CYBER SECURITY AND HEALTHCARE: HOW SAFE ARE WE?

Journal:	*BMJ*
Manuscript ID	BMJ.2017.038003
Article Type:	Analysis
BMJ Journal:	BMJ
Date Submitted by the Author:	14-Feb-2017
Complete List of Authors:	Martin, Guy; Imperial College London, Departmemt of Surgery and Cancer Kinross, James; Imperial College London, Division of Surgery 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,
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

Mr. James Kinross[1] Senior Lecturer in Surgery

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

1. Department of surgery and Cancer, Faculty of Medicine, 10th Floor, QEQMW 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, QEQMW, 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.

The advent of the digital era in healthcare holds great promise, but this could be undermined if weaknesses in cyber security 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 to transform the delivery of healthcare[1]. In the rush to digitise serious security risks have been overlooked and the majority of electronic health systems remain potentially vulnerable to attack. This critical patient safety issue is now of global importance as patients, clinicians and institutions become ever more integrated and dependent on shared access to health data. Here the growing cyber security threats to healthcare are reviewed and future directions for the digital evolution of cyberdefence in health care are outlined with practical examples of how individuals and organisations can protect themselves.

MAIN TEXT

Cyber crime – a universal challenge

The purpose of cyber attacks is usually to steal money, data or intellectual property, although in a growing number of cases the aim is to cause overt disruption or political effect. Cyber crimes are often transnational, and attributing them to individuals is difficult. Increasingly they are state sponsored and highly sophisticated. The majority go undetected or unreported, and only a small minority enter the public domain; among the best-known recent examples are the major breaches at TalkTalk, Mossack Fonseca, The US Democratic National Committee, The US Office of Personnel Management and Yahoo. The total cost of cyber crime globally in 2014 was estimated to be up to $575 billon[2].

Cyber crime and healthcare

Healthcare faces even larger cyber risks than other sectors because of inherent weaknesses in its security posture (*Figure* 1). Healthcare is regularly identified as one of the most targeted sectors globally, with 81 per cent of healthcare organisations and more than 110 million patients in the US having had their data compromised in 2016[3]. Only half of healthcare providers feel they are capable of defending themselves from cyberattack, and there has been a 300% increase in known attacks in the past 3 years[3,4], 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 personal data and it is a soft target. The current and emerging cyber threats to healthcare are outlined in *Figure 2.*

Cyber security is intended to protect the Confidentiality, Integrity and Availability ('CIA') of data. In the context of healthcare, *Confidentiality* is about ensuring that sensitive information does not reach the wrong people and that patient privacy is maintained. In 2015 criminals stole 80 million sets of personal records from the US health insurance company Anthem. Individual medical records are traded on the Dark Web for around $50 each, giving the breach a value of a billion dollars or more[5]. Medical records are worth much more on the black market than credit card details because they contain multiple permanent identifiers, together with financial and sensitive personal information[6]. Unlike credit card details, these identifiers cannot be reset, and an individual's health record contains 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. A growing number of cyberattacks are affecting availability as well as confidentiality. For example, in 2016 an 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. This attack used a common type of malicious software (malware) known as ransomware which encrypts

the victim's data, effectively putting it beyond use. The attackers promise to unlock the data if the victim pays a ransom, usually in the form of crypto-currencies such as Bitcoin. In this case, the hospital authorities paid the ransom (reportedly a mere 40 Bitcoins, or about $17,000) and got their hospital back. Thankfully, no one came to significant harm [10]. It is thought that the infection probably took place when an employee clicked on an attachment to a 'phishing' email, unwittingly downloading ransomware onto the system. 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%[6]. Ransomware has also affected several hospitals in the UK. One NHS Trust was forced to cancel all operations and transfer high-risk patients to other hospitals for two days following an attack in 2016[9,10]. Other similar cases include attacks on the Boston Children's Hospital and hospitals in Germany[11]. Two Freedom of Information (FOI) requests in the UK found that in 2015-16 up to half of NHS Trusts were hit by ransomware during the preceding year[8].

