Medical Devices: Evidence and Research

Dovepress

open access to scientific and medical research

Open Access Full Text Article

REVIEW

Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem

This article was published in the following Dove Press journal:
Medical Devices: Evidence and Research
20 July 2015
Number of times this article has been viewed

Patricia AH Williams
Andrew J Woodward

eHealth Research Group and Security Research Institute, Edith Cowan University, Perth, WA, Australia

Abstract: The increased connectivity to existing computer networks has exposed medical devices to cybersecurity vulnerabilities from which they were previously shielded. For the prevention of cybersecurity incidents, it is important to recognize the complexity of the operational environment as well as to catalog the technical vulnerabilities. Cybersecurity protection is not just a technical issue; it is a richer and more intricate problem to solve. A review of the factors that contribute to such a potentially insecure environment, together with the identification of the vulnerabilities, is important for understanding why these vulnerabilities persist and what the solution space should look like. This multifaceted problem must be viewed from a systemic perspective if adequate protection is to be put in place and patient safety concerns addressed. This requires technical controls, governance, resilience measures, consolidated reporting, context expertise, regulation, and standards. It is evident that a coordinated, proactive approach to address this complex challenge is essential. In the interim, patient safety is under threat.

Keywords: cybersecurity, security, safety, wireless, risk, medical devices

Introduction

Recent technical advances have resulted in transformations in health care delivery, which have the capacity and capability to improve patient care. A prime example of this is the increase in interconnectivity between medical devices and other clinical systems. This interconnectivity leaves medical devices vulnerable to security breaches in the same way other networked computing systems are vulnerable. However, unlike other networked computing systems, there is an increasing concern that the connectivity of these medical devices will directly affect clinical care and patient safety.

The integration of medical devices, networking, software, and operating systems means that the relative isolation and safety of medical devices are challenged. With integration comes complexity and challenges in management and thus protection. These challenges are known collectively as cybersecurity vulnerabilities. The term cybersecurity is used to cover a broad spectrum of context specific adversarial challenges.[1] "Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption".[2] The inevitable crossover from standalone medical devices to integrated equipment, networks, and software is creating not only problems of management and protection, but also one of definition. In a world where medical devices require safety approval, this creates a multitude of previously non-existent problems.

Increasingly, health care is a prime target for cyberattack with a recent SANS Institute report reporting that 94% of health care organizations have been the victim

Correspondence: Patricia AH Williams
School of Computer and Security Science, Edith Cowan University,
270 Joondalup Drive, Joondalup,
WA 6027, Australia
Tel +61 8 6304 5039
Fax +61 8 6304 2599
Email trish.williams@ecu.edu.au

of a cyberattack. This includes attacks on medical devices and infrastructure.[3] Regulatory authorities, such as the US Food and Drug Administration (FDA), have responsibility for assuring the safety, effectiveness, and security of medical devices. The regulatory bodies have acknowledged the seriousness and enormity of the problem by publishing recommendations for managing cybersecurity risks and protecting patient health information, to assist manufacturers in their submissions for FDA approval of medical devices.[4] While these are non-binding recommendations, they acknowledge that there has been a shift in the operating environment for medical devices, and that this shift needs urgent attention. Consequently, there is also debate over the definition of a medical device, and under what circumstances software is considered a medical device. The international standards community has taken a lead role in developing and modifying existing standards to address such issues. New and innovative models of health care are facilitated by the opportunity for interoperability, while supporting improvements in patient safety. However, the proprietary nature of previously non-interoperable medical devices has limited integration between vendors' products, and can result in errors in communication when integration is achieved.[5] Integration does not equate to interoperability, and interoperability does not equate to security.

Over the past 4 years, there has been increasing confusion over the definition of what constitutes a medical device, arising from the FDA ruling that medical device regulation includes "software, electronic and electrical hardware, including wireless", where this claims to be useful for medical purposes under the Medical Device Data System Rule.[6] The problem is that this definition includes data storage and data transfer, which to date has not been a security focus for medical device manufacturers. In the demand for interoperability to support data exchange and collation of data sources to aid clinical decision-making, perhaps the subsidiary cybersecurity vulnerabilities of this interoperability are a bigger problem than is currently manageable. These vulnerabilities are not confined to device characteristics and connectivity, and include technology issues, software risks, and human factors.

