Cybersecurity of Cardiac Implantable Electronic Devices

David Slotwiner, Arnab Ray, Kevin Fu, and Bruce L. Wilkoff

Introduction

Any illusions that cardiac electronic implantable devices (CIEDs) might not be susceptible to cybersecurity risk were shattered on August 25, 2016, when Muddy Waters Research LLC, an investment research firm, released a report claiming that cybersecurity researchers at MedSec, a firm focused on the healthcare industry, had determined that St. Jude remote transceivers were vulnerable to hacking and could allow an intruder to reprogram an implanted device [1]. This report, released directly to the public, claimed that approximately 500,000 St. Jude CIEDs were susceptible to unauthorized reprogramming due to security weaknesses in their Merlin@home remote transceiver.

Patients, the public, and the medical community were uncertain if and/or how to respond to the claims made by Muddy Waters LLC. St. Jude issued its first response 3 weeks later, on September 16, denying the claim [2]. They also cited evidence that Muddy Waters distributed the report for the purpose of reducing the stock price in order to bolster the firm’s short-selling position as Abbott was in the final stages of negotiating the purchase of St. Jude Medical. Cybersecurity experts at the University of Michigan’s Archimedes Center for Medical Device Security were quick to find flaws with Muddy Waters’s report but did not exclude the possibility that the vulnerabilities might exist [3]. Little additional information was available to the public until August 29, 2017, a full year after the initial publication by Muddy Waters, when the FDA and Abbott, which had by this time acquired St. Jude, announced the release of a firmware update that could be installed on each CIED that would eliminate the vulnerability [4].

The most serious claim issued by Muddy Waters and MedSec was that the Merlin@home remote transceiver could be transformed into a device capable of reprogramming an implantable defibrillator. Details of the vulnerability have now been made available to the public and summarized for a lay audience by cybersecurity researcher Matthew Green [5]. MedSec researchers were able to purchase a St. Jude CIED programmer and Merlin@home remote transceiver on eBay. They then identified the computer code used by the programmer to communicate and authenticate its identity with an implanted St. Jude CIED. Next, they copied this code and installed it on a Merlin@home remote transceiver, rendering it capable of issuing reprogramming commands to the CIED. This highlighted two underlying security vulnerabilities.

The first vulnerability was that reprogramming commands could be sent using radiofrequency communication from a distance of several feet without first requiring much closer interaction between the CIED and the programmer using inductive coupling. CIEDs communicate with a programmer via two distinct mechanisms: Near-field communication is established via inductive coupling which requires very close proximity between the programmer and implanted device (centimeters). This is typically established by placing the programmer wand on the patient’s chest. Radiofrequency communication is used to communicate over longer distances – usually several feet. This is the technology used for wireless remote monitoring in patients’ homes. For security purposes, most CIEDs will only accept reprogramming commands if communication is first established via inductive coupling, requiring the wand to be physically placed within centimeters of the implanted unit. Once this communication is established and the devices are paired, the CIED then will accept reprogramming commands via radiofrequency...
communication between the programmer and the implanted unit for a period of time. MedSec’s findings revealed that St. Jude CIEDs did not first require communication between the programmer and CIED to be established by inductive coupling before the implanted device would accept reprogramming commands via radiofrequency.

The second vulnerability pertained to the security protocol employed by St. Jude that enabled a programmer to identify (authenticate) itself to the implanted device as an authentic St. Jude programmer. When the cybersecurity researchers at MedSec identified the computer code that allowed the St. Jude programmer to send reprogramming commands to the implanted device, they also identified the protocol used to encrypt the commands. An encryption or authentication tag must be present and correct with each command issued by the programmer, or the implantable device will refuse to accept the command. Typically an encryption tag is calculated using a secure cryptographic function with a fresh secret key that cannot be predicted by an attacker. But MedSec and Bishop Fox found that instead, St. Jude authenticated the programmer to the implantable device using a key table that was hard-coded within the programmer. This meant that any individual who obtained a St. Jude programmer could gain the ability to calculate the correct authentication tags needed to produce viable commands without using the programmer itself. More concerning, MedSec identified that St. Jude had a shortcut built in that could be used to bypass the encryption: a universal 3-bit authentication tag was built in that could be used instead of the calculated encryption code. This 3-bit code was sufficient to issue a command shock from a Merlin@home transceiver.

The Muddy Waters/MedSec report and subsequent sequence of events brought to light how unprepared the medical community was to evaluate and manage a potential cybersecurity crisis. Fortunately, no patients were harmed, and lessons learned from this event have included a recognition that healthcare providers must be better informed and must recognize their role in minimizing the risks of cybersecurity breaches. It also has advanced our understanding of what patients expect and need from their healthcare provider.

In this chapter, we will provide an overview of the present cybersecurity landscape including the existing infrastructure focused on minimizing cybersecurity vulnerabilities, US federal agencies involved in evaluating and minimizing risks, industry guidance to develop medical devices that “fail gracefully” if hacked rather than catastrophically, and our role as healthcare providers. Finally, we will review the emerging consumer privacy regulations that are being enacted to grant individuals control over their personal data – whether acquired legally or through a cybersecurity breach – and the implications of these regulations for healthcare and particularly for the stakeholders managing patients with CIEDs.

