DO NO HARM

PROTECTING CONNECTED MEDICAL DEVICES, HEALTHCARE, AND DATA FROM HACKERS AND ADVERSARIAL NATION STATES

MATTHEW WEBSTER

Table of Contents

List of Tables

List of Illustrations

Figure 10-1: Network communication via the OSI model

Do No Harm

Protecting Connected Medical Devices, Healthcare, and Data from Hackers and Adversarial Nation States

Matthew Webster

WILEY

Introduction

Along with the expanding challenges of the COVID-19 pandemic was another pandemic hitting our hospitals and healthcare systems in the United States—ransomware. Ransomware is software that cybercriminals use to render a computer or machine unusable. They then demand a ransom for a code that will (ideally) enable the compromised organization to disable the software and restore the machine to a usable state. The vulnerabilities and the weaknesses inherent in internet-connected medical devices helps to enable these cybercriminals.

This book is about the relationships between vulnerable internet-connected medical devices, cybercriminals, and nation-state actors and how they not only take advantage of exceptionally vulnerable devices, but also profit from it.

But the story relating to insecure medical devices is much deeper than this. It is the story of American innovation and ingenuity—a story where cybersecurity often takes a back seat to the needs of saving human lives. That story, through no particular person's or organization's fault, has started to leave our hospitals in a more vulnerable state than ever before. Through the pandemic, the fundamental flawed state of many internet-connected medical devices, along with insufficient global legal protections, has allowed organized crime and nation-state actors to collect trillions of dollars.

If you care about your data, your privacy, and why the situation is so dire from a cybersecurity perspective, this book is worth reading. It also offers a glimpse inside the perspective of a Chief Information Security Officer

regarding the security and privacy of our data as a result of the decisions we have collectively made.

This book leans heavily on the cybersecurity perspective, as that is the perspective I know best. It does dive into the technical aspects of internet-connected medical devices, but then it jumps into law, big data, and other global challenges and ties them together in an overarching story about hospitals, data, and cybercriminals.

This book touches heavily on the technical aspects of protecting internet-connected medical devices, but its scope is much broader than that. It provides a larger legal, privacy, and threat landscape perspective, which completely shapes the context for why having insecure medical devices presents a challenge for today's hospitals.

What Does This Book Cover?

This book covers a broad range of subjects in and around the protection of data and the challenges related to IoMT.

Chapter 1: The Darker Side of High Demand This chapter sets the stage for why internet-connected medical devices are so insecure. It explores some of the chief drivers for today's healthcare and why healthcare tends not be overly focused on cybersecurity, historically speaking.

Chapter 2: The Internet of Medical Things in Depth This chapter dives into the technical side of internet-connected medical devices. It defines what is and is not an internet-connected medical device, and explores the larger context of those devices and how they fit together with other technologies.

Chapter 3: It Is a Data-Centric World This chapter explores many of the different facets of what is and is not medical data. The definition is often blurrier than we might expect, and the ramifications can be large—especially once big data is part of the overarching picture. The ramifications and risks are often not what they may seem.

Chapter 4: IoMT and Health Regulation This chapter covers how HIPAA and other regulations relate to the deluge of data created as a result of internet-connected medical devices. It also looks at the enforcement mechanisms related to HIPAA through the Office of Civil Rights.

Chapter 5: Once More into the Breach This chapter focuses on the actions of cybercriminals once they take initial steps into an organization. It covers why cybersecurity is so difficult with the vulnerabilities

that internet-connected medical devices have and how attackers take advantage of those vulnerabilities.

Chapter 6: Say Nothing of Privacy This chapter explores the history and evolution of privacy and how that privacy relates to both HIPAA data and the proliferation of data relating to internet-connected medical devices. It also brings surprising ties to big data and the challenges to the data market.

Chapter 7: The Short Arm of the Law This chapter explores the global legal landscape and the related enforcement challenges and how that landscape only amplifies the challenges related to vulnerable internet-connected medical devices.

Chapter 8: Threat Actors and Their Arsenal This chapter explores, at a high level, the various threat actors, some of the characteristics of their arsenal, and why they are so effective at their tradecraft.

