Journal of Clinical Monitoring and Computing
https://doi.org/10.1007/s10877-023-01013-5

REVIEWS

The elephant in the room: cybersecurity in healthcare

Anthony James Cartwright[1]

Received: 8 March 2023 / Accepted: 5 April 2023

Abstract
Cybersecurity has seen an increasing frequency and impact of cyberattacks and exposure of Protected Health Information (PHI). The uptake of an Electronic Medical Record (EMR), the exponential adoption of Internet of Things (IoT) devices, and the impact of the COVID-19 pandemic has increased the threat surface presented for cyberattack by the healthcare sector. Within healthcare generally and, more specifically, within anaesthesia and Intensive Care, there has been an explosion in wired and wireless devices used daily in the care of almost every patient—the Internet of Medical Things (IoMT); ventilators, anaesthetic machines, infusion pumps, pacing devices, organ support and a plethora of monitoring modalities. All of these devices, once connected to a hospital network, present another opportunity for a malevolent party to access the hospital systems, either to gain PHI for financial, political or other gain or to attack the systems directly to cause erroneous monitoring, altered settings of any device and even to access the EMR via this IoMT window. This exponential increase in the IoMT and the increasing wireless connectivity of anaesthesia and ICU devices as well as implantable devices presents a real and present danger to patient safety. There has, at the same time, been a chronic underfunding of cybersecurity in healthcare. This lack of cybersecurity investment has left the sector exposed, and with the monetisation of PHI, the introduction of technically unsecure IoT devices for monitoring and direct patient care, the healthcare sector is presenting itself for further devastating cyberattacks or breaches of PHI. Coupled with the immense strain that the COVID-19 pandemic has placed on healthcare and the changes in working patterns of many caregivers, this has further amplified the exposure of the sector to cyberattacks.

Keywords Cybersecurity · Cyberattack · Phishing · COVID · Protected health information · Internet of things

1 Introduction

Electronic computers were developed in the 1940's and with their advancement, the miniaturization of components and reduction in cost, current computers may be held in the palm of the hand and weigh grams, the advancement being described by Moore's Law [1]. Along with almost universal access to computers and accessibility of the internet, computers have become central to every single aspect of life and society. From a healthcare perspective, this wireless connectivity allows the real time interaction of computers, ventilators, medication pumps, operating tables, operating robots, and any other networked device that is involved in healthcare. This interconnectivity allows the collection of a huge amount of data which can aid decision making, monitor and alert to unsafe situations and can expedite patient care.

Along with these bounds in computing, network technology and ability also came the risks inherent in allowing these machines to play such a central and pivotal role in society [2]. There will always be the individual or group, independent or state sponsored, who have used the ubiquitous nature of the digital revolution to cause harm for their own gain or strategic advantage [3], and it is this realisation that cyber-attacks could be used to generate financial gain that is the main aim of the attacks on healthcare institutions [4, 5]. The Internet of Things (IoT) represents devices with sensors, processing ability, software and other technologies that collect data and exchange this data with other systems or devices. They present their own benefits and risks and are extending into commercial areas, including healthcare [6]. Increasingly, syringe pumps, ventilators, monitors, and other monitoring and care devices are using wireless networks and will have access to the hospital network. Implantable

✉ Anthony James Cartwright
CartwrA1@clevelandclinicabudhabi.ae

[1] Cleveland Clinic Abu Dhabi, Abu Dhabi, United Arab Emirates

Published online: 24 April 2023

medical devices can connect wirelessly to update themselves, collect data and report back to the healthcare provider to monitor the patient's health and progress. One of the most technologically involved areas of healthcare is within anaesthesia and Intensive Care. It is apparent that with the widespread introduction of the Electronic Medical Record (EMR) and wireless device connectivity that the threat surface for malevolent actors has boomed and anaesthesia and Intensive Care could very well be a major risk area in this respect.

At a time when these changes were having increasing impact, the COVID-19 pandemic started early in 2020 and millions of people started to work from home. They used their own home network and computer to access work systems and the use of videoconferencing exploded [7]. Videoconferencing was also used by the caregivers to enable telemedicine to become an essential component of care [7]. The security principles that companies had developed over time became moot as workers were now working from home with little or no network security and cybersecurity knowledge rendering easy access to many highly sensitive systems. This is of particular concern to the healthcare sector due to the impact of a cyberattack and the potential for patient harm.

Whilst the attacks themselves are of obvious concern, the healthcare sector is seeing changes brought about by the very rapid increase in the use of the EMR [10], the IoT [11] and the use of implantable electronic medical devices [12]. There are obvious benefits to all these technologies; real-time monitoring leading to improved patient care, greater treatment options, monitoring patient compliance with a treatment plan, remote monitoring and health alerts and the list goes on. However, there are also risks; medical device hacking, the theft of PHI which may include not just health data but also personal, insurance and financial data, disrupting network traffic and interrupting healthcare delivery processes. These risks are increasing due to the huge increase in cyber-attack surface [13] provided by the increasing IoT and networked healthcare devices. The increasing use of Internet of Medical Things (IoMT) devices also presents significant risks as they are ubiquitous in anaesthesia and Intensive Care and range from ventilators, infusion pumps, monitoring equipment to implantable devices and specific organ support. Disruption or hacking of any of these devices could have the potential to cause irreparable damage to a system, delay or alter patient care and could even cause irreparable harm to a patient or caregiver.

2 Cybersecurity in healthcare: the elephant in the room ?

Healthcare cybersecurity is complex, and many data breaches have been the result of human error, as opposed to the perceived sole threat of the cybercriminal [8]. Jiang and Bai evaluated the causes of Protected Healthcare Information (PHI) breaches in the United States and a summary of their findings is presented in Table 1 [9].

