Maturitas 113 (2018) 48–52

Contents lists available at ScienceDirect

Maturitas

journal homepage: www.elsevier.com/locate/maturitas

Cybersecurity in healthcare: A narrative review of trends, threats and ways forward

Lynne Coventry*, Dawn Branley

Northumbria University, Newcastle upon Tyne, UK

ARTICLE INFO

Keywords:
Cybersecurity
Medical devices
Electronic health record

ABSTRACT

Electronic healthcare technology is prevalent around the world and creates huge potential to improve clinical outcomes and transform care delivery. However, there are increasing concerns relating to the security of healthcare data and devices. Increased connectivity to existing computer networks has exposed medical devices to new cybersecurity vulnerabilities. Healthcare is an attractive target for cybercrime for two fundamental reasons: it is a rich source of valuable data and its defences are weak. Cybersecurity breaches include stealing health information and ransomware attacks on hospitals, and could include attacks on implanted medical devices. Breaches can reduce patient trust, cripple health systems and threaten human life. Ultimately, cybersecurity is critical to patient safety, yet has historically been lax. New legislation and regulations are in place to facilitate change. This requires cybersecurity to become an integral part of patient safety. Changes are required to human behaviour, technology and processes as part of a holistic solution.

1. Introduction

Healthcare technologies have the potential to extend, save and enhance lives. Technologies range from those providing storage of electronic health records (EHRs); devices that monitor health and deliver medication (including general purpose devices and wearables, and technology embedded within the human body); to telemedicine technology delivering care remotely – even across countries. Patients increasingly use their own mobile applications, which can now be integrated with telemedicine/telehealth into the medical Internet of Things [1] for collaborative disease management and care coordination.

As healthcare devices continue to evolve, so does their interconnectivity. Whilst traditionally standalone, many are now integrated into the hospital network. There are currently 10–15 connected devices per bed in US hospitals [2]. Interconnection has many benefits—e.g., efficiency, error reduction, automation and remote monitoring. These benefits are transforming the treatment of both acute and chronic long-term conditions. Interconnected technology outside of the clinical environment allow health professionals to monitor and adjust implanted devices without the need for a hospital visit or invasive procedures. EHRs can improve patient care by making health information more broadly available [3]. Unfortunately, interconnection introduces new cybersecurity vulnerabilities. Cybersecurity is concerned with safeguarding computer networks and the information they contain from penetration and accidental or malicious disruption. There are growing concerns that cybersecurity within healthcare is not sufficient and this has already resulted in a lack of medical information confidentiality [4] and integrity of data [5,6].

Of course, privacy breaches were a concern prior to the emergence of digital health records. However, the interconnectivity of today's records provides multiple potential gateways to access; the ability to access remotely (whereas historically paper records would have been safeguarded within hospitals and only accessible via physical breaches); the ability for data theft to go unnoticed; and access to a more complete health record providing a more valuable resource for potential attacks (whereas previously health records may have been split between many different hospital(s)/departments). Historically, misplaced paper records or a stolen laptop may have exposed hundreds or thousands of patients to a potential date breach, now that this information is electronic and available on numerous networks, a privacy breach has the potential to affect millions of people [7]. To illustrate further, celebrity health records have always been a target for breaches [8]. However prior to the emergence of electronic records, these breaches were limited to hospital staff who could gain access to the physical paperwork. Now celebrity health records can be potentially remotely accessed—increasing the potential for breaches. That said, electronic records also have a key privacy benefit over paper records—the ability to track staff access (a recent report suggests that over half of healthcare breaches come from inside the organisation [8]). Whereas previously it

* Corresponding author at: 153 Northumberland Building, Northumbria University, Newcastle upon Tyne, NE1 8ST, UK.
E-mail address: Lynne.coventry@northumbria.ac.uk (L. Coventry).

https://doi.org/10.1016/j.maturitas.2018.04.008
Received 2 March 2018; Received in revised form 16 April 2018; Accepted 18 April 2018

could be difficult to detect who had a 'sneak peek' at paper medical records, it is often easier to track who has accessed electronic records. Although there are ways around this for more sophisticated/external attackers.

As illustrated by breaches reported in the media, cybersecurity vulnerabilities are being exploited. Healthcare is currently one of the most targeted sectors. Reports highlight the growth of attacks and the rise in medical identity theft—with millions of medical records stolen globally [9–12]. Breaches can arise from hacking, malware and insider threats. Hacking is defined as unauthorised access to a computer system to gain information or cause disruption [13]. Malware ("malicious software") refers to programs designed to infiltrate computers without users' consent and includes threats such as viruses and ransomware. While insider threats are issues created by the mistakes or deliberate actions of staff (e.g., responding to phishing emails—a social engineering attack to extract login credentials or to launch a malware attack, erroneous security settings, misuse of passwords, losing laptops and sending unencrypted emails).