The paper frames this complex problem in order to identify the vulnerabilities and methods of attack. The potential impact of security breaches are presented as a backdrop to the discourse on how these vulnerabilities occur from a systemic perspective. Rather than taking a purely technical view, the paper encapsulates the conceptual view of the complete environment of implementation of medical devices with respect to the cybersecurity vulnerabilities. Therefore, some of the content is necessarily general in nature with regard to cybersecurity. Consequently, a multifaceted approach to the solution space is presented, together with the challenges of creating this solution space. The paper concludes with the factors that may influence future medical device development with regard to the cybersecurity of medical devices.

Framing the problem

The problem of cybersecurity vulnerability associated with medical devices requires framing as it consists of multiple and disparate factors. These include the transfer from isolated devices to networked, and the tensions this creates between security and safety; why this is not just a technical problem; and the subsequent contention between regulation and manufacture. Examples of incidents are provided to highlight the diversity of the cybersecurity problem.

Definition of medical devices

The historically well-defined description of a medical device has evolved from unconnected equipment, through to wirelessly reprogrammable implantable devices, to software applications. Therefore, it is necessary to define what a medical device is in a networked and mobile world. This paper refers to medical devices as:

> An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory […] intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease […]

As per the FDA definition.[7] This definition is constrained to exclude broader consideration of health and wellness applications running on mobile devices. Further, with software increasingly embedded into medical devices, the shift to software as a medical device (SaMD) has inevitably occurred.

> Well-developed and validated software has the potential to significantly and positively impact the delivery of patient care, transforming how we manage healthcare across the globe. Software is embedded in a medical device to assist in function and operation.[8]

Various interested parties and standards organizations are considering the implications of this change, and starting to address the fundamental design issues and safety concerns this raises. The current state of this fundamental variation in the concept of what constitutes a medical device is important

in the discussion of vulnerabilities. This ontology is more difficult to use when assessing cybersecurity risks in relation to device failures when the supporting network affected is not proximate to the device or the potential impact.

Tension between safety and security

Medical device information flow is conventionally unidirectional from the device to the health care provider. However, as technology has advanced, remote interaction with devices has become possible, and contemporary devices are networked to monitoring systems and electronic medical record (EMR) systems. To understand the structure of the vulnerabilities that this connectivity creates, it is essential to appreciate that medical devices are no longer a stand-alone component of the clinical care process, and therefore are not afforded the protection against cybersecurity attack that was once provided by stand-alone segregation.

Implantable medical devices capable of being reprogrammed wirelessly, such as pacemakers, drug (eg, insulin) pumps, defibrillators, and neuro-stimulators are used for monitoring and treating patients. The foundational study by Halperin et al[9] demonstrated the vulnerabilities of such devices, which is detrimental to their safe operation, and the availability, confidentiality, and integrity of the associated data. This study highlighted the tensions between safety and security while emphasizing the complexity of skills from the medical, technical, and security disciplines that are required to evaluate security risk and contribute to the protection of such devices. The connection of unconventional peripherals such as cardiac tissue connected to an electrical stimulation device illustrates this complexity. To date, research into security vulnerabilities has focused on Type 1 devices[9–13] such as implantable medical devices, where the greatest concerns reside with respect to patient safety adverse events. It should be noted that when assessing risk (eg, in International Electrotechnical Commission [IEC] 62304) embedded software is classified further into levels of potential harm from failure of the device or software.

The increased use of wireless network connectivity and connection of devices to the Internet, coupled with the desire to make use of the information collected on a medical device in other health systems, has made medical devices more open and subsequently vulnerable to cybersecurity threats. It is important to note that vulnerabilities were always inherent in these devices, and that it is the exposure to a greater threat landscape, through these network connections, that is responsible for the increased risk. Thus, the responsibility for maintaining device functionality, integrity and confidentiality of information, patient privacy, device and information availability, to prevent adverse effect on patient safety is now shared by manufacturers, health care providers, and patients.[4]

Cybersecurity incidents

The once seemingly futuristic exploit of implanted medical devices has been made present with the demonstration of successful attacks against devices such as the insulin pump[14] and pacemakers.[15,16] Research from the Archimedes – Ann Arbor Research Center for Medical Device Security at the University of Michigan has demonstrated the potential compromise to implanted devices.[17] The lack of device embedded security controls is of greater concern than the incidents they result in. Research has demonstrated that issues such as web interfaces to infusion pumps, default hard coded administration passwords, access to the Internet through devices connected to internal networks, are just a few of the common vulnerabilities found in devices used in the hospital environment.[18] Embedded web services, with unauthenticated and unencrypted communication are one of the biggest vulnerabilities, as an attacker can potentially affect these devices remotely from anywhere in the world.