Chapter 9: Enter Cybersecurity This chapter provides an in-depth introduction to what cybersecurity is. It explores some of the basic tradecraft of cybersecurity and related disciplines.

Chapter 10: Network Infrastructure and IoMT This chapter explores what a network is, how it is set up, and some basic network architectures and tools that can be used to protect internet-connected medical devices from harm.

Chapter 11: Internet Services Challenges This chapter reviews some of the basic services of the internet and how those services relate to internet-connected medical devices.

Chapter 12: IT Hygiene and Cybersecurity This chapter describes the basics of IT hygiene, what it is,

and why it is important. IT hygiene is also something that is not possible with internet-connected medical devices, which brings increased risks to those devices.

Chapter 13: Identity and Access Management This chapter explores the complex world of identity and access management. It touches on the technology, the governance, the challenges that many internet-connected medical devices have, and how internet connected medical devices affect the security posture of organizations.

Chapter 14: Threat and Vulnerability This chapter explores the various tools and techniques related to discovering vulnerabilities within an environment and the associated challenges with internet-connected medical devices.

Chapter 15: Data Protection This chapter explores some basic data protection strategies, governance, and tools related to protecting data. It has ties back to privacy, big data, IT, and other considerations.

Chapter 16: Incident Response and Forensics This chapter explores incident response and forensics from a disciplinary perspective and how internet-connected medical devices can be a challenge to the two disciplines.

Chapter 17: A Matter of Life, Death, and Data This chapter takes a step back from the details of cybersecurity to examine how all of the cybersecurity considerations fit into the bigger governance frameworks and why decision-making can be so challenging.

Chapter 18: Seeds of Change This chapter explores some of the changes we need to better protect

internet-connected medical devices. It explores everything from decision-making processes to hospitals, supply and demand, and so on.

Chapter 19: Doing Less Harm This chapter covers some strategies that we can focus on to optimize the overall balance between competing needs related to securing internet-connected medical devices.

Chapter 20: Changes We Need Despite the many we have talked about, there are still fundamental changes that need to take place in order to better protect hospitals, data, and internet-connected medical devices.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

To submit your possible errata, please email it to our Customer Service Team at wileysupport@wiley.com with the subject line “Possible Book Errata Submission.”

How to Contact the Author

We appreciate your input and questions about this book! Email me at awakenings@mindspring.com.

Part I
Defining the Challenge

If we step back and look at the big picture related to insecure internet-connected medical devices, the concerns are primarily around risks to healthcare organizations and risk to data. Fortunately, there have been very few deaths related to these insecure devices, but as adoption of internet-connected medical devices continues to rise, so will the associated risks. If COVID-19 has taught us one thing, it is that tragedy for some is an opportunity for others. From a cybersecurity perspective, it is important to understand who these actors are, what they are motivated by, and how can we stop, or at least reduce, the number and/or effectiveness of these attacks.

Before we can do this, it is extremely helpful to understand why poor security on internet-connected medical devices is such a challenge for IT and cybersecurity practitioners and why the devices have so many challenges to begin with. Looking at poor security as an origin story provides us with the context for understanding how to proceed. The world of IT, and especially internet-connected medical devices, is filled with a complex interrelation of social, technological, and economic challenges. It is important to understand this complex relationship if we are to devise a strategy for best protecting the devices, our hospitals, and the associated data.

As you read this first part of this book, keep the bigger picture in your head in order to more fully understand how we ended up where we are today. We have legal requirements that are not always followed by

manufacturers, which creates both challenges and victories for protecting our healthcare, our data, and occasionally our lives.

CHAPTER 1
The Darker Side of High Demand

The road to Hell is paved with good intentions.

—Henry G. Bohn, *A Handbook of Proverbs*, 1855

“First, do no harm” is attributed to the ancient Greek physician Hippocrates. It is part of the Hippocratic oath. The reality is that every day, doctors and hospitals need to make decisions about how to best help patients under the existing conditions. If doctors need to operate, they may harm the patient by making an incision—sometimes to save a patient's life. This is a calculated and acceptable harm from a moral perspective.

