption to systems or the loss of data due to the unintentional actions of staff using outdated and at-risk systems

Figure 2 – common and emerging cyber threats in healthcare

Set up a risk management regime – assess the risks to your organisation as you would for financial, clinical or operational risk. Embed cyber in risk management processes across the organisation
Network security – defend your networks and filter out unauthorised access or malicious content e.g. through use of firewalls and intrusion detection systems
Malware prevention – establish effective anti-malware defences
User education and awareness – produce a cyber security policy, and ensure this goes hand-in-hand with staff training. Cyber security 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 (e.g. memory sticks), and scan all media for malware before allowing access to systems. Consider whether there is a need to allow any access e.g. by blocking ports
Secure configuration – ensure all relevant patches and updates are applied, and ensure regular updates to both hardware and software
Home and mobile working – develop a secure mobile working policy and train staff to follow it. Remember that data needs 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 whilst ensuring there are regular activity log audits

Figure 3 – key steps that healthcare organisations and individuals can take to improve their cyber security and resilience[24]