Incidents such as a malware attack that infected US Department of Veterans Affairs medical devices running over a trusted network, has led to an isolation approach to protection (for some 50,000 medical devices), thereby defeating the point of interoperability and connectivity.[19] Such incidents, together with the national Ponemon and SANS research reports, prompted the US Federal Bureau of Investigation (FBI) to investigate health care as a potential high profile risk, and issued a private industry notification (FBI case no 140408-010). This stated that:

> Cyber actors will likely increase cyber intrusions against health care systems – to include medical devices – due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market.[20]

Recognition of the increasing vulnerability of medical networks, as well as medical devices connected to these networks, is reflected in the revisions to the international standard International Organization for Standardization (ISO)/IEC 27000-series "Information security management systems" and ISO/IEC 80001 "Application of risk management for IT networks incorporating medical devices". However, consideration of the threat to the devices themselves and subsequently the resulting patient safety

concerns are of greater concern when the connections are to wireless networks.

What complicates the security risks with medical devices is that these devices expose both data/information and potentially the control of the device itself. In addition, the cybersecurity discipline tends to take a risk approach to any problem. Traditionally security has been viewed as a technological solution space, and subsequently the change in the operating environment driven by technology such as wireless, has been focused on controlling the risk with technology. This perspective has gradually altered over time with acknowledgment that those practical security solutions in health care need to take a socio-technical approach.[21] Further, for practical security solutions to be effective, research shows that they must, at the very least, consider clinical workflow, if not seamless integration with this workflow.[22]

Contention between manufacture and regulation

The contention between medical device manufacture and regulation is not a new issue. The current discussion around the security of medical devices parallels that which occurred in critical infrastructure devices over a decade ago.[23] Balancing this contention with innovation, while focusing on assuring efficacy and safety can be problematic.[24] Rigorous clinical trials are not part of the process for approval of all devices, and in both the US and the European Union, this is handled through pre-market submission and post-market surveillance.[25] However, this does not consider non-clinical safety issues with networked medical devices. The reality is the occurrence and reporting of attacks has increased, and medical devices are not immune to this.[26]

The recognition of cybersecurity as a significant vulnerability in medical devices has driven guidance, albeit in draft mode, by regulatory authorities.[27] The most notable being the FDA recommendations for managing cybersecurity risks to protect the patient and the information contained, created and processed by the medical device. Guidance such as "Content of pre-market submissions for management of cybersecurity in medical devices"[4] is aimed at considering protection in the design and development stages by identifying potential security risks. The major issue with this guidance is that it also recommends that patches and update plans be submitted for review to the FDA. In an environment where software patching can be an almost daily occurrence, this would be unworkable for the certification required by medical device manufacturers. The gap in patch application is a result of the multi-step process required for medical devices, even without re-certification. If the software supplier releases a patch, the device manufacturer has to perform the engineering analysis prior to the verification and validation. Once released to the health care provider, testing in the target environment and an impact analysis on patient safety, workflow, scheduling, and patient care is required. The final step, which often results in delayed rollouts, is the distribution and installation to all devices. High profile instances where patches have not been applied, such as the Conficker virus, are only the apex of a much larger problem.[28]

Further, the FDA recommendations are standard across any cybersecurity risk-assessment process. The differentiating point is that, to date, medical device manufacturers have not had to consider intentional as well as unintentional compromise of a device based on cybersecurity vulnerabilities, and therefore cybersecurity risks have not been considered as part of a product's design. It is unfortunate that the evolutionary development of medical devices has resulted in software validation as a separate activity in the medical device certification process. Indeed, the international standard "IEC 62304 Medical device software – Software life cycle processes", to which medical devices must be certified, was developed specifically for this purpose. However, it does not include network connection or cybersecurity considerations.