It is of interest to note that by far the majority of PHI breaches, as a frequency, are due to theft, unauthorised access, loss or improper disposal of records, however the number of patients that had their medical records breached by hacking or IT incident dwarfs the number of all other breaches combined [9].

2.1 The frequency and potential impact of the threat

As the world increasingly relied on computer interconnectivity, there was an increasing development of malware, malicious software intentionally designed to cause disruption to a computer or network. Cybercrime also escalated quickly costing industry many trillions of dollars [14, 15]. The US healthcare industry leads other industries with a data breach costing an average of $7.13 m, 84% more than the average globally [15]. The global cost of cyber-attacks has made this a major industry, projected to cost the healthcare sector $6 trillion in 2021, an increase from $3 trillion in 2015 [16].

The frequency of PHI breaches in the US has increased steadily over the last decade and has increased by almost 40% between 2018 and 2019 (Fig. 1) [17].

Table 1 PHI breach causes (Jiang and Bai 2019)

Breach category	Frequency (% of all)	Patients affected	Further details
Theft (equipment or PHI)	41.5	22.2 m	Theft performed by employees, outsiders or unknown
Unauthorised access or disclosure	25.0	20.3 m	Employee disclosing information by accident or without authorisation
Hacking or IT incident	20.5	133.8 m	Malware or virus, phishing attack, unauthorised login use, accidental PHI exposure through the internet
Loss	10.1	5.7 m	Misplaced paper or electronic records by courier, employee or other
Improper disposal	3.4	0.7 m	Paper records not destroyed properly or electronic devices not purged of PHI

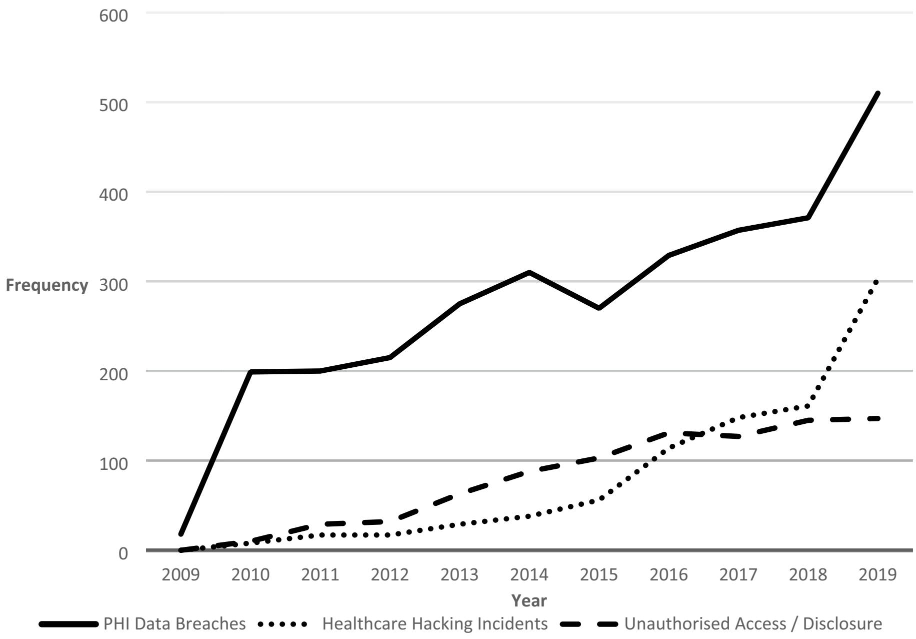

Fig. 1 PHI data breaches, healthcare hacking incidents and unauthorised access since 2009 in the United States (Robinson and Zoltan 2021)

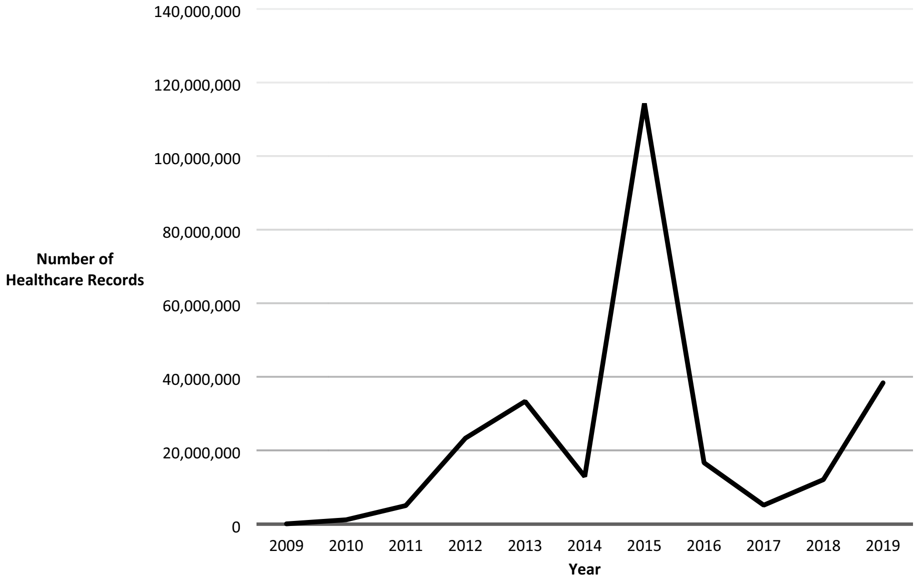

Fig. 2 Individuals affected by PHI breach (Robinson and Zoltan 2021)

Although this data reflects the number of breaches in the hundreds, the actual number of patients affected over the same period is in the hundreds of millions as can be seen in Fig. 2 [17]. Each attack can expose many thousands, or even millions of individual patient records [17].