Cybersecurity Landscape

Inserting or damaging computer code in order to cause malfunction or dysfunction, in other words computer hacking, and unauthorized accessing of personal data are an unintended consequence of our highly interconnected medical environment. Adjusting the pacing rate of the first Medtronic pacemakers, implanted in 1960, required inserting a screwdriver through the patient’s skin and rotating a dial on the implanted device. Because there was no way to communicate with the implanted device other than physically interacting with it, there was no mechanism by which the computer code could be altered. This provided the ultimate cybersecurity. Once wireless telemetry communication was introduced, a potential access door to the device was opened (Fig. 29.1). The same is true throughout our medical environment. In our hospitals, virtually no equipment or information technology systems operate in isolation. For example, imaging equipment obtains demographic data from the hospital’s admissions and discharge system. It also transmits the images to a picture archiving and communications system (PACS). Even equipment that may appear to operate in isolation such as IV pumps, respirators, and external defibrillators have access through (typically) a USB port in order to allow the manufacturer to update the software and retrieve information about the device’s performance. Each communication point is a potential access door that an intruder might use to hack a medical device. Given enough time and resources, a skilled intruder is likely to find a vulnerability in the computer cod-

![Fig. 29.1](image) Devices that can access the programmed parameters of a cardiac implantable electronic device (CIED). The remote transceiver and smartphone can download the programmed parameters and data stored by the CIED, but only the programmer can make changes to the programmed parameters.
ing, allowing the intruder to hack the device. The goal of cybersecurity is to make it so difficult to hack a device that the resources needed to succeed are greater than those available to the hacker. A secondary goal is to develop underlying computer code that can detect if it has been hacked and have the device default to a safe backup mode in order to avoid catastrophic failure (i.e., fail gracefully).

**Medical Device and Data Vulnerabilities**

Intravenous infusion pumps were the subject of the first FDA cybersecurity advisory to the medical community. On July 31, 2015, the FDA advised healthcare facilities to discontinue using the Hospira Symbiq infusion system due to a security vulnerability detected by an independent cyber security expert, Billy Rios [6]. The Department of Homeland Security (DHS) following a lead detected by Billy Rios determined that a remote attack could be launched on patients by accessing a hospital’s network, allowing an unauthorized user to control the device and change the dosage the pump delivers. There was no evidence any patients had been harmed or that the vulnerability had been exploited. The model affected, Hospira’s Symbiq infusion system, was no longer being manufactured, but the company worked quickly with FDA to provide a software update eliminating the vulnerability.

On February 4, 2015, the second largest health insurance agency in the USA, Anthem, announced that hackers had broken into their database and obtained personal information such as social security numbers, addresses, and employment information on almost 80 million customers and employees [7]. The attackers, employing a sophisticated technique called email spear-phishing, leveraged publicly available information on Anthem employees to pose as a known or trustworthy sender. If an employee opened the email, malicious files were downloaded to the user’s computer which allowed hackers to gain remote access to that computer and many other computers within Anthem [8]. The hackers were able to then move across Anthem’s network, escalating privileges and gaining greater ability to access information and make changes to the network until they finally reached Anthem’s data warehouse where consumer personally identifiable data was stored. An exhaustive investigation concluded that the attack was the work of a Chinese national, Fujie Wang, and another unnamed co-defendant [9]. Prosecutors were unable to find clear links to the Chinese state, but the suspicion is that it was carried out on the government’s behalf. The Anthem attack bears many similarities to the hacking of Equifax in 2017, which was proven to be linked to four members of the Chinese military with the goal of obtaining sensitive financial information on US intelligence members [10]. One important lesson learned in the Anthem investigation was that a breach of such large magnitude could begin from a phishing email, demonstrating the “human perimeter” to be the weakest link and calling attention to the need to educate all members of an organization to minimize cybersecurity risk [8].

Perhaps the single most damaging cybersecurity breach to affect healthcare (even though it was not the primary target) was the WannaCry ransomware cryptoworm which targeted computers running an outdated version of the Microsoft Windows operating system (Fig. 29.2). Friday, May 12, 2017, computers infected by the ransomware began displaying an alert demanding payment in bitcoin in order for the user to gain access to their files [11]. Healthcare organizations in the UK were particularly hard hit, with over 48 hospitals being infected. Within the USA, power injectors manufactured by Bayer Medrad used to inject IV contrast became infected [12]. The vulnerability exploited by WannaCry propagated through an exploit developed by the US National Security Agency known as EternalBlue. Existence of the exploit was stolen and leaked by a group called The Shadow Brokers. Microsoft was aware of the exploit and had released a patch to close it. Therefore, only organizations that had not applied this patch or organizations using older Windows systems that were past their end-of-life cycle were vulnerable to WannaCry. The healthcare environment learned two important lessons: first, the importance of installing software updates to minimize risk from known cybersecurity vulnerabilities and, second, the need to consider software life cycles in addition to hardware life cycles when purchasing capital equipment. Often the hardware components of equipment purchased by a healthcare organization are expected to function for 15–20 years. But the underlying software usually becomes obsolete much more quickly. This means that the software is no longer supported by the vendor and that updates will no longer be released to correct for vulnerabilities detected beyond the end-of-service date. This was the case with the Bayer Medrad power injector. Such equipment poses an unacceptable cybersecurity risk to organizations.

A complete cybersecurity safety communications issued by the FDA is available on their website [13]. To date, the FDA is not aware of any patient injuries or deaths associated with cybersecurity incidents.

**Motivations of Hackers**

Financial gain is the most common motivation driving hackers with malicious intent to disrupt or manipulate the function of computers and/or to steal valuable personal data. However, the direct financial link may not be readily apparent. Take for example the Anthem and Equifax cybersecurity breaches. The data stolen included personal and financial identifiers, which could be used possibly to make financial transactions. Alternatively, the data could be used to manip-
ulate the individual’s behavior. An intelligence officer in financial distress may be more susceptible to bribery. There are other reasons hackers might be motivated. Individuals or groups known as hacktivists may try to disrupt access to an organization’s website and/or deface its webpages to publicize a political or ideological stance or to protest an organization’s activity. Causing disruption and causing fear are also potential motivating factors.