It is important to recognize that compliance with regulation does not equate to security. Compliance is demonstration against a set of static principles, usually articulated in regulation or policy. Security, on the other hand, needs to address a dynamic and uncertain environment that is difficult to predict, manage, and therefore define for compliance.

A cybersecurity perspective on the vulnerabilities

Vulnerability is considered a weakness that may be exploited, be it in hardware, software, firmware, operating systems, medical devices, networks, people, and processes. All of these elements comprise an information system and are critical to its functioning. A threat is the potential for a vulnerability to be exploited, and the risk is calculated by consideration of the likelihood that a threat can occur together with a measure of the severity of any potential impact. Mitigation is a risk management strategy used to minimize the impact of an attack. Intrinsic in the calculation of risk is the outcome of an attack, and the aspect of security it affects.

Harm of cybersecurity vulnerability

Information security theory defines the basic goals of security protection to be confidentiality, integrity, and availability

of information. As such, networked medical devices are open to the following:

- confidentiality may be compromised from unauthorized access due to poor access control measures. The impact of this is:
  - non-compliance with regulations (HIPAA [Health Insurance Portability and Accountability Act of 1996], Australian Privacy Principles),
  - reputational damage,
  - litigation and financial consequences.
- Integrity may be affected from poor configuration, corruption of data, or unauthorized manipulation of information. This will impact:
  - patient safety from potentially incorrect clinical decisions,
  - patient safety from the device being operated by an attacker.
- Availability where access to data or a device is limited or lost. The impact of this on:
  - patient safety from limiting access to relevant critical information and affecting subsequent clinical decisions,
  - patient safety where critical alerts are not received.

Motivation of attack

To further understand the potential vulnerabilities and assess risk, the definition of the cyber threat landscape should be considered from both the motivation for attack, and the type of attack that is carried out. The motivation factors can be defined generally as:

- financial (criminals, organized crime, motive for attack is to make money),[29]
- nation state (state sponsored, eg, Stuxnet, People's Republic of China cyber-army),[30]
- hacktivist or cyber terrorist (to make a political statement – usually asymmetrical).[31]

The generic method by which an attacker seeks to attack can be broadly defined as methods of attack:

- external – local (attacker has physical access to the device),
- external – remote (attacker has remote access to the device),
- insider – deliberate (inside attacker deliberately attacks the network, can be remote or local),
- insider – inadvertent (inserts infected USB stick, configuration error by administrator),
- inadvertent/random – no specific threat actor involved (worm or power failure).

The key security threats, and for which incidents have been recorded, includes malware and hacking to cause intentional harm. The susceptibility to such incidents has prompted the authorities, including the US Department of Homeland Security, to investigate the cybersecurity flaws in this sector of health care provision.[32,33] From a security perspective, this is clearly a critical infrastructure protection issue. In addition, physical incidents such as theft of devices and electromagnetic (EM) interference are present regardless of integration into networks, and affects primarily availability, and potentially confidentiality.

Network and wireless vulnerabilities

Attacks that use networks as a vector and aim to exploit vulnerabilities in computers and devices attached to the network are usually aimed at the following three targets: web servers, databases, and application software.

1. Web servers. The use of a web service is quite common in interfacing with medical devices, providing a graphical interface through which to configure or interact with a device. The weakness of using such an interface is that web services commonly contain vulnerabilities, readily exploitable by an attacker. There are many attack tools, which are freely available to download and use, which scan web interfaces and highlight any vulnerabilities in the web service. An attacker can use this information to construct a specific payload to attack a vulnerable target.
2. Database servers. Many devices and systems have a database or data store to retain information for that device, commonly referred to as a database back-end. Many of these databases run a form of structured query language (SQL), and if not configured correctly to sanitize input data, are highly vulnerable to SQL injection. An SQL injection is a very serious attack, as it degrades all three of the goals of information security (confidentiality, integrity, and availability). The attacker can delete all information in the database, rendering it unavailable. They can read all of the information, a breach of confidentiality, and they can inject false data, which is a loss of integrity of the data.
3. Application software. This applies to any software running on a device, be it in conjunction with either of the previous two categories or on its own. This type of attack is likely to be successful where software has not been through rigorous software vulnerability testing to determine what vulnerabilities may be present. Many successful cyberattacks have exploited vulnerabilities in

code not rigorously tested prior to deployment in a live environment.