The significant spike in 2015 is due to a single hack and data breach of the healthcare insurance company, Anthem Inc., resulting in the theft of 78.8 million unencrypted healthcare records [4, 6, 18].

A patient record contains a huge amount of information; everything from individual demographics and contact details, to sensitive medical information, financial, insurance and social security details, identification documents and prescription orders. This information is worth up to 10 times that of credit card information [19]. A credit card can be cancelled, nullifying its value, however medical records are part of a person's very identity and therefore extremely difficult to change. A full set of these medical record details may be worth anything up to $1000 on the dark web [20]. The details within the medical record are then used to create fraudulent documents to enable illicit financial gain or other fraud, obtain controlled medications and even for bribery or coercion, especially in the case of high-profile individuals [21]. The healthcare institution which has been compromised bears limited responsibility, however the individual whose record has been compromised may have to take extreme steps over many years to correct the impact of this fraud.

On top of the financial cost, there is the direct and indirect impact on the health of the population served by the compromised system. A perfect example of this impact was demonstrated during the WannaCry ransomware attack on 12 May 2017 affecting 230,000 systems in over 150 countries, including the National Health Service (NHS) in the UK [22, 23]. As a result, between 13 and 16 May 2017, five acute NHS Trusts had to divert Accident and Emergency patients to other Trusts that had uninfected systems [23-25] and a number of Trusts had issues with CT and MRI imaging systems [24]. The disruption caused the cancellation of almost 20,000 appointments or operations [23] and cost the NHS almost £92 m [26]. The population was affected immediately and directly with a reduction in access to healthcare, cancelled clinic appointments, the cancellation of operations and even the closure of Emergency Departments [23, 24]. Later indirect impacts included worsening patient health due to delayed treatments and missed diagnoses due to these cancelled appointments and procedures. From a network perspective, the biggest risk was the loss of data if the ransom was not paid; this is a common intent as it requires little effort with potential great reward. There is, additionally the risk of a breach of PHI which is also a common reason for an attack on Healthcare Institutions for financial gain. The control of medical equipment is much less common however is perfectly possible [27, 28]. The objective with this type of attack is often less about money, but more about the challenge or causing disruption or deliberate harm.

Historically, it is clearly established that IT, and more specifically cybersecurity, has been grossly underfunded within the healthcare sector globally [4, 13]. This has led to the continued use of older equipment [23], a deliberate abandonment of support and patching services [29, 65], reduced IT and cybersecurity staff employment and caregiver training which has created an environment which is ripe for the cybercriminal [30]. This is the perfect storm to increase the frequency of attacks [31] on a perceived soft target and an increasing threat surface as healthcare adopts the inevitable digital transition into EMRs and the IoMT. The monetisation of healthcare records has also made the healthcare sector a rewarding target [19] and this focus is not going to abate soon.

2.2 The benefits and risks of emerging technologies

We are living in the digital revolution and seeing developments and changes which were in the realms of science fiction within even our lifetime, for example wireless and remote monitoring, computers making healthcare decisions, automated anaesthetic machines, infusion pumps with pharmacological infusion models and even the smartphone. Many new smartphone apps gather vast amounts of personal and healthcare data and allow the transfer and sharing of this data. Advanced monitoring devices are making their way into healthcare allowing the monitoring of organ systems which has not been possible before. For example, the monitoring of cerebral function, EEG and cerebral oxygenation is now commonly used in the operating room and the ICU. Robots are playing their part enabling the advancement of direct patient care, especially surgically and for social care [32]. Hacking of these machines also has consequences that would be specific to the machine modality.

Within anaesthesia and Intensive Care, there has been an explosion in wired and wireless devices used daily in the care of almost every patient. This IoMT includes ventilators, anaesthetic machines, infusion pumps, pacing devices, organ support and a plethora of monitoring modalities [30]. These devices provide tremendous opportunities to assist in the care of patients undergoing procedures and in the care of those who are critically ill [30]. All these devices, once connected to a hospital network, present another opportunity for a malevolent party to access the hospital systems, either to gain PHI for financial, political or other gain or to attack the systems directly to cause erroneous monitoring, altered settings of any device and even to access the EMR via this IoMT window. It has already been proven that anaesthesia machines [27] and infusion pumps [28] can be hacked and their settings changes without the knowledge of the physician.

Artificial Intelligence (AI) is starting to become involved in patient care and this area will provide potentially amazing benefits; a physician's aid, diagnosing and planning treatments and even undertaking virtual appointments. They will also come with an equitable level of risk due to hacking, erroneous decision making and the moral and ethical issues of accountability for a machine system.

2.3 Wireless network vulnerabilities

Wireless networks have increased in speed and availability dramatically in the last decade with download speeds over 5G now up to 20Gb per second [33] and an experimental institution proving internet speeds of 319 Terabytes per second [34].

The ubiquitous nature of wireless access has numbed many to the risks involved [35]. Public, or 'guest,' networks that can be found in many establishments and public areas are often completely unsecure [36] with no verification required at all to log in. There is often no password required and there is usually no requirement for certificates to be validated leaving a connected unencrypted device wide open to being accessed [36]. Even if a password is required often anyone can ask for it, including a hacker, rendering the password effectively useless. Very few people understand or regularly use security solutions, such as a Virtual Private Network (VPN) connection whilst accessing these networks, and therefore pass all manner of personal and confidential information over this unsecure network. A VPN provides end-to-end wireless and wired encrypted connections thereby making it extremely challenging and time consuming to obtain the contained data. Without a VPN or other security it is therefore incredibly simple to access all this unencrypted information over an unsecure network using readily available and cheap technology and freeware (free software).