Countries that lack traditional military power may try to make up for it through technology and the use of cyberattacks. This technique, known as asymmetrical warfare, has been successfully employed by Iran to disrupt US interests [14]. While most attacks have focused on financial institutions, in 2018, an attack on a Saudi Arabian petrochemical company nearly succeeded in causing an explosion that would have resulted in fatalities [15]. The sophisticated attack targeted Schneider’s Triconex controllers, which keep the equipment operating safely by performing tasks like regulating voltage, pressure, and temperatures. The only reason an explosion did not occur was due to a mistake in the attacker’s computer code. Those controllers are used in about 18,000 plants around the world, including nuclear and water treatment facilities, oil and gas refineries, and chemical plants. Cyberwarfare is not likely to inflict significant short-term damage, but it may have insidious effects causing irritation, confusion, and a loss of confidence in trusted institutions.

**Common Hacking Attacks**

Computer hacking techniques continue to evolve and increase in sophistication. An attack may actively seek to alter a system’s or device’s operation or passively obtain data to learn or make use of information gathered. Attacks typically fall into one of the following categories: [16].

**Backdoor**

- A backdoor in a computer system is any secret method of bypassing normal authentication or security controls. They may exist for several reasons, including by original design or from poor configuration. They may have been added by an authorized party to allow some legitimate access or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.

**Denial of service**

- Denial of service (DoS) attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim’s account to be locked, or they may overload the capabilities of a machine or network and block all users at once.
Direct access attacks

- In this instance, an attacker gains physical access to a computer and may copy data from it or compromise security by making operating system modifications; installing software worms, keyloggers, and covert listening devices; or using wireless mice.

Eavesdropping

- Eavesdropping is the act of surreptitiously listening to a private computer “conversation” (communication), typically between hosts on a network. The FBI and NSA have used eavesdropping on the systems of internet service providers.

Phishing

- Phishing refers to a common method of attempting to deceive a user to provide sensitive information such as usernames, passwords, and credit card details. Phishing is typically carried out by email spoofing (defined below), and it often directs users to enter details at a fake website whose “look” and “feel” are almost identical to the legitimate one. The fake website often asks for personal information, such as login details and passwords. This information can then be used to gain access to the individual’s real account on the real website. Preying on a victim’s trust, phishing can be classified as a form of social engineering.

Privilege escalation

- Privilege escalation describes a situation where an attacker with some level of restricted access can, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to exploit a vulnerability in the system to gain access to restricted data or even become “root” and have full unrestricted access to a system.

Social engineering

- Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer.

Spoofing

- Spoofing is the act of masquerading as a valid entity through falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain. There are several types of spoofing, including the following:
  - Email spoofing, where an attacker forges the sending (From, or source) address of an email
  - IP address spoofing, where an attacker alters the source IP address in a network packet to hide their identity or impersonate another computing system
  - MAC spoofing, where an attacker modifies the Media Access Control (MAC) address of their network interface to pose as a valid user on a network
  - Biometric spoofing, where an attacker produces a fake biometric sample to pose as another user

Tampering

- Tampering describes a malicious modification of products. So-called “Evil Maid” attacks and security services planting surveillance capability into routers are examples.

Infrastructure to Reduce Risks and Identify Vulnerabilities

US Food and Drug Administration

The US FDA allows devices to be marketed when there is a reasonable assurance that the benefits to patients outweigh the risks. Medical devices are increasingly connected to the internet and to other medical devices which enables features that improve healthcare and allow more patient-focused delivery of care [13]. However, these features also increase the risk of cybersecurity threats. The FDA does not conduct premarket testing of products for cybersecurity, and it views cybersecurity to be the responsibility of manufacturers, healthcare delivery organizations, physicians, and patients working together. Specifically, the FDA states that medical device manufacturers must remain vigilant in identifying risks associated with their medical devices. Healthcare delivery organizations must evaluate their networks and protect their systems. Both the manufacturer and the healthcare delivery organization must work together to put appropriate mitigation in place to minimize patient risk. Medical staff and patients must understand their roles in minimizing cybersecurity risks.

The FDA issues guidance documents for industry to assist manufacturers in developing products using methodology that the agency recognizes as robust and associated with best manufacturing processes. Vendors are not required to follow FDA guidance, but doing so often facilitates the review process, expediting final approval. The FDA has issued three
cybersecurity guidance documents and is in the process of completing the fourth [13]. Guidance is divided into premarket submissions (for vendors developing new medical devices not yet approved by the FDA) and postmarket guidance (management of cybersecurity for devices throughout the product life cycle that have received FDA approval and are being marketed and distributed).

FDA Guidance for Premarket Management of Cybersecurity in Medical Devices
The FDA’s guidance document for premarket submission of cybersecurity in medical devices is in draft form, and details are subject to change [17]. However, the general intent is to provide recommendations to industry regarding cybersecurity device design, labeling, and documentation. The FDA recommends software design and validation include a set of cybersecurity design controls to ensure medical device cybersecurity and to ensure the medical device functions safely and effectively. If the manufacturer chooses to follow the FDA guidance document it, is more likely the agency will find the device meets requirements for approval.