Further to these categories, the method of exploit can be direct attack, social engineering, malware, or a combination of any of these. Direct attack can be through a direct connection to the device, over either a wireless or a physical connection, where the user is in proximity to the device, or is able to make a direct connection over a network, locally or over the Internet. Social engineering describes that phase of an attack where the attacker acquires information from people who have knowledge of the system or its security measures, such as passwords, by talking, emailing, or impersonation. Most successful attacks contain some element of social engineering. The last category is comprised of viruses, worms, Trojans, and advanced persistent threat malicious software. This software targets, and exploits, known vulnerabilities in software to gain control of, or corrupt, a system. Traditionally, antivirus software is used to mitigate this threat, but this has become increasingly ineffective.[34]

The discrete nature of some medical devices mean they cannot be protected using traditional network defenses such as firewalls, antivirus, or intrusion detection systems. This is because such devices are not permanently connected to the wide IT infrastructure; rather they are accessed on an ad hoc basis as required. The protective functionality, could in theory, be built into these devices; however, this would mean a more powerful processor would be required, with a corresponding increase in power usage, resulting in reduced battery life. The only way to overcome this limitation would be to use a larger battery resulting in a larger device. As such, they are more vulnerable than similar networked devices, and this must be considered as part of the use or deployment of these devices.

The use of wireless networks to exchange data and information presents significant challenges in achieving the security goals of confidentiality, integrity, and availability. Wireless networks are fundamentally a radio signal, sent between two or more devices, which have been encoded to carry information. More specifically, it is an EM wave that has been modulated to carry digital data, and as such, it is vulnerable to interference from other EM waves. There are two significant issues presented by this. Firstly, it means that jamming these signals is a trivial exercise, which prevents connection to the device and vice versa. Secondly, tracking the source of the jamming can be difficult, as can removing or stopping this jamming. This type of attack is commonly referred to as a denial-of-service attack, and directly affects the availability of information. The following devices all use EM waves to send and receive information and thus are all vulnerable to this type of denial of service: Wi-Fi (Institute of Electrical and Electronics Engineers [IEEE] 802.11) networks, Bluetooth devices (IEEE 802.15), ZigBee devices (IEEE 802.15.4), and radio frequency identification devices (includes smart cards). In reality, most sources of interference are classified as inadvertent because the source of interference is usually another such device, which operates on the same frequency. Logic would dictate that frequencies are reserved for particular devices, which would seemingly eliminate this problem. However, these devices operate in so-called license free bands, and as such operate under a public park policy and reservation of frequencies or channels is not allowed.

There are also issues that make achieving the goals of the integrity and confidentiality of the data a challenging task. Interception of data exchanged between an insulin pump and a connected device is not usually a particularly high risk, although this affects confidentiality through eavesdropping. This data, if revealed to a third party, is not likely to result in any particular patient safety issue, although confidentiality may be compromised. However, integrity is crucial, and this is particularly challenging when using a wireless connection. As the mechanism of transfer is a radio wave signal, this signal cannot only be intercepted, but an attacker can send his or her own signal. This is referred to as a man-in-the-middle attack. This type of injection is extremely high risk, as an attacker could reprogram a device to operate in a manner that could severely affect patient safety. Certain protocols, such as the IEEE 802.11 contain mitigations and preventions for such attacks, but these protections are optional, and it is up to the manufacturer to have considered these risks and implemented these protections. Frequently, such attacks are not considered by engineers, who are concerned primarily with the continued operation and functionality of the device within normal parameters.

Why are medical devices open to these vulnerabilities?

A number of factors complicate protection of medical devices, and contribute to a continued state of insecurity. These are a result of technical, management and human causes.

- Providing hackers with vital information: certification agencies publish device verification information, such as spectrum; radio frequency transmission data are published in device manuals; and the device workings are available on patent databases. It is a misconception to depend on security through obscurity even where proprietary protocols are used for communication. Not only does this limit interoperability, but it also leaves a gap

for reverse engineering from which little protection can be applied.[13] Using sound and proven cybersecurity approaches provides better protection.