The introduction of 5G broadband cellular network also has technical risks [37]. One often highlighted risk is that to support increasingly different systems, 5G can 'slice' its own stream of data [37]. A corporation can then utilise its own 'slice' for a specific operation for example, banking or PHI. Simply creating this slice enables a labelled piece of information and could encourage a more focussed attack [37].

2.4 Software and patching

Widely used generic operating systems and software allows systems to be used across a broad work environment or multiple sites, such as a hospital, reducing costs. The disadvantage of this is that a widely used system will naturally be the focus of cybercriminals who are looking for a weakness to leverage as much as possible from their efforts and can use one attack to compromise multiple institutions in widely varying sectors. The WannaCry attack of 2017, for example, used a weakness in the Microsoft Windows XP operating system [29] to cause havoc in the NHS and also Nissan Motor Manufacturing UK, Renault, Spain's Telefonica network, FedEx couriers and Deutsche Bahn along with many other companies across the world [22]. With respect to anaesthesia, GE's Aestiva and Aespire ventilators and anaesthetic machines were found, in 2018, to use a proprietary protocol for changing settings. If these machines were connected to a network it is fairly straightforward to send commands over the network to silence alarms, alter records and change the composition of inspired gases used in both models [27]. Infusion pumps are not immune. The Alaris Gateway Workstation, which controls several infusion pumps in one portable module, was found to have a security weakness that enabled an individual to place malicious firmware on the pump and change infusion rates [28]. Obviously, adjusting the rates of critical care infusions, sedation, analgesia or other medication could all have fatal consequences.

Software needs support and regular patching to ensure that these vulnerabilities are secured before they are discovered and used for criminal purposes. Without these updates, there may well be vulnerabilities in the outdated software enabling a hacker to gain access. Regular updates enable all IoMT devices to remain as secure as possible, limiting the risk to patient care.

Whilst patching and updates are vital, the human factor is often the weakest link [9] and a number of simple interventions can reduce this liability. Caregivers' passwords should have a minimum requirement and include numbers and punctuation. Password renewal should not allow the addition of a number or a letter to the previous password. Training and regular fake phishing emails sent from IT will help heighten an individual's suspicion. Another frequently used solution is to put a highlighted header on all emails from an external source, to make the recipient more alert about the contents.

In an ideal world, an EMR server would not be connected to the internet, however this is becoming increasingly impractical. With the march of the paperless world, health data is shared between hospitals locally and across the world to enable appropriate care on a mobile population. Encryption is key. The fact that these servers are online for this reason and therefore exposed leads to an often-overlooked recommendation, which is to back up all data securely and regularly, at least daily. These back-ups should be on a separate server not connected to the internet, but able to restore a system efficiently and accurately in the event of an outage of any origin, including hacking or ransomware.

The widespread use of smartphone apps also presents its own issues. Again, there is great benefit in using the power of the smartphone in monitoring, storing, and transmitting information via an App. Many Apps can link directly into the EMR of a hospital, feeding real time information about a patient's condition, vitals and symptoms and this information is therefore PHI. There are also smartphone Apps that allow direct connection to patient monitoring devices remotely [38]. Apps are being used and have proven to be useful in contact tracing and enforcing social distancing during the COVID-19 pandemic [39]. This tremendous power comes in a small, highly desirable device which is worth a lot of money. They are frequently stolen and with them, the data is potentially exposed. Whilst the devices are reasonably secure, there are methods to obtain all the data stored on a smartphone without the login [40].

2.5 Hardware, the internet of things and medical devices

Up to date hardware is as important as up to date software, however older hardware is all too common, increasing the risk of cyberattack.

The IoT is one of the principal threats to cybersecurity currently. IoT has previously been defined and can exist in almost every environment from factory, home, hospital to even the car, to name but a few. A huge amount of personal information can be collected by these devices, and this obviously leads to privacy and confidentiality concerns. From a healthcare perspective, the IoMT may be employed for remote monitoring and emergency notification of medical conditions and is being found to be particularly applicable in the care of the elderly [41]. Increasingly, devices such as ventilators, infusion pumps, pacemakers, radiology equipment, laboratory equipment and the EMR is connected to the intranet in a hospital, usually wirelessly, and often also the internet. Wearable IoT devices can increasingly be used in healthcare to record heart rate and rhythm, blood pressure and to monitor blood sugar levels in diabetic patients [41, 42]. From a pandemic perspective, IoT wearables can be used to enforce social distancing [43] and also to enforce quarantine by limiting the user to a location, for example their home, using GPS sensor technology—Geofencing [43]. If the wearer breaches their allocated area, the IoT device alerts authorities [43] with consequent possible repercussions. The scope of 'things' in the IoT is huge and the consequent ratio of things/people grew from 0.84 in 2003 to 1.84 in 2010 and was projected to reach 6.58 by 2020 [41].

This massive explosion of connected devices is of particular concern due to the nature of their construction and the way in which they function and the fact that these devices are so pervasive in our personal lives, in healthcare as well as controlling wider critical infrastructure. There is currently little enforced regulation for IoT device design and production. An IoT device is often made from cheap, insecure components, typically has a proprietary operating system, and is often connected to some sort of App which may upload data to a server. Software updates are often difficult to locate and sometimes not offered at all. The security features are usually limited and, even when present, are often not changed by the end user [44] leaving the device in a default insecure mode. These security shortcomings have caused the IoT to be in the crosshairs of cybercriminals, with a particular focus on domestic internet routers and webcams [45].