FDA Guidance for Postmarket Management of Cybersecurity in Medical Devices
The FDA’s postmarket management of cybersecurity in medical devices guidance document provides recommendations to industry for structured and comprehensive management of cybersecurity vulnerabilities of devices throughout the product life cycle after they have been approved by the agency and the products are being marketed and distributed [13]. This document emphasizes that manufacturers must monitor, identify, and address cybersecurity vulnerabilities as part of their postmarket management of medical devices. It also clarifies when a cybersecurity update must be reported to the FDA. The majority of routine cybersecurity updates and patches are considered device enhancements, and the FDA does not require advanced notification by the company or approval. However, if a cybersecurity vulnerability poses a potential health risk, the FDA requires the device manufacturer to notify the agency. Risk is assessed based on an evaluation of the likelihood that a vulnerability might be exploited and the potential impact of exploitation on the device’s safety and performance and the severity of patient harm if exploited.

The Association for the Advancement of Medical Instrumentation

The Association for the Advancement of Medical Instrumentation (AAMI) is a voluntary organization of representative engineers from industry, healthcare professionals, regulators, scientists, academics, and other interested parties for the purpose of advancing the development of medical devices as well as safe and effective use of medical technology. It serves as a unique forum for convening industry engineers across a broad range of medical specialties and provides a structure for engineers from otherwise competing vendors to collaborate with each other in order to develop or revise existing practice standards that address the use, care, and processing of performance requirements to be met by medical devices and technology. Well over 100 committees exist covering topics ranging from standard related to external cardiac defibrillators and automatic external defibrillators (Defibrillator Committee) to standard dealing with diagnostic, cardiac, and ambulatory electrocardiographic monitoring equipment as well as the cables, leads, and arrhythmia monitoring electrodes used for ECG machines (ECG Committee), to standards related to devices that measure intracranial pressure (Intracranial Pressure Device Working Group), and to a group that develops performance and safety standards for sharps containers (Sharps Containers Working Group) [18]. The Cardiac Rhythm Management Device Committee has been responsible for developing many of the CIED standards that cardiac electrophysiologists take for granted. These include, for example, the IS-1 and DF-4 lead standards and the battery status indicator standards (elective replacement indicator, end-of-service indicator). The work product of the AAMI committees and working groups for medical devices are technical information reports. Once these are approved by AAMI, they are considered binding by the manufacturers that participated in their development.

The AAMI Device Security Working Group is the forum in which the cardiac rhythm management industry, regulators, cybersecurity experts, healthcare professionals, and other interested parties have developed two technical information reference documents related to cybersecurity of medical devices: AAMI TIR57: Principles for medical device security – risk management giving guidance for premarket product development and AAMI TIR97: Principles for medical device security – postmarket risk management for device manufacturers.

AAMI TIR57, published in 2016, provides medical device manufacturers with guidance on developing cybersecurity risk management processes in new product development. This guidance document has been recognized by the FDA. It applies standards-based principles to minimize security threats that could impact confidentiality, integrity, and/or availability of a medical device or information processed by the device. TIR57 lists six steps involved in the security risk management process: security risk analysis, security risk evaluation, security risk control, evaluation of overall residual security risk acceptability, security risk management report, and production and postproduction information. AAMI TIR97, published in 2019, is meant to compliment
TIR57 by extending guidance to the production and postproduction phases of the medical device life cycle.

Together, TIR57 and TIR97 provide robust guidance to industry for developing products that are more resistant to hacking, more likely to fail “gracefully” rather than catastrophically if hacked, and able to receive cybersecurity updates, just to name a few of the benefits. These guidance documents complement the FDA cybersecurity guidance documents and give industry a clear recommendation on best practices.

**Evaluation Process for Potential Vulnerabilities**

The US Department of Homeland Security’s (DHS’s) National Cybersecurity and Communications Integration Center (NCCIC) is tasked with analyzing and reducing cybersecurity threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities (Fig. 29.3). When an incident occurs or is reported, NCCIC triages and collaborates a response to the incident. The FDA becomes involved in the evaluation of a threat if it is deemed possible to result in patient harm. In such an event, the agency’s role and responsibilities fall largely in line with non-cybersecurity responsibilities. For example, in the event of a CIED cybersecurity vulnerability, the FDA’s Center for Devices and Radiological Health (CDHR) interacts with the manufacturer to assess the vulnerability and develop mitigating and/or corrective action. In the event of a cybersecurity breach in which protected health information is exposed, the Department of Health and Human Services (HHS) Office for Civil Rights may coordinate with affected health plans, healthcare clearinghouses, and healthcare providers. The operating divisions of HHS such as the FDA, Office for Civil Rights, Office of the National Coordinator for Health Information Technology (electronic health records), and Office of the Assistant Secretary for Preparedness and Response coordinate regularly within the HHS Cybersecurity Working Group and on an as-needed basis, through established mechanisms, and during cyber events, such as WannaCry. Interactions between HHS and other agencies such as DHS and the FBI also occur on a routine and event basis.

**NIST Cybersecurity Framework**

Evaluating and managing cybersecurity risks is now of paramount importance to national security, economic stability, as well as public safety and health. Yet most organizations do not have the necessary expertise or resources to assess and minimize their vulnerabilities. Recognizing this, on December 18, 2014, the US federal government signed into law the Cybersecurity Enhancement Act of 2014 [19]. The Act authorized the National Institute of Standards and Technology (NIST) to develop a voluntary framework that organizations of any size would be able to apply to assess and reduce cybersecurity risks [20]. Published on April 16, 2016, the NIST cybersecurity framework enables organizations – regardless of size or cybersecurity sophistication – to apply the principles and best practices of risk management to improve their organizations’ security and resilience.