Healthcare data is usually stolen to sell or encrypted for ransom. However, some incidents have no financial motive. In 2016, the Australian Red Cross Blood Service suffered a major breach in which 1.28 million donor records were dumped on a public website. The records contained large amounts of sensitive personal information, including whether donors had engaged in high-risk sexual activities[9]. Cyberattacks may also be used to create overt political effects – most notably in the 2016 attacks against the World Anti-Doping Agency (WADA), in which the medical records of prominent athletes were released following an attack attributed to the Russian group Fancy Bear[12,13]. More recently ISIL-linked hackers have directly targeted NHS websites for propaganda purposes[14]. It is easy to imagine other scenarios in which high-profile individuals are targeted through their medical records in order to damage reputations or potentially far worse.

Why is healthcare so vulnerable?

The vulnerability of the healthcare sector to cyberattack reflects a combination of factors, notably resource constraints and fragmented governance. Compared with other potential targets, such as financial services, retail and government organisations, healthcare institutions have chronically under-invested in their IT infrastructure. Many of them run on heterogeneous legacy systems built on old technology, including some that are no longer supported with security updates. In the UK, many NHS trusts are still using Windows XP, an operating system which Microsoft ceased to support in 2014. This troubling fact emerged from FOI requests to 63 NHS Trusts, in which 90 per cent said they were still using XP[15]. It is not only creaking infrastructure that leads to 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 creating a lack of clarity over who is responsible for securing systems and data. The UK healthcare sector comprises around 10,000 distinct entities, ranging from national organisations to individual primary care surgeries, all of which have their own IT and governance structures. 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 cyber security, but nonetheless makes sense when the alternative would be delays in treatment.

What does the future hold?

So far, cyberattacks on healthcare have mainly affected the confidentiality or availability of data for the purpose of financial gain. However, we face the real prospect of cyberattacks that intentionally or unwittingly affect integrity by altering data. It takes little imagination to think of the harm that could be caused by subtly changing millions of patients' health records – for example, 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 [6]. In October 2016 Johnson & Johnson warned patients using its Animas OneTouch insulin pump of a cyber security vulnerability which could allow hackers to take control of the device[16]. Barnaby Jack, a well-known hacker, demonstrated how he could remotely control a Medtronic insulin pump to deliver a potentially lethal dose of insulin[17]. The cyber security literature contains numerous other examples of vulnerable devices including pacemakers and arterial blood gas machines; risks which are only going to increase with the rapid growth in the use of consumer and mobile health technologies[6,18,19].

In addition to the risk to patient safety, there are significant financial and reputational risks for healthcare providers. Every European institution, including the entire healthcare sector, should be thinking hard about the implications of the EU General Data Protection Regulation (GDPR), which comes into effect in May 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 euros or 4% of annual global turnover. Arguably, an even bigger worry than fines and legal action is that large-scale compromises of data would undermine public confidence in the healthcare sector, making patients reluctant to share their personal information with clinicians or researchers.

What can the healthcare sector do?

Cyber security can never be 100% effective and it therefore pays to be resilient (figure 1). Resilience is about reducing the risk by lessening the impact of a successful attack, and a straightforward way of doing this is by keeping secure and up-to-date backup copies of data so that even a serious cyberattack will not result in its permanent loss. In the case of a cyberattack on Papworth Hospital in the UK in 2016, a ransomware infection happened to take place just after the daily backup, so no data was lost[20]. More frequent backup reduces the risk. More generally, good cyber security must be designed-in from the beginning of projects to develop new systems. Security that is bolted-on at the end of a project is often

more expensive and less effective. Systems can also be designed to make them inherently more secure; for example, systems for processing sensitive patient data can be designed such that the 'full picture' is only brought together briefly when needed to provide direct patient care.[21].

Another common mechanism for enhancing resilience is insurance. Cyber security insurance is a rapidly growing business with global annual sales of $2.75 billion in 2015[22]. However, the rising cost of individual cyberattacks is causing insurance companies to tread with caution. When a single attack can result in losses of a billion dollars or more, cyber insurance starts to resemble terrorism insurance – a commercially high-risk business that requires the ultimate backing of governments. Even so, fostering the right insurance regime can drive improvements in cyber security by providing financial incentives for organisations to take better care of themselves. Healthcare organisations need to find a cost-effective way to protect themselves against the potentially crippling costs of cyberattacks, in much the same way as they currently protect themselves against clinical negligence claims. Their cyber security can be further bolstered by nationally-driven support for cyber security incident management, organisational cyber security preparedness, threat advice and the dissemination of best practice specific to healthcare. The mechanisms for providing such support are only just beginning to emerge. For example, the CareCERT initiative led by NHS Digital in the UK [23]. The UK National Cyber Security Centre (NCSC) offers expert advice and guidance on how individuals and organisations can protect themselves and grow resilience; a summary of some measures pertinent to healthcare is shown in *Figure 3.*