The aim of this narrative review is to explore the following questions:

1. Why is healthcare vulnerable?
2. Why is healthcare targeted?
3. What threats and consequences is healthcare currently experiencing?
4. What is the role of legislation and standards?
5. How can the healthcare sector move forward?

2. Method

2.1. Data sources and search strategy

The PubMed database was searched for full text, English language, peer-reviewed articles from April 2012 to April 2018. The keywords used were cybersecurity and healthcare. This returned 2475 hits. Since cybersecurity is constantly changing; this was changed to 2014–2018 which reduced the return to 1249 articles. The bibliographies of key texts were then used to source further articles.

Article titles and abstracts were screened by the principal researcher. Articles were retained where there was evidence of cybersecurity issues, clear implications for healthcare settings, organisational practice, individual practice or health technology development. Also included were systematic reviews regarding the education and behaviour of healthcare workers. Security research papers exploring future technological solutions were excluded as were articles relating to medical research. Key themes were agreed by consensus between the two researchers to limit bias.

3. Findings

The review of the literature revealed the following information relating to the research questions:

3.1. Why is healthcare vulnerable?

Traditionally people believed that no one would be motivated to attack healthcare systems and protective measures were not deemed necessary. No healthcare organisation exists to provide cybersecurity. Emphasis has traditionally—and understandably—been focused upon patient care. There are several issues that complicate healthcare cybersecurity and have increased vulnerability over time:

- Increasingly connected technology to provide efficient ways to care for patients, particularly with chronic conditions [14]. This provides multiple ways of connecting to medical devices [15]. Devices are often easily accessible which increases the likelihood that attackers will find them. A single device could provide a potential entry point to larger hospital networks, bypassing the firewalls. There also tends to be a time lag between an attack occurring and detection of the breach, helping to further increase vulnerability.
- More focus on keeping patients healthy leading to more continuous patient monitoring outside the clinical environment [14,16]. More devices being used in the wider healthcare setting increases vulnerability to breaches.
- Mobile consumer devices (e.g., smartphones) being widely adopted; making it difficult to protect health data from risks posed by general purpose devices [14].

Alongside this growth of new technologies, many healthcare organisations are still using legacy systems in other areas, for example Window XP has not been supported since 2014 [17] allowing hackers and malware to easily avoid detection—for instance, the recent Wannacry attack [18]. The propriety nature of medical device software means that healthcare IT teams may not be able to access the internal software in medical devices, so they depend on manufacturers to build and maintain security in those devices (which has been lacking).

Lack of funding for cybersecurity is also problematic, while organisations are spending funding to become more integrated; they are not spending enough time and money to keep software updated and systems secure. This is aggravated by a lack of cybersecurity expertise within the sector resulting from a general lack of technology and the prohibitive expense of cybersecurity personnel [14,19].

In summary, a rapid move to electronic health records and interconnected devices, alongside historic and continual lack of investment in cybersecurity and a failure to understand the security workaround behaviours of health staff has left the health sector vulnerable to attack.

3.2. Why is healthcare targeted?

While healthcare has vulnerabilities to exploit, attackers must be motivated to carry out attacks. Motivation includes the potential for financial and political gain and potentially to take lives in a form of cyberwarfare. The strongest of these motivations is financial gain. Healthcare data is substantially more valuable than any other data. The value for a full set of medical credentials can be over $1000 [20]. Stolen medical identities can be used to obtain health services and prescription medication by assuming someone's identity or insurance credentials. Uses extend to sophisticated fraud perpetrated by organized crime. Fraudsters have earned billions in the last few years by filing fraudulent claims and dispensing drugs to sell on the dark web [21–23]. Sometimes there is even sufficient information in medical records to open bank accounts, secure loans or obtain passports [24].

Data held within health organisations also has political value. For example, the World Anti-Doping Agency was attacked and the records of prominent athletes made public [25]. NHS websites are accessed by millions of citizens, making them a prime site for publishing propaganda, e.g., NHS websites were hacked by cyberterrorists and images of Syrian civil war were uploaded [26].

Over the past decade we have seen numerous headlines warning of the potential for medical devices to be used as part of a futuristic cyberwar campaign. Nation state actors could disrupt healthcare in a foreign country by denying access or targeting individuals through their medical devices, or by collecting sensitive data.

Those with cybersecurity skills enjoy the challenge of finding and exposing security vulnerabilities in networks and medical devices. For example, in 2016 an individual scanning for security vulnerabilities was able to access a file containing data of people who had registered with the Australian Blood Donor service [27].

In summary, healthcare is targeted due to the potential for financial or political gain, or to expose vulnerabilities by cybercriminals, hacktivists and political activists.