The framework provides a common organizing and structured approach to cybersecurity by assembling standards, guidelines, and best practices of risk management to improve security and resilience. The core consists of five activities or functions designed to achieve specific security outcomes (Fig. 29.4a). The first step is to identify what assets are potentially vulnerable. The second step is to develop and implement safeguards to ensure proper function of assets. In the event an intrusion occurs, there must be appropriate

---

**Fig. 29.3** Evaluation and notification sequence of a new cybersecurity vulnerability threat: Assessment of a potential cybersecurity vulnerability requires expertise from the Department of Homeland Security’s National Cybersecurity and Communications Integration Center and the manufacturer. The FBI becomes involved if there is potential criminal activity. If the vulnerability is validated, the discussion between a healthcare professional and patient should consider these five topics. If the claim of a new vulnerability is released directly to the public, there will be a period of uncertainty and anxiety while the claim is being evaluated.
tools to identify a potential cybersecurity intrusion and then a mitigation strategy to contain the impact of the potential cybersecurity event. Last, there should be a plan to restore functions impaired by a cybersecurity event and associated data with minimal disruption to services. The NIST CCF was developed for use by organizations of all sizes and is useful as we consider cybersecurity of CIEDs both within the healthcare delivery organization (HDO) and beyond, through remote monitoring. An example of how the NIST cybersecurity framework could be applied to a CIED device clinic is provided in Fig. 29.4b.

Role of Supply Chain Management

Managing cybersecurity risk has become a critical function of supply chain management. The point of purchase is now an important juncture at which point both the purchaser and the supplier are able to review the needs and capabilities of their respective organizations. It is essential that a healthcare organization understands what equipment (both hardware and software) exists under its purview so that if at a future point in time a cybersecurity vulnerability is identified, the organization will be aware

**Table: NIST Framework Core Applied to CIED Clinic**

| Stage of Framework Core | Action | Vendor Responsibility | Health Care Delivery Organization Responsibility |
|-------------------------|--------|-----------------------|---------------------------------------------------|
| Identify                | Identify assets that need to be protected | CIED Programmer integrity (computer code and configuration) | Hospital IT equipment |
| Protect                 | Develop and implement safeguards to ensure proper function of assets. | Follow NIST guidance to implement controls appropriate for CIED programmer | Physical access to programmers |
| Detect                  | Develop and implement appropriate activities to identify a potential cybersecurity intrusion. | Cybersecurity log collection: Service technician uploads programmer logs (for non-networked programmers) | Electronic health record, PCs, operating systems, wireless networks, etc. |
|                         | | Vendor monitors programmer files streamed to vendor portal (for networked programmers) | Physical location |
|                         | | Intrusion detection system, traffic pattern monitoring, malware scanning. Cameras to protect physical location. | Login/passwords |
|                         | | Monitor user access | Background check of employees |
| Respond                 | Develop ability to contain the impact of a potential cybersecurity event. | Restore programmer to secure state, patch if needed | Hospital IT: Incident response, patching, network restrictions. |
|                         | | | Physical location of programmers: Law enforcement |
|                         | | | Unauthorized access: User ID/Password deprovisioning, blacklisting |
| Recover                 | Develop ability to restore functions impaired by a cybersecurity event and associated data with minimal disruption to services. | Restore PHI if possible | Hospital IT: Restore data |
|                         | | | Physical location: repair physical breach. |
|                         | | | User ID/Password: Reprovisioning |

Fig. 29.4 (a) The NIST framework applied to evaluate and manage security risk for a CIED clinic. In this example, the responsibility for the actions at each stage of the framework is assigned to the appropriate vendor or the healthcare delivery organization. Physical and electronic security of vulnerable assets must be considered. CIED cardiac implantable electronic device, IT information technology, PHI personal health information, NIST National Institute of Standards and Technology, PC personal computers. (b) The NIST framework applied to evaluate and manage security risk for a CIED clinic. In this example, the responsibility for the actions at each stage of the framework is assigned to the appropriate vendor or the healthcare delivery organization. Physical and electronic security of vulnerable assets must be considered. CIED cardiac implantable electronic device, IT information technology, PHI personal health information, NIST National Institute of Standards and Technology, PC personal computers.
of its risk and be able to isolate and eventually patch that risk. Obtaining a software bill of materials (SBOM) from a vendor at the point of purchase is now standard operating procedure. Software is typically created by assembling a combination of open source and commercially available software components. The SBOM lists the individual components of software. This is important because if, at a point in the future, an individual software component is identified as having a vulnerability, the organization will be able to identify its risk and be able to take mitigative and corrective action.

Archimedes Center for Medical Device Security

Until recently, security in the healthcare industry was often an afterthought, with priority given to innovation. This left many organizations struggling to catch up to understand the security concerns and develop strategies to meet their needs. The Archimedes Center for Medical Device Security, based at the University of Michigan School of Computer Science and Engineering, was founded in 2008 by Kevin Fu in part to raise awareness of the looming threat to the healthcare industry and to serve as a resource to industry, healthcare organizations, academia, and regulatory agencies to educate, collaborate, and promote implementation of security standards across the industry [21].

Despite increased awareness, cyberattacks on the healthcare industry continue to grow, with over 750 healthcare providers in the USA being attacked with ransomware in 2019 [22]. Most recently, the World Health Organization and healthcare organizations on the front line of fighting the COVID-19 pandemic have been targeted by cybercriminals [23, 24]. The financial costs of cybersecurity breaches are higher than other industries, but the bigger concern goes beyond finances. Recent attacks have resulted in interruption of 911 systems, patient record deletions, cancelled surgeries, and some practices being forced to close [22]. The Archimedes Center, which hosts an annual leadership workshop in cybersecurity as well as a medical device security 101 conference for participants of all levels of expertise, provides an industry-neutral forum in which medical device manufacturers, regulators, healthcare delivery organizations, and other interested stakeholders can convene to learn and network to keep up to date with this rapidly evolving field.