What isn't always as obvious to hospitals is the harm introduced by using an internet-connected medical device. In many cases, such as in hospitals, the doctors may have limited input about which devices are chosen for their environment. These devices have critical medical value not only for the hospital or doctor's office, but also from the patient's point of view. They are at the forefront of today's medical transformations. Often the harm that is introduced is unknown, unseen, or downplayed—if it is assessed at all.

This chapter explores, at a high level, the state of internet-connected medical devices and how those devices are impacting hospitals and unfortunately, and indirectly, human life. More importantly, this chapter covers the overall trends related to hospitals, partially as a result of internet-connected medical devices and how businesses evolved to the state they are in today. First, we need to

understand the risks that internet-connected medical devices pose.

Connected Medical Device Risks

What exactly are the risks related to internet-connected medical devices? The hit TV show *Homeland* popularized the idea of an attacker assassinating someone by taking over a pacemaker. While this is not beyond the realm of possibility, the most common forms of attack utilizing internet-connected medical devices are ransomware and distributed denial of service attacks (DDOS).[1] In the former case, the attacker takes over a system (often with malware, but sometimes with a password) and prevents (often through the use of encryption) the end user from using the system. In latter case, the attacker will own the device and use it to attack other sites.

Ransomware

Ransomware is essentially software that prevents systems from running. Criminals require that the owners pay to be able to gain access to their own systems. Imagine you had pictures of your family on your home computer and you could no longer access them unless you paid a fee. Now imagine critical medical systems rendered inoperable instead of family pictures. To make matters worse, once attackers are inside of systems, they often leave behind a way to gain access to them over and over again—meaning they are more susceptible to future attacks. This trend has only increased in the time of COVID. Obviously, the attackers do not care about the lives of others enough to not do the attacks.

Ransomware has been evolving tremendously over the last few years, and the number of the ransom demands has

gone up significantly from a few years ago. In 2019 alone, 764 healthcare providers in the United States were hit with ransomware.[2] One might be tempted to think that the attackers would not go after hospitals in a time of a global pandemic, but while this is the case for some attackers, the reality is that ransomware attacks are on the rise since COVID-19 hit.[3] What is worse is that while ransom demands used to be a few hundred dollars, now they are growing and are often more than a million dollars. With so much to gain, it is no wonder that ransomware demands are on the rise. Clearly, hospitals have a great deal of risk related to ransomware.

The effect that ransomware has had on hospitals is crippling. The attackers are well aware that COVID-19 has severely stretched the resources at hospitals. They know that this is a life-and-death situation, which makes hospitals even more likely to pay the ransom,[4] especially the smaller hospitals that may not have as mature of an IT and/or security program in place to protect their environments from the ravages of ransomware.[5] Essentially, they are easier targets. Sadly, even larger, more mature organizations are susceptible to ransomware attacks, but can sometimes respond to them more effectively.

September 10, 2020, unfortunately marks a grim milestone for ransomware—the first indirect death. A patient was rerouted from Duesseldorf University Hospital in Germany as 30 of its internal servers were hit with ransomware. As a result of the subsequent delay getting the much needed medical treatment, the patient died.[6] This particular attack was aimed at Heinrich Heine University and mistakenly hit the hospital because it is part of the same network. In this case, the perpetrators provided the keys to decrypt the systems and withdrew their extortion demands, but despite that, the hospital's systems were disrupted for a week.[7]

That was not the only death associated with ransomware in September 2020, unfortunately. Universal Health Services (UHS) was hit with a massive ransomware attack. UHS is a Fortune 500 company with more than 400 healthcare facilities in the U.S. and the UK. It provides services to more than 3 million patients yearly. In many cases whole hospitals were shut down and services were rerouted to other hospitals. Because of this rerouting of services, four people died.[8] With the frequency of ransomware growing, these kinds of problems will not only continue, but will likely become worse before they get better.