- Legacy operating systems and software (typically devices, systems, and software that is over 5 years old or has been replaced by a new version), and incompatibility between systems leaves vulnerabilities such as misconfiguration and security holes. This includes vulnerabilities from non-negotiated interfaces with third party software, often through web interfaces.[35]
- Lack of timely software updates and patches. This is often an issue where concerns with workflow and service disruptions are present. Although health care providers, such as the US Veteran Affairs, have considered improved patch management,[36] this will remain an ongoing issue in settings where large numbers of devices are used and are a constituent part of other clinical information systems.
- Medical devices do not have basic security features. For instance, computed tomography scanners delivering measured radiation can be tampered with, potentially creating life threatening patient safety issues. Security features added after design, sometimes at implementation, can disrupt clinical workflow and are implemented poorly.
- Web services are a popular solution for interfacing to existing systems. For instance where increased interoperability with EMR systems is required, these are insecurely implemented (with insecure authentication and unencrypted). This means that information can be modified as it is transferred to EMR systems. With the increasing reliance on information presented in electronic information systems, the integrity of information in health care is vital.
- Compromised medical devices can be used to attack other sections of the health care organization network. The demand for interoperability and seamless integration between systems, networks, and devices increases the risk for cybersecurity breaches.
- Lack of awareness of the cybersecurity issues, and poor security practices compound the underlying problem of mixed cybersecurity programs in device development and certification. These poor practices include lack of secure disposal of devices containing information or data, password sharing, and distribution of passwords particularly in devices where passwords are required for device access. Inconsistent education and training on cybersecurity risks and impacts also underpin the continued cybersecurity vulnerabilities.
- Achieving a balance between security and privacy goals and health care utility and safety can be challenging. For instance, using strong encryption and access control measures enhance security, but place the patient at greater risk in the case of an emergency.[37]
- Limited power and resources of medical devices mean that encryption can slow down medical devices, and reduce the usable battery life.

These issues highlight the complexity in the control and management of cybersecurity risk and contribute to the overall lack of security seen in the health care field currently.

Solution space and its challenges

The solutions space for the range of vulnerabilities discussed is as multifacetted as the issues themselves. This section details the guidance that can be used to devise suitable protection mechanisms, mitigations, and processes. The aspects include information security processes, reporting and feedback loops, risk management, regulation, resilience activities, and standards, as well as best practice technical controls. This challenge is made more complex with the propagation of device functionality. This evolving nature of security threats means that some of the security challenges with networked medical devices are as yet unknown.[38]

Information security processes

Selecting and implementing information security processes is further complicated where there are multiple manufacturers of devices and equipment in the physical network, as well as the logical clinical workflow. While interoperability may be achieved, this does not mean that it is secure interoperability because of the number and diversity of the devices, equipment, and platforms being connected. The secure configuration of the network and attached devices, together with the subsequent coordination required for patch management (software updating) is a major confounding factor.

Reporting and feedback loops

Good feedback and notification systems are required between health care providers and medical device manufacturers, to ensure effective mitigation of potential cybersecurity issues. In addition, legislation to mandate reporting of cybersecurity incidents would assist in identifying issues from all health care providers. This would require a greater understanding by the regulatory bodies to distinguish between a patient safety incident and a cybersecurity incident. Unfortunately, cybersecurity incidents are currently only categorized as

safety issues where they result in an identifiable detrimental patient safety outcome.

Auditing, including network and access monitoring specifically where medical devices are used, should become part of normal operational practice, and reportable to the governance level of the organization. A lack of reporting, and even recognition, of security breaches creates an added challenge in that not all errors, malfunctions, security incidents, and information leaks are identified, or reported immediately. The consistency with which post-market surveillance identifies security and privacy issues is marginal at best.[10] This reveals that collecting data on cybersecurity events, when not identifiably and directly linked to patient adverse events, or recalls of devices, is highly problematic.