Role of Healthcare Providers

When confronted by cybersecurity concerns, the initial reaction of healthcare providers is to point to the medical device and health information technology industries. The topic is a black box for most providers, and they assume it requires technical expertise beyond their level of knowledge. As the Anthem cybersecurity hack demonstrated, humans at all levels of an organization remain the most common access points for intruders [8]. It is therefore necessary that providers and support staff receive appropriate education on basic cybersecurity practices and be instructed to report any suspicious findings to the appropriate authority within the organization (Table 29.1).

Healthcare providers of patients with CIEDs serve a unique and critical role in educating patients on the importance of proper cybersecurity practices, including the likelihood that their device will require software updated during the device life cycle. Introducing this concept to patients even prior to device implant sets patient and family expectations and serves the important function of educating them that cybersecurity is a concern and that there are ongoing processes in place to minimize risks. Most individuals appreciate the importance of updating software on smartphones or PCs, and so it is a familiar concept that they can extend to CIEDs. In the event that a cybersecurity vulnerability is identified, patients depend upon their provider to help interpret the level of risk associated with the vulnerability and weigh that risk against the known benefits of the therapy. While patients appreciate that the provider is not a cybersecurity expert, they also view their provider as uniquely qualified to assess the potential benefit of a medical therapy for an individual patient and weigh that against a possible cybersecurity threat as described by a true cybersecurity authority [25]. It is important to take into consideration the ease of exploiting a potential vulnerability as well as the consequences if it occurred. In the case of the Muddy Waters examples, even though the vulnerabilities were ultimately confirmed, the resources required to exploit them were significant and would have required a hacker to be in close proximity to a patient. Such factors need to be considered when advising patients. Often there may be strategies that can be employed to mitigate the risk of exploitation of a vulnerability until a software patch is available. Once a security update has been issued, there is a small and difficult to quantify risk that installing the patch will result in unanticipated consequences, potentially resulting in more rapid battery
depletion or even device malfunction. Therefore, the clinician’s expertise is again required to advise the patient on the potential risks and benefits of the update compared with the risk of the vulnerability being exploited, all in the context of the relative benefit of the therapy for the patient.

**Coordinated Disclosure**

The vast majority of cybersecurity vulnerabilities are identified by the cybersecurity research community. These individuals and organizations seek to identify potential vulnerabilities and responsibly report them to the National Cybersecurity and Communications Integration Center as well as the device manufacturer (Fig. 29.3). The manufacturer then evaluates the claim and determines if it is valid and whether a software patch is required. If there is a potential for patient harm, the US FDA also becomes involved. If the claim is validated, the manufacturer and FDA develop a strategy to mitigate the risk. Only once this process has been completed is a formal announcement released to the public. This process, called coordinated disclosure, minimizes the risk of public confusion, fear, and misinformation and is therefore the optimal sequence of events. However, it is always possible for an individual or organization to release notice of a potential vulnerability directly to the public as Muddy Waters did in 2016. When a claim is released directly to the public, the manufacturer, and the medical community simultaneously, there will necessarily be a period of uncertainty, confusion, and ultimately fear. The manufacturer must evaluate the claim, while the medical community has insufficient evidence with which to guide patients. In

| Topic | Action/Impact |
|-------|---------------|
| Physical security | Restricting physical access to specific areas and equipment within the healthcare environment is an important component of cybersecurity. CIED programmers illustrate the reasons for this: Programmers must be immediately available to providers in case of an emergency. Limiting access by password protection is more likely to result in patient harm as the risk of unauthorized use is lower than the frequency of patients requiring urgent evaluation and/or reprogramming of a CIED. Restricting access to programmers will deter unauthorized use by a potential bad actor. |
| Social engineering | Understand the role of social engineering in cybersecurity breaches. Be aware that requests to disclose sensitive information such as passwords, credit card numbers, etc. may come from sources with malicious intentions who may try to impersonate an individual or source of authority such as a supervisor, bank, or business partner. Be alert for possible email phishing schemes. |
| Role of supply chain management | The point of purchase/acquisition has become a critical juncture at which an organization must evaluate and understand What potential vulnerabilities a new product might introduce to their organization What steps the manufacturer has taken to address these potential risks An organization must also obtain a software bill of materials (SBOM) listing each software component so that in the event of a vulnerability being identified in the future, the organization will be aware of its risk and be able to take mitigating actions. |
| Software updates and product life cycle | Routine software updates are a critical tool used by manufacturers to both add and improve functionality but also patch potential cybersecurity vulnerabilities as they are identified. Installing recommended updates is an important component of reducing the risk of cybersecurity breaches. A product’s software life cycle must be considered and tracked by an organization. Any product in use beyond the manufacturer’s supported software life cycle is a potential cybersecurity vulnerability to the organization. |
| Patient education | Patients expect their provider to be their advocate and advise them in the case of a cybersecurity vulnerability. If a vulnerability is identified, the provider should be able to explain Potential consequences if it is exploited Options to mitigate risk of exploitation Relative ease/likelihood of exploiting the vulnerability Benefits of therapy vs. risk if cybersecurity vulnerability is exploited Long-term solutions to eliminate vulnerability Risks associated with software/firmware update if/when it becomes available |
| Process for evaluating potential cybersecurity vulnerabilities | Most vulnerabilities are identified by cybersecurity researchers. Once identified, researchers inform the manufacturer and the National Cybersecurity and Communications Integration Center. The manufacturer is responsible for informing the FDA if there is a potential for patients to be harmed. |
| Coordinated disclosure | Cybersecurity researchers and manufacturer work together to verify a potential vulnerability. The manufacturer develops strategy to mitigate or eliminate vulnerability. The public is then informed of both the vulnerability and mitigation strategy simultaneously. |
these instances, generating fear and confusion may be the goal of the individual or organization releasing the claim. Coordinated disclosure is always the preferred route, but the possibility of claims being released to the public directly will always remain a possibility. By educating patients up front about cybersecurity risks, periodic software updates, and possible strategies to mitigate a cybersecurity vulnerability, they will be less likely to panic and act without consulting their provider.