Medical devices are usually better constructed to meet industry specific regulations and standards however, again, security is difficult to institute in many IoMT devices due to the proprietary software and firmware [11, 46]. Proprietary software and firmware enable the production of a device with a specific and limited function, reducing manufacturing and programming costs and allowing updates solely by the manufacturer of the device.

IoMT devices are also unable to support third party software solutions such as antivirus software [11] and manufacturers therefore sometimes rely on the security of the communications to and from the device to protect against a cyberattack. Surprisingly, most medical devices do not use encryption as this shortens battery life [12, 46]. Implantable electronic devices may be viewed as an IoMT device and are available for an increasing range of conditions. Many of these devices, such as pacemakers, ICDs, deep brain stimulators and infusion pumps to name but a few, have wireless connectivity for programming and, occasionally, for uploading information so that a patient's condition can be monitored remotely by the physician. These implantable devices have been shown to be vulnerable to hacking via their wireless connectivity [47-49] and the implication is that patients could be harmed [49]. The United States' Secret Service was sufficiently concerned in the early 2000's that they disabled the wireless connectivity function of the pacemaker of the then Vice President, Dick Cheney [50]. As we have seen, syringe pumps can be made to give boluses [28] if hacked and anaesthesia machines and ventilators have been proven to have their vulnerabilities [27]. Even the monitors on which we rely can be altered and alarms silenced. Worryingly, it is possible to hack and use deep learning to alter CT and MRI scan images via an institution's radiology server in a way that would not be detected by a radiologist or Artificial Intelligence (AI) examination [51]. This sort of cyber-attack could be easily used to impact the career of a politician, undermine a research establishment, or perform an act of indirect terrorism by altering healthcare management of a public figure. Robots have limited use in healthcare currently, however where they are used, they generate huge amounts of data [15] which is classified as PHI and therefore must be secured. Again, the principle risk is the breach of this data and its illicit use, usually financial gain. Robots have a place in direct patient care, and the thought of these systems being hacked and controlled seems horrific, but technically, is possible as has occurred with a surgical robot [52]. These devices are going to be the next security nightmare for the healthcare sector [53]. Already, there is malware that can infect IoMT devices and spread across a hospital network until it reaches a workstation and then the EMR [54].

As the digital revolution continues, there are huge challenges ahead with the support and development of the IoMT and ensuring that these devices are appropriately secured to reduce the threat of an attack [11, 13]. Regulations need to be written and enforced with manufacturers [11] and this needs to be a priority as these devices are being introduced at an exponential rate. The devices on which we rely, as physicians, all have the ability to be hacked and manipulated [27, 28] and this needs to be remedied.

It can easily be seen that IoT and, specifically, the IoMT can bring great benefits, for example rapid data collection and transmission, early intervention, predicting potential complications, improving patient engagement, all of which aid the caregiver. However, there are huge safety risks if these devices are not secured and protected from attack or abuse due to the potential for sabotaging the devices to cause harm or erroneous treatment, or the theft of PHI for potential illegal activity.

2.6 Human factors

With all these technologies becoming available to even the smallest of healthcare establishments, the risk surface is increased, however one of the most important determinants of absolute risk is the behaviour of the human in the system and this is usually the weakest link. In 2014, IBM stated that "over 95% of all [security] incidents investigated recognize 'human error' as a contributing factor" [55]. Infoguard Cyber Security stated that 46% of data breaches in healthcare in 2017 were due to employee behaviour [56].

An increasing technology in the last decade has been that of social engineering. This is an act that causes a recipient to take an action that may or may not be in their best interests [57]. This frequently takes the form of an email or some form of communication with malicious links or attached malware; a phishing attack. The email will be designed to use the weaknesses of the individual or society to cause the recipient to click on the link or attachment. This was particularly prevalent during the COVID-19 pandemic and the uptick in cyber-attacks reflects the use of social engineering by cyber criminals aimed at an individual's health concerns and personal protection around COVID-19. The risk from these types of attacks is still increasing.

It is vital that the healthcare workforce is cyber-aware and understand that even with the best cybersecurity systems in place, they may still be the recipient of a phishing attack which could jeopardise the hospital and all connected devices, both in and outside of the perioperative and Intensive Care environments. The healthcare sector needs to have a culture change to one of IT being an enabler, a defender and a vital asset of any hospital, rather than the IT department often being viewed with derision and as an obstruction. This culture change should encourage the attitude of an email or weblink being viewed with zero trust rather than the implicit trust that is often assumed at present [6]; a 'zero trust' culture. This requires effort and the education of all staff in cyber-awareness and the risks of a cyberattack [6].

Irrespective of the direct patient care risks, 30% of the world's data belongs to healthcare [58], and it is imperative that this is secured and regulated correctly, particularly considering the content of this data and its value to the criminal.

3 Specifically, the impact of the COVID-19 pandemic on Healthcare Cybersecurity

One of the first reactions to the COVID-19 pandemic was to move to a working from home environment for many workers. Home working was not a new concept, however the scale and speed with which this was introduced was breath-taking [59]. Obviously, front line medical staff remained in the clinical environment, however many administrative and secretarial staff were forced to work from their homes. Working from home necessitated workers to log in from their own private network, often on their private computer. The cybersecurity in a residential address and on a private computer would be almost non-existent compared to a healthcare institution. Certainly, in the UK only 38% of businesses had any cybersecurity policy in place at the time of the first lockdown [59]. From a physical security perspective, a computer in a house is often used by many members of the family and this then introduces the risk of exposing PHI to individuals who should not have this access.