It is important to note that medical devices are not the only avenue for ransomware attacks, but they are, arguably, the most egregious vector due to the gaps in their fundamental security, inability to patch cybersecurity flaws in some circumstances, and the volume of problems they have—especially in the long run. One report shows that malware against internet-connected devices (not just medical devices) is up 50% from 2019.[9] That being said, they are a unique avenue due to the kinds of flaws they have. For example, the range of flaws in today's internet-connected medical devices is staggering. Take medical imaging devices: 70% of the devices are based on retired operating systems or systems that are under limited support.[10] The potential for vulnerabilities is extremely high. In many cases internet-connected medical devices run on Windows XP, which is no longer supported. There continues to be new vulnerabilities found—many of which allow complete compromise of the whole system. Associated with a compromised system is a whole host of risks, including everything from the system not functioning to data being exfiltrated. Either way, these are risks to both patients and to hospitals.

Now let us think about connectivity. Today's world is also much more connected than ever before. Many systems connect back to something referred to as “the cloud.” While I will go into greater depth in later chapters about the cloud, it should be noted here that the cloud aggregates and correlates data in one location. It also comes with a whole new set of risks that adds an extra layer of complexity for IT and cybersecurity teams.

Let's take a ransom in another direction—from a personal perspective. If you had a pacemaker, what would you be willing to pay to save your own life if someone threatened you with turning off the pacemaker? If attackers do not care about the lives of multiple people, they will not care about the life of one person. Attackers typically go for the easiest targets that offer the most reward. If they started targeting the rich who had internet-connected medical implants, that could be a lucrative route going forward. Of course this is not as lucrative as having a hospital pay a ransom.

Risks to Data

What does not often come to mind is the data risk related to internet-connected medical devices. Data can be as potentially deadly a risk as any device. An insulin pump that received the wrong amount of information can potentially kill someone with diabetes. A number of events can cause errors—everything from human error to machine flaws. This too deserves a much deeper dive as the data is far more interconnected than at any point in history, and that interconnection is only going to accelerate with the advent of new internet-connected medical devices.

Some risks are due to existing flaws in medical devices combined with the desire for people to have a better quality of life. For example, diabetics have hacked their

own pumps to achieve innovation the manufacturers have not. While many of the devices have been recalled, people have been hurt by insulin overdoses as a result of hacking their own devices.[11] Keep in mind that this was with commercial-grade systems that were attacked. These are not systems purchased off the black market.

Not everyone opts for commercially viable solutions. The cost associated with some of these solutions is too high for many to afford. As a result, they go through alternative sources that may not have the strict quality control that the commercial world has. In some cases, unknowingly, people will work with devices that are actually from the black market, such as insulin pumps that may be even less secure because they are not subject to the stronger regulation that exists today.[12]

While ransomware is taking the spotlight as of late, a host of other attacks are related to internet-connected medical devices. These will be described in greater detail in Chapter 8, but suffice it to say that numerous attacks can be leveraged, many of which could be avoided with sufficient cybersecurity practices. In many of these attacks, the attacker could have complete control of the data on the device. A few of the attacks against connected medical devices are listed in Figure 1-1, but this is far from a complete list. The lesson here is that quite often the vulnerabilities that can physically harm someone can also be leveraged to steal data. Data theft, by far, is much more common than the physical harm that could occur as a result of the internet connection. The stark difference is that the harm of data theft may or may not be known.