Risk management

Processes, procedures, and robust governance mean that risk identification and understanding risk management factors and incident response are essential. This is in addition to the regulatory compliance required for patient safety. Risk management and governance processes should include documenting data flows with regard to networked medical devices. This would ensure that appropriate protection is provided at each stage of data transfer, processing, and storage. Such management has to be defined by organizational policy, and supported with appropriate procedures. The evolution of medical devices and their proliferation has hampered timely and effective cyber threat mitigation controls. The volume of devices in a health care organization that can be networked creates multiple points of vulnerability. While, these should be identified through the risk management process, the reality is that risk management frameworks do not yet include the use of medical devices, or their associated vulnerabilities. This issue is understandable from an evolutionary perspective as in most hospitals, medical devices are managed by the biomedical technicians, while the IT network is under the auspices of the IT department. Added to this is the acknowledged factor that an IT person is not a security specialist. A specialist in cybersecurity has to have the ability to recognize complex and emergent behavior and provide appropriate responses to new cybersecurity threats.[39]

Regulation

The requirement for renewed FDA approval when any changes are made to a medical device, including the embedded software, means additional cost and time to market. This leaves known vulnerabilities open longer than would otherwise occur, and imposes additional cost to the manufacturer in the regulatory compliance process. Further, the regulatory bodies are concerned with the security of the device and not of the embedded code, which may have inherent security vulnerabilities. The FDA Safety and Innovation Act (FDASIA) report identified that with the increase in data exchange between devices and EMR systems, and the use of the wireless spectrum, that the FDA needed to be clearer in its aspects of regulation that will apply to cybersecurity vulnerabilities.[5]

Resilience activities and contingency planning

Network segregation, particularly for legacy devices, is a sound resilience and protection measure. This may include setting up virtual local area networks, firewalls, limiting access, and the use of uninterruptible power supplies on critical care devices. All of these measures are a standard part of contingency planning, but, similar to risk assessment, have not fully considered medical devices to be part of the information system network. Contingency planning for information systems is comprised of business impact analysis, incident detection and response, disaster recovery, and business continuity.[40] This plan documents pre-defined processes, providing a governance approach to system resilience, as well as handling and recovering from incidents. In the adoption of a governance approach, the three levels of organizational structure all play a role in the protection of resources including the medical devices and associated networked technologies. At the strategic level, compliance with regulation, policy development, and business process are the culmination of the lower level activity. From the tactical perspective, proactive approaches to risk management, auditing, education, and contingency planning are needed. At the day-to-day operational level, everyday practices such as implementing technical controls (eg, encryption) routinely and using processes integrated seamlessly into workflow can ensure that mitigations are effective.

Standards

Standards provide good practice yet need application and interpretation. While there are a number of international standards that are pre-requisites for the certification of medical devices, these are limited to the development and design risk assessment process. These standards do not focus on the specificity required for cybersecurity within the complex deployment setting. However, since many security flaws and subsequent vulnerabilities are a consequence of poor software design, which may include medical device software, the standards related to this are included in the list below. Poor

software design and testing can result in application software vulnerabilities such as SQL injection and buffer overflow attacks. The design aspects in 62304/82304/80002 are key to cybersecurity protection, and hence have been included in the list. These standards include:

- ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity standard provides guidance on addressing cybersecurity issues and its relationship to other types of security to highlight the basic practices in cybersecurity.
- IEC 62304:2006 – Medical device software – software life cycle processes define the medical device software lifecycle requirements. This standard is currently under revision and harmonization with ISO 82304.
- IEC/ISO CD 82304 Health software – Part 1: General requirements for product safety (under development) is a standard for the safety of health software, and an evolution of IEC 62304. This standard provides requirements for the safety of health software products, and while situations where health software is part of – or embedded in – a physical device are not part of this standard, where medical devices are software only, this standard should be used. Both 82304 and 62304 focus on the process of product design, software validation and testing. These form important guidance since it is reported that software failures result in 24% of all medical device recalls.[41]
- ISO/IEC 80001 series of standards detail guidance for Application of risk management for IT-networks incorporating medical devices.
- ISO/DTR 80002-2 Medical device software – Part 2: Validation of software for regulated processes is a technical report under development, which considers embedded and associated software with all medical devices.
- IEC/TR 80002-1:2009 Medical device software – Part 1: Guidance on the application of ISO 14971 to medical device software. This provides the risk management practitioner advice on meeting the requirements of ISO 14971, and is used as the principal standard for risk management regulation.
- IEC/TR 80002-3:2014 Medical device software – Part 3: Process reference model of medical device software life cycle processes (IEC 62304). This provides the description of the software life cycle processes and the associated safety class definitions, derived from IEC 62304.