Telemedicine, which enables video or phone appointments between a patient and their caregiver, was already established and experienced an unprecedented increase in use during COVID-19 to become an essential component of care in many hospitals [7]. This would be using hospital equipment to connect to patients on their personal devices on unsecure networks outside of the hospital, again, raising security issues. Videoconferencing also exploded at this time with a 10-fold use of some platforms for workplace meetings [7]. This increase in the use of virtual appointments and meetings has remained in many institutions and is often being routinely offered to patients. The huge uptake of this platform has been used by cybercriminals to install malware onto computers by developing genuine looking software installers which have built in malware and data skimming attachments giving the malicious entity access to the system for hacking purposes or simply to silently listen to all the data passing through a system.

The attack surface of all sectors, including healthcare institutions, was hugely increased due to these changes and cybercriminals made good use of this exposure [60]. The scale of the social engineering phishing attacks was exponential during the COVID-19 pandemic and increased by 600% by March 2020 since the start of COVID-19 [61, 62]. By April 2020, Google was stopping 18m COVID-19 related malware and phishing emails daily [63]. This social engineering was preying on the fear, concern and isolation that many people felt about COVID-19, lowering their guard and making phishing attacks more likely to be successful [58].

With these security risks in mind, it is important to note that fear, isolation and some degree of paranoia that many felt during this pandemic caused patients to be selective about the medical information that they were willing to divulge [64] resulting in suboptimal patient management.

COVID-19 has placed a massive burden on the healthcare sector, both clinically and administratively and few institutions were able to bear this well [31]. The huge increase in the use of remote access due to working from home massively increased the attack surface in every sector, including healthcare, and this has been utilised by the cybercriminal community with deliberately socially engineered phishing attacks and malicious links and websites [30]. Coupled with a population who were fearful, socially isolated, and largely unaware of the appearance and risks of a cyberattack, a successful attack was, and still is, inevitable [30].

There have been dramatic, and necessary, advances in healthcare provision because of the COVID-19 pandemic, however this progression brings with it risks, principally exposure of PHI for gain, corruption of a network or hacking of the EHR and malevolent interference with IoMT devices. Malicious actors will seize these opportunities long before appropriate security and governance are in place.

4 Conclusion

Challenges have been highlighted that have coincided and amplified cybersecurity vulnerability and the risk to the healthcare sector. These challenges are a lack of funding leading to outdated equipment and software, reduction of skilled IT and cybersecurity staff leading to reduced support and patching updates, and caregiver training. This has coincided with the COVID-19 pandemic and a huge uptick in cybersecurity attacks globally. Correcting these shortfalls requires funding and the amount that is being currently invested is simply not going to support a robust cyber defence system, let alone place the healthcare sector on a level footing with industry.

The explosion of IoMT demands that regulatory bodies be established to regulate the design, manufacture and distribution of these devices including basic standards of encryption and communication protocols. Without some form of regulation, the IoMT is setting itself up as a huge and unsecure attack surface in an industry which has the highest price for data on the dark web.

All software and devices, including the IoMT must be regularly updated and patched to ensure that they are up to date with current threats. Without this, again, the attack surface is greater and readily exposed as was seen in the Wannacry attack on the NHS in 2017.

All data should be encrypted and securely backed up regularly to provide continuity and a safe Healthcare system which is fit for purpose in the event of attack. Without encryption, the data is vulnerable to abuse if obtained illicitly and without back-ups the Institution is helpless to provide any standard of care in the event of an outage of any sort.

But the biggest single difference, which should be made by all Institutions, is to train all their staff, irrespective of role. They should have annual online courses reminding them about cybersecurity and, particularly phishing. They should be trained about the lack of security on public networks as well as how to make themselves more secure. Regular fake phishing emails should be sent from IT. All external emails should have a banner or highlighted bar to focus attention to a potential risk. Passwords should have a minimum strength and should be renewed regularly with a completely fresh password. All these interventions will have the biggest impact as it is the staff of an Institution that are the biggest cybersecurity risk to the systems and their data.

All these interventions require funding and the lack of funding in Healthcare Cybersecurity is lamentable. Without this funding and the expertise that is required the likelihood of an attack is inevitable. The only question is "when."

Author contributions AC wrote the manuscript text and prepared all of the figures and tables based on data presented in the referenced publications.

Funding The author declares that no funds, grants, or other support were received during the preparation of this manuscript.

Declarations

Competing interests I declare that the authors have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper.

References

1. Moore GE. Cramming more components onto integrated circuits. Electronics. 1965;38(8):114–7.
2. World Economic Forum. What new technologies carry the biggest risks? https://www.weforum.org/agenda/2017/01/what-emerging-technologies-have-the-biggest-negative-consequences/#:~:text=The%20emerging%20technology%20with%20by,deprive%20millions%20of%20their%20jobs (2017). Accessed 25 Mar 2023.
3. HM Government. National Cyber Security Strategy 2016–2021. London, United Kingdom: HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (2016). Accessed 12 Dec 2020.
4. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we? Br Med J (Clinical Res Ed). 2017;358:j3179. https://doi.org/10.1136/bmj.j3179.
5. Verizon. 2019 Data Breach Investigations Report. https://enterprise.verizon.com/en-gb/resources/reports/dbir/ (2019). Accessed 5 Jan 2021.
6. Ghafur S, Fontana G, Martin G, Grass E, Goodman J, Darzi A. Improving Cyber Security in the NHS. London, United Kingdom: Imperial College London Institute of Global Health innovation. https://www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf (2019). Accessed 15 Nov 2020.
7. Jalali MS, Landman A, Gordon WJ. Telemedicine, privacy, and information security in the age of COVID-19. J Am Med Inform Assoc. 2020;28(3):671–2.