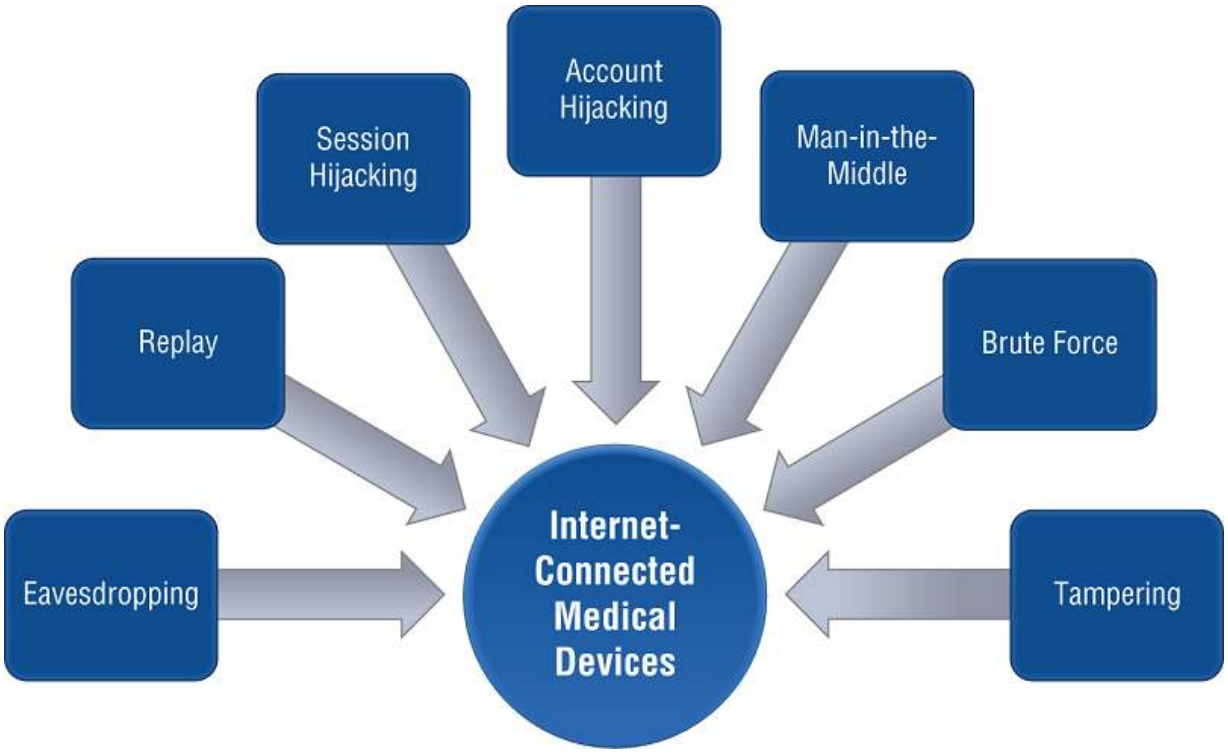

Figure 1-1: Example types of attacks against internet-connected medical devices

The vulnerabilities related to internet-connected medical devices are having an impact on organizations, and these weaknesses are not just trivialities. Nuspire, a managed security services provider, put out a few interesting statistics. The first statistic is that "18% of medical devices were affected by malware or ransomware in the last 18 months."[13] That is not a small number. Roughly 1 out of 5 devices have been affected by malware. If there is an average of 15 devices around a patient, roughly 3 of them have the possibility of being infected. Further, that malware can often be used to infect other devices. The other statistic that Nuspire mentioned was that "89% of health care organizations have suffered from an IoMT Related Security Breach." IoMT is short for internet of medical things. For our purposes, think of IoMT as internet-connected medical devices. That alone is another concerning statistic. It means that the connected medical

devices are a serious concern for healthcare organizations. It makes protecting these critical organizations all the more difficult.

If risks to human life are on one end of the spectrum, the other end of the spectrum relates to data risks. Healthcare data is one of the most sought-after data types on the internet. Security reports over the years have shown the value of a healthcare record to be worth anywhere from $10 to $1,000. By contrast, the typical credit card is worth only a few dollars. The reason is that most credit card companies have robust fraud departments that stop fraudulent transactions relatively quickly. After one or more transactions, the card is usually cut off. This is not typically true for health records. The process of detecting problems can take much more time.

From a patient perspective, the associated fraud can be a painful and lengthy road to deal with. Advisory Board, a leader in the healthcare advisory space, had an article that illustrated this quite clearly. A patient's identity was stolen, and the result was $20,000 worth of medical procedures that the victim was responsible for. It kept up over billing cycles, and the perpetrator was eventually caught and jailed, but there are still serious questions about the integrity of the victim's medical files.[14] Imagine what that can do to the victim. There may be conflicting information about the health information contained in many hospital records. In a worst-case scenario, this can be life threatening.