CONCLUSION

The cyber security sector is complex, fragmented and chronically short of human and financial resources, yet it holds large amounts of sensitive and valuable data. Cyber security is not however just about protecting data; it is fundamental to protecting the safety and privacy of patients and maintaining their trust in the healthcare system. Cyber security must

be an integral part of digital transformation policy and future patient safety research strategies. Without funding to support these activities, urgently required innovation in health cybersecurity will remain challenging as the threats to the confidentiality, integrity and availability of that data increase, along with the risk of malicious attacks on medical devices. It is now imperative that these dynamic risks are defined, monitored and tackled at both national and local levels as part of a coordinated global response.

KEY MESSAGES

- The threat from cyberattacks on healthcare is real and growing dramatically
- Good security means more than just protecting data. We now face the potential for large scale disruption of healthcare delivery, making cyber security fundamental to 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

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

3 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

4 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

5 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

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

7 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

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

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

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 (accessed 21 Dec2016).

11 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).

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

13 Cyber Security Intelligence. Making sense of cyber insurance. 2016.Making Sense Of Cyber Insurance (accessed 6 Jan2016).

14 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

15 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).

16 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).

17 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).

18 Food and Drug Administration. Cybersecurity. 2016.http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm (accessed 6 Jan2017).

19 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/

20 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).

21 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.

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

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

24 National Cyber Security Centre. 10 steps to cyber security. 2016. https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

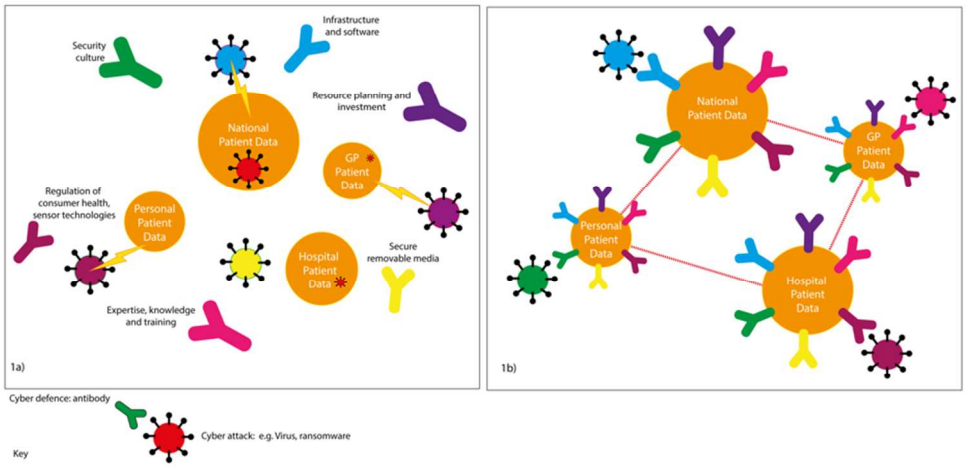

Figure 1a –the current cyber defence architecture and challenges in healthcare can be viewed in terms of the immune system. Current threats are multiple, and may take the form of e.g. ransomware attacks, viruses or trojans. The system is too large to build a security wall around, and thus defence architecture is typically non-specific and poorly coordinated across the global healthcare system. This problem is magnified because there is vulnerability at multiple points of access, and inevitably there are breaches with invasion of foreign agents (such as a Trojan) into theoretically closed systems. Like a biological virus, these agents may lie dormant until activated by the aggressor, and these attacks may also be coordinated in a systematic fashion. 3b - Future health cybersecurity requires a systems level response that allows not only a coordinated defence with communication between healthcare providers, but also resilience at a local level to multiple threat types. Current defensive approaches must therefore be deployed robustly across all types of data or digital devices, and protection must be bespoke to the needs of the patient and clinicians interacting with digital technologies or data sets.

Data theft for financial gain– stealing of personal data for the purposes of monetary gain (e.g. names, addresses, social security details)
Data theft for impact – theft and public release of sensitive medical information (e.g. celebrities or politicians)
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)

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