8. Wirth A. COVID-19 and what it means for cybersecurity. Biomed Instrum Technol. 2020;54(3):216–9.
9. Jiang JX, Bai G. Evaluation of causes of Protected Health Information Breaches. JAMA Intern Med. 2019;179(2):265–7.
10. Sittig DF, Singh H. A socio-technical approach to preventing, mitigating, and recovering from Ransomware attacks. Appl Clin Inf. 2016;7(2):624–32.
11. Royal Academy of Engineering. Cyber safety and resilience: strengthening the digital systems that support the modern economy. London: Royal Academy of Engineering. 2018.
12. Best J. Could implanted medical devices be hacked? British Medical Journal (Clinical Research Ed), 368, m102. https://www.bmj.com/content/368/bmj.m102 (2020). Accessed 23 Feb 2021.
13. Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas. 2018;113:48–52.
14. Williams CM, Chaturvedi R, Chakravarthy K. Cybersecurity Risks in a Pandemic. Journal of Medical Internet Research, 22(9), e23692–4. https://www.jmir.org/2020/9/e23692/ (2020). Accessed 23 Feb 2021.
15. O'Brien S. Average Cost of Data Breach in Healthcare Industry Hits $7.13 Million. https://securityitsummit.co.uk/briefing/average-cost-of-data-breach-in-healthcare-industry-hits-7-13-million/ (2020). Accessed 12 Dec 2020.
16. Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber Security in the age of COVID-19: a Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the pandemic. Comput Secur. 2020;105:102248.
17. Robinson J, Zoltan M. US Healthcare Data Breach Statistics. https://www.privacyaffairs.com/healthcare-data-breach-statistics/ (2021). Accessed 15 Apr 2021.
18. Ghafur S, Grass E, Jennings NA, Darzi A. The challenges of cybersecurity in health care: the UK National Health Service as a case study Comment. Lancet Digital Health. 2019;1(1):e10–e12.
19. Sulleyman A. NHS cyber attack: why stolen medical information is so much more valuable than financial data. http://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html (2017). Accessed 12 Dec 2020.
20. Stack B. Here's How Much Your Personal Information Is Selling for on the Dark Web. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (2017). Accessed 25 March.
21. Scott J, Spaniel D. Your life, repackaged and resold: the deep web Exploitation of Health Sector Breach victims. New York: ArtOfTheHak; 2019.
22. Cyber-attack: Europol says it was unprecedented in scale. https://www.bbc.com/news/world-europe-39907965 (2017). Accessed 27 Nov 2020.
23. Mayor S. Sixty seconds on. the WannaCry cyberattack. British Medical Journal (Clinical Research Ed), 361, k1750. https://www.bmj.com/content/361/bmj.k1750 (2018). Accessed 11 Mar 2023.
24. Department of Health and Social Care. Lessons learned review of the WannaCry Ransomware Cyber Attack. London, United Kingdom: Department of Health and Social Care. https://www.england.nhs.uk/wp-content/uploads/2018/02/06_pb_08_02_18-lessons-learned-review-wannacry-ransomware-cyber-attack.pdf (2018). Accessed 12 Dec 2020.
25. Martin G, Ghafur S, Kinross J, Hankin C, Darzi A. WannaCry-a year on. British Medical Journal (Clinical Research Ed), 361, k2381. https://www.bmj.com/content/361/bmj.k2381 (2018). Accessed 19 Dec 2020.
26. National Health Executive. WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled. https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled (2018). Accessed 26 Mar 2023.
27. Whittaker Z. GE admits security flaws in its hospital devices could cause patient harm. https://techcrunch.com/2019/07/09/flaws-anesthesia-respiratory-devices-tampering/ (2019). Accessed 6 Mar 2023.
28. Whittaker Z. A widely used infusion pump can be remotely hijacked, say researchers. https://techcrunch.com/2019/06/13/alaris-infusion-pump-security-flaws/ (2019). Accessed 6 Mar 2023.
29. Martin G, Kinross J, Hankin C. Effective cybersecurity is fundamental to patient safety. British Medical Journal (Clinical Research Ed), 357, j2375. https://www.bmj.com/content/357/bmj.j2375 (2017). Accessed 26 Mar 2023.
30. Pranggono B, Arabo A. COVID-19 pandemic cybersecurity issues. Internet Technol Lett. 2020;2021(4):e247.
31. Baumgart DC. Digital advantage in the COVID-19 response: perspective from Canada's largest integrated digitalized healthcare system. NPJ Digit Med. 2020;3(1):1–4.
32. Houses of Parliament. Robotics in social care. London: Houses of Parliament; 2018.
33. Looper C. What is 5G? Everything you need to know. https://www.digitaltrends.com/mobile/what-is-5 g/ (2021). Accessed 18 May 2021.
34. Sharma B. With 319 Terabytes per second, Japan sets new world record for internet speed. What does this mean? https://www.wionews.com/technology/with-319-terabytes-per-second-japan-sets-new-world-record-for-internet-speed-what-does-this-mean-399033 (2021). Accessed 25 Mar 2023.
35. Petrosyan A. Share of global adults who trust public Wi-Fi networks to keep info safe 2019. https://www.statista.com/statistics/1147501/share-adults-trust-public-location-wifi-network-information-safe/ (2022). Accessed 25 Mar 2023.
36. Cyberunit. Can You Trust Public WiFi? https://www.cyberunit.com/blog/can-you-trust-public-wifi (2021). Accessed 25 Mar 2023.
37. McNamee K. 5G – What could go wrong? [Conference Presentation]. ISC2 Security Congress 2020, Online (2020).
38. Patel H, Hassell A, Keniston A, Davis C. Impact of Remote Patient Monitoring on Length of Stay for Patients with COVID-19. Telemedicine and E-Health. 2020. https://doi.org/10.1089/tmj.2021.0510.
39. Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dorner L, Parker M, Bonsall D, Fraser C. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science. 2020;368(6491):eabb6936.
40. Skorobogatov S. The bumpy road towards iPhone 5c NAND mirroring. https://arxiv.org/pdf/1609.04327.pdf (2016). Accessed 27 June 2018.
41. Evans D. The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. San Jose, United States of America: Cisco. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (2011). Accessed 18 Oct 2020.
42. Ericsson. Wearable technology and Internet of things. https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/wearable-technology-and-the-internet-of-things (2016). Accessed 6 Mar 2023.
43. Nasajpour M, Pouriyeh S, Parizi RM, Dorodchi M, Valero M, Arabnia HR. Internet of things for current COVID-19 and future pandemics: an exploratory study. J Healthc Inf Res. 2020;4(4):1–40.
44. Cisco. Defending against today's critical threats. San Jose, United States of America: Cisco. https://www.cisco.com/c/dam/global/en_uk/assets/pdfs/en_cybersecurityseries_thrt_01_0219_r2.pdf (2019). Accessed 18 Oct 2020.