From a hospital's perspective, it means that they can lose a great deal, too. They can perform procedures essentially for free because they performed surgery on a misauthorized individual. The victims also have a great deal to do because they have to work through the fraud with the hospitals and the insurance companies—at no fault of their

own. Health and Human Services, in conjunction with the Office of the Inspector General, put out a report citing they won or negotiated $2.6 billion dollars in fraud adjustments in 2019. There were 1,060 new criminal investigations in 2019.[15] Undoubtedly the numbers are much higher if you consider the cases that were thrown out or were never detected. It takes constant vigilance to detect fraud cases.

The protection of the data related to medical records is absolutely critical. We have only touched the tip of the iceberg finding all the different forces that tie into the safety of information. It is such a complex web of interrelated societal forces that need to be explored more fully to ultimately understand the ripple effect from a few vulnerabilities in connected medical devices and how everything is related to Medicine 2.0—the type of next-generation healthcare we are entering into now.[16]

Escalating Demand

The roots of why there has been such radical transformation in healthcare the last few years are on a few different levels. One of the key drivers is to reduce healthcare costs, which have been escalating. One of the avenues of that change has been as a result of the Patient Protection and Accountable Care Act (PPACA), which President Obama signed into law in March 2010. There were a few key provisions within this bill. The first provision was to create a Patient-Centers Outcomes Research Institute (PCORI), which would compare clinical effectiveness of medical treatments. The goal was to help the healthcare profession determine the most effective strategy for providing treatments. The second provision was a penalty that prohibited payments to states for hospital-acquired infections. Other provisions included reduced payments for hospital readmissions.[17]

As a result, hospitals were more incentivized to stay clean and to improve what they were doing—not just in the cleanliness, but how care would be administered. This required rethinking through many of the processes, changing hospitals' approach to technology, and catching medical issues more proactively than reactively. It would involve rethinking how they currently approach treatment and becoming more proactive. It would also involve the use of more connected technology and devices to treat and monitor patients, not just when they come to doctor's offices, but also remotely so conditions could be detected prior to onset of a more serious illness. America needed to revolutionize its way of caring for patients. Doctors would have to rely on a new generation of medical devices for their transformation effort—devices that would be internet connected to provide real-time capabilities or more real-time capabilities than they already do.

America responded as it always does by being innovative and thoughtful about the approach to help the medical community achieve its goals. The new generation of medical devices not only met the goals needed by physicians, but it jump-started continual changes in the technology. These new devices helped to lower per-patient costs, improve efficiency, provide better response care, offer greater convenience, and provide a better overall patient experience. In short, the existing value we are getting from medical devices will fuel the desire for more medical devices. But let us look at these positives, because within the desire for positive changes lies the seeds of the challenges related to the security of internet-connected medical devices.

Types of Internet-Connected Medical Devices

If we step back in time a hundred years, there were only a small number of electronic medical machines. They were

bulky, crude, and not able to store or send information. Everything had to be done by hand. By modern standards, this is painstakingly slow and inefficient. Now we have streamlined systems that not only can alert, but help with centralization of alerts meaning that, for example, a nurse does not have to be in physical proximity to a patient and/or device to be aware of a potential problem. While not everything connects together harmoniously, many devices are centralized to create alerts. In a hospital setting this is particularly important because a nurse does not have to hear an alarm from the physical machine in order to know there is an issue with a patient. A random walkthrough of the environment is not required. Nurses can be more focused on patients. Not only that, but patients who need long-term monitoring and want freedom from being at a hospital can get the care they need thanks to remote monitoring. This means the patient has a better quality of life.

Four types of medical monitoring devices are important to consider—wearable, on the skin, ingestible, and implanted. Some of these are sensory in nature, which means they can collect information or detect problems and relay them back to a centralized information source and potentially provide an alert. They are electronic in nature and can have a variety of follow-on actions such as alert for emergency medical systems.

Other systems are more protective and can respond, in a limited way, to the environment. These are referred to as *smart systems*. A good example of this is implanted insulin-releasing needles. If the blood sugar levels are off, the smart system can release the appropriate level of insulin to best protect the patient. In some cases, this can literally transform the lives of those who are diabetic, making it possible for them to have almost near normal lives.