**Privacy Regulations**

Responding to the vast quantities of personal data collected – both legally and illegally – the European Union and the state of California have introduced sweeping new privacy regulations. While not directed specifically at the medical community, these regulations have profound implications for healthcare organizations, the medical device and information technology industries, and healthcare providers. The European Union’s General Data Protection Regulation (GDPR) and California’s Consumer Privacy Act (CCPA) both aim to give individuals control over their personal data and simplify the regulatory environment. While there are important differences between GDPR and CCPA, the underlying aims are similar: both govern how personal information may be collected and managed, with a clear structure of accountability in the event that data security becomes compromised as well as a mechanism for an individual to question or revoke an organization’s permission to have access to their personal information (the right to be forgotten).

The GDPR categorizes any individual or organization collecting and retaining personal data as a “data controller.” Individuals or organizations that may assist the data controller in processing the personal data (e.g., a cloud storage vendor) are categorized as “data processors.” The GDPR grants individuals the right to request information from a data controller about how their personal data is being stored and how it is being used, and they have the right to access their own data. They also have the right to be forgotten and have their data erased. Individuals also are granted the right of data portability. They must be able to receive their personal data in a structured, commonly used, and machine-readable format that allows them to transmit the data to another controller. Potentially crippling financial fines may be levied against individuals or organizations that fail to comply with the GDPR requirements. The first fine of a healthcare institution occurred in July 2019 for a breach of a single patient’s medical record, which occurred in 2018. Authorities in the Netherlands issued a $516,000 fine against the Haga Hospital in The Hague after a well-known Dutch person’s medical record was viewed without authorization by several hospital employees. Investigators concluded that the hospital (the data controller) had poor internal security controls and was not taking appropriate security measures to protect personal data in violation of the GDPR requirements.

GDPR has significant implications for all parties involved in remote monitoring of CIEDs. Both the manufacturer of the device and the practice managing the patient with a CIED are considered data controllers, while the myriad of vendors involved in storing and communicating the data both for the manufacturer and the practice are considered data processors. In order to comply with the GDPR requirements, patients must be informed of each vendor or individual involved in this process along with contact information sufficient to allow patients their rights under the regulation (right to access data, right to be forgotten, and right to receive their data in a structured commonly used machine-readable format). An upcoming guidance document from the European Society of Cardiology/European Heart Rhythm Society is tasked with advising clinicians and other involved parties how to most effectively comply with the regulation. When offered remote monitoring of their CIEDs, patients in the European Union will be presented with a lengthy consent form explaining the regulations as well as the necessary documentation regarding the data controllers and data processors specific to their healthcare provider and CIED manufacturer.

**Conclusion**

The risk of cybersecurity hacking and data theft is a reality of the new, interconnected environment in which we exist. Healthcare is particularly vulnerable because of the potential value of personal data as well as the complexity and interconnected nature of the modern healthcare environment. While cybersecurity vulnerabilities of medical devices have been detected, to the best of our knowledge, no patients to date have been harmed. But the motivation and innovation of hackers must not be underestimated, particularly given the potential value of the data. The FDA and medical device industry have developed robust new guidance documents for manufacturers to build devices with increased attention to cybersecurity making them more difficult to hack and less vulnerable to catastrophic failure. These documents also include guidance to develop tools for devices to monitor their function and warn of possible intrusion, and they make it easier for manufacturers to provide software updates throughout the device life cycle. But these actions will take some time to have full effect as older products will remain in use for at least 5–10 years. Healthcare providers, institutions, and patients must participate as equal partners with industry and regulatory agencies if the risks of cybersecurity breaches are to be effectively minimized. No device will ever be invulnerable to hacking (unless we return to the earliest pacemaker
in which the rate could only be adjusted with a screwdriver). Emerging privacy regulations – while well intentioned – may have the unintended consequence of discouraging the use of beneficial therapies such as CIED remote monitoring due to the burden they impose. We, as healthcare providers, must advocate for our patients to ensure there is a proper balance of security and privacy while still promoting innovation and delivery of therapies that have been demonstrated to be effective and meaningfully beneficial for patients. The benefits of advanced technologies are tremendous, and with cooperation and all parties working together, the risks can be managed.

**References**

1. Muddy Waters is Short St. Jude Medical (STJ:US) - Muddy Waters Research [Internet]. https://www.muddywatersresearch.com/. 2016 [cited 2020 Aug 2]. Available from: https://www.muddywatersresearch.com/research/stj/mw-is-short-stj/.

2. St. Jude response to cybersecurity protections [Internet]. https://www.abbot.com/consumer/cardiovascular.html. 2016 [cited 2020 Jun 29]. Available from: https://www.cardiovascular.abbot/content/dam/bss/divisionalsites/cvs/pdf/guides/merlin-patient-letter.pdf.