45. Symantec. Internet Security Threat Report. Mountain View, United States of America: Symantec. https://docs.broadcom.com/doc/istr-24-2019-en (2019). Accessed 19 Jan 2021.
46. Zou X, editor. IoT devices are hard to patch: Here's why—and how to deal with security. Retrieved from https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security. Accessed 18 Oct 2020.
47. Food and Drug Administration. Firmware update to address cybersecurity vulnerabilities identified in Abbott's (formerly St Jude Medical's) implantable cardiac pacemakers: FDA safety communication, 29 Aug 2017. https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals (2017). Accessed 18 Oct 2020.
48. Food and Drug Administration. Cybersecurity vulnerabilities affecting medtronic implantable cardiac devices, programmers, and home monitors: FDA safety communication, 21 Mar 2019. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home (2019). Accessed 18 Oct 2020.
49. Newman LH. A New Pacemaker Hack Puts Malware Directly on the Device. https://www.wired.com/story/pacemaker-hack-malware-black-hat/ (2018). Accessed 12 Dec 2020.
50. Peterson A. Yes, terrorists could have hacked Dick Cheney's heart. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/ (2013). Accessed 15 July 2020.
51. Mirsky Y, Mahler T, Shelef I, Elovici Y. CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning. https://arxiv.org/pdf/1901.03597.pdf (2019). Accessed 15 July 2020.
52. MIT Technology Review. Security Experts Hack Teleoperated Surgical Robot. https://www.technologyreview.com/2015/04/24/168339/security-experts-hack-teleoperated-surgical-robot/ (2015). Accessed 18 Oct 2020.
53. Newman LH. Medical Devices Are the Next Security Nightmare. https://www.wired.com/2017/03/medical-devices-next-security-nightmare/ (2017). Accessed 18 Oct 2020.
54. Storm D. MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks. https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html (2015). Accessed 15 Dec 2020.
55. IBM Global Technology Services. IBM Security Services 2014 Cyber Security Intelligence Index. Somers, United States of America: IBM Corporation. http://i.crn.com/custom/IBMSecurityServices2014.PDF (2014). Accessed 8 Mar 2020.
56. Infoguard Cyber Security. 5 industries that top the hit list of cyber criminals in 2017. https://www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/ (2017). Accessed 15 Dec 2020.
57. Hadnagy C. Social Engineering: the Science of Human Hacking. 2nd ed. Indianapolis: Wiley; 2018.
58. Hoffman S. Cybersecurity threats in healthcare organizations: exposing vulnerabilities in the healthcare information infrastructure. World Libraries. 2020;24(1)
59. Furnell S, Shah JN. Home working and cyber security–an outbreak of unpreparedness? Comput Fraud Secur. 2020;2020(8):6–12.
60. Hackett M. Number of cybersecurity attacks increases during COVID-19 crisis: Hackers are taking advantage of provider distraction to breach health systems. https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis (2020). Accessed 16 Dec 2020.
61. Shi F. Threat spotlight: coronavirus-related phishing. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing (2020). Accessed 19 May 2021.
62. Sjouwerman S. Q1 2020 coronavirus-related phishing email attacks are up 600%. https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600 (2020). Accessed 19 May 2021.
63. Kumaran N, Lugani S. Protecting businesses against cyber threats during covid-19 and beyond. Retrieved from https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond (2020). Accessed 20 May 2021.
64. Ronquillo JG, Winterholler JE, Cwikla K, Szymanski R, Levy C. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. J Am Med Inf Assoc Open. 2018;1(1):15–9.
65. Gibbs S. UK government PCs open to hackers as paid Windows XP support ends. Retrieved from https://www.theguardian.com/technology/2015/may/26/uk-government-pcs-open-to-hackers-as-paid-windows-xp-support-ends (2015). Accessed 19 Dec 2020.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.