3. Archimedes Center for Medical Device Security. Holes found in report on St. Jude medical device security - University of Michigan News [Internet]. 2016 [cited 2020 Aug 2]. Available from: https://news.umich.edu/holes-found-in-report-on-st-jude-medical-device-security/.

4. U.S. 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 | FDA [Internet]. 2017 [cited 2020 Aug 2]. Available from: https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals.

5. MatthewGreen. A few notes on medsec and St. Jude Medical [Internet]. https://blog.cryptographyengineering.com/2018/02/17/a-few-notes-on-medsec-and-st-jude-medical/. 2018 [cited 2020 Aug 2]. Available from: https://blog.cryptographyengineering.com/2018/02/17/a-few-notes-on-medsec-and-st-jude-medical/.

6. Reuters. FDA warns of security flaw in Hospira infusion pumps - Reuters [Internet]. https://www.reuters.com/article/us-hospira-fda-cybersecurity-idx/USKCNOQ52GJ20150731. 2015 [cited 2020 Aug 16]. Available from: https://www.reuters.com/article/us-hospira-fda-cybersecurity-idx/USKCNOQ52GJ20150731.

7. Wall Street Journal. Health Insurer Anthem hit by hackers [Internet]. https://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720?mod=article_inline. 2015 [cited 2020 Aug 17]. Available from: https://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720?mod=article_inline.

8. BankInfoSecurity. A new in-depth analysis of Anthem Breach [Internet]. https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627. 2017 [cited 2020 Aug 17]. Available from: https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627.

9. Wall Street Journal. Chinese national indicted on hacking charges related to Anthem Breach [Internet]. https://www.wsj.com/articles/chinese-national-indicted-on-hacking-charges-related-to-anthem-breach-11557433541. 2019 [cited 2020 Aug 17]. Available from: https://www.wsj.com/articles/chinese-national-indicted-on-hacking-charges-related-to-anthem-breach-11557433541.

10. Wall Street Journal. Four members of China’s Military indicted over massive Equifax Breach [Internet]. https://www.wsj.com/articles/four-members-of-china-s-military-indicted-over-massive-equifax-breach-11581346824?mod=hp_lead_pos1. 2020 [cited 2020 Aug 17]. Available from: https://www.wsj.com/articles/four-members-of-china-s-military-indicted-over-massive-equifax-breach-11581346824?mod=hp_lead_pos1.

11. Wikipedia. WannaCry ransomware attack [Internet]. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack. 2018 [cited 2020 Aug 17]. Available from: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

12. Forbes. Medical devices hit by ransomware for the first time in US hospitals [Internet]. https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#29676fc6425c. 2017 [cited 2020 Aug 17]. Available from: https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#29676fc6425c.

13. U.S. Food and Drug Administration. Cybersecurity [Internet]. https://www.fda.gov/medical-devices/digital-health/cybersecurity. 2020 [cited 2017 Aug 17]. Available from: https://www.fda.gov/medical-devices/digital-health/cybersecurity.

14. The United States Institute of Peace. The invisible U.S.-Iran Cyber War - The Iran Primer [Internet]. https://iranprimer.asip.org/blog/2019/oct/25/invisible-us-iran-cyber-war. 2019 [cited 2020 Aug 17]. Available from: https://iranprimer.asip.org/blog/2019/oct/25/invisible-us-iran-cyber-war.

15. The New York Times NPCK. A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try [Internet]. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html. 2018 [cited 2020 Aug 17]. Available from: https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

16. Wikipedia. Computer security [Internet]. https://en.wikipedia.org/wiki/Computer_security#Vulnerabilities_and_attacks. 2020 [cited 2020 Aug 17]. Available from: https://en.wikipedia.org/wiki/Computer_security#Vulnerabilities_and_attacks.

17. U.S. Food and Drug Administration. Content of premarket submissions for management of cybersecurity in medical devices [Internet]. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices. 2018 [cited 2020 Aug 16]. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices.

18. Association for the Advancement of Medical Instrumentation. Technical standards development [Internet]. https://www.aami.org/standards/view-full-committee-list. 2020 [cited 2020 Aug 16]. Available from: https://www.aami.org/standards/view-full-committee-list.

19. Library of Congress. S.1353 - 113th Congress (2013-2014): Cybersecurity Enhancement Act of 2014 [Internet]. congress.gov. 2020 [cited 2020 Aug 17]. Available from: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

20. National Institutes of Standards and Technology. Cybersecurity framework [Internet]. https://www.nist.gov/. 2020 [cited 2020 Aug 17]. Available from: https://www.nist.gov/cyberframework.

21. Archimedes. Archimedes Center for Medical Device Security [Internet]. 2020 [cited 2020 Aug 24]. Available from: https://www.archimedes.org/

22. Emsisoft | Security Blog. The State of Ransomware in the US: report and statistics 2019 [Internet]. 2019 [cited 2020 Aug 17]. Available from: https://www.emsisoft.com/security_blog/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.
23. TheHill. Hackers are targeting the COVID-19 response and putting lives at risk [Internet]. 2020 [cited 2020 Aug 18]. Available from: https://thehill.com/opinion/cybersecurity/500607-hackers-are-targeting-the-covid-19-response-and-putting-lives-at-risk.

24. World Health Organization. WHO reports fivefold increase in cyber attacks, urges vigilance [Internet]. 2020 [cited 2020 Aug 20]. Available from: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

25. Slotwiner DJ, Deering TF, Fu K, Russo AM, Walsh MN, Van Hare GF. Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians-proceedings of the Heart Rhythm Society’s leadership summit. Heart Rhythm. 2018;15(7):e61–7.