These standards, while providing good practice in risk and development lifecycle processes, do not deal with the fundamental cybersecurity protection required in the environment of use for medical devices. While SaMD cannot be ignored, it is not discussed in detail in this paper. The development of SaMD regulation and standards is under development, yet take an identical approach to protection, through risk assessment in the software development lifecycle. The existing medical device manufacturers rather than software developers have driven this direction. Indeed, development of ISO 82304 has included robust discussion to obtain shared perspectives on the definition of stand-alone health software.

Best practice technical controls

A diverse range of best practice technical controls is available for protection from cybersecurity vulnerabilities. However, it is the secure application of the controls, within a complex system, that remains the challenge. For instance, encryption and passwords are standard protection mechanisms, and identifying which medical devices are not employing the mechanisms is important. Further, proximity-based access control and distance bounding may be suitable solutions to the vulnerabilities of remote access and insecure web interfaces, but are not commonly used. Data leakage detection, prevention, and monitoring embedded into information management systems can aid in instances where sensitive information is concerned. Software for data leakage prevention is available that can undertake this activity, yet it is dependent on comprehensive organizational policy definition and configuration. Clearly, such measures have to be part of an enterprise solution and are not, of themselves, a solution to the whole gamut of cybersecurity vulnerabilities.

Further, there are difficulties in using standard cybersecurity vulnerability detection products, such as network scanning tools, because medical devices, in particular older devices running proprietary operating systems, are not recognizable by such tools. Conversely networked medical devices running on standard operating systems are susceptible to the same vulnerabilities as other standard IT networks. A lack of access by cybersecurity practitioners to the real-world devices, particularly implanted medical devices, for testing and experimentation creates another potential failure in effective protection. This coupled with the lack of collaboration between the disparate disciplines required to address the biomedical-security challenges, creates further complexity.[37] Medical device manufacturers will need to have additional expertise in medical networks both wired and wireless, and work closely with health care providers and organizations to both understand and mitigate potential threats.

It is not possible to view the solution space for medical device cybersecurity protection in isolation of the systems they connect to, and the environment in which they operate. Clear definition of the responsibility for the infrastructure,

patching, operating systems, policy development as well as monitoring and resolution of incidents, is required.

Conclusion

In the health care setting, patient safety will always come before cybersecurity requirements. The challenge is to close the gap between the two objectives, minimizing compromise and ensuring patient safety, while being responsive to the evolving cybersecurity threat environment. Medical devices are now an integral component of medical networks and therefore their security should be an integral component of cybersecurity protection. This will require increased collaboration between the medical physicists and IT professionals, as well as collaboration by medical device manufacturers and network vendors, and may require input from cybersecurity experts.

The cybersecurity vulnerabilities that are associated with medical devices are similar to any other networked system. What delineates the medical device environment from other networked environments is the potential detrimental impact on patient safety that exploitation of cybersecurity vulnerabilities may have. To shift the protection of medical devices to more mainstream cybersecurity protection will require the acceptance of medical devices as standard connections in the implementation of a network. This shift is essential, given the current lack of governance of networked medical devices, together with limited risk management, reliance on medical device regulatory approval, lack of awareness of the actual security risks, and lack of preparation by organizations to deal with the risks. While jurisdictional legislation has been the driver in the US to enforce increased protection, through the HIPAA Privacy and Security Rules, the HITECH (Health Information Technology for Economic and Clinical Health) Act, and linkage to funding through the Meaningful Use 2 and 3, this compliance does not mean effective security. Data breach legislation and mandatory reporting has resulted in a proactive decreed approach to promoting a more cybersecurity aware health care environment, however, such an approach has been slow to be adopted outside of the US.

There is little argument that controlling cybersecurity in evolving and expanding medical networks, inclusive of medical devices, is a significant challenge. The first step in tackling the challenge is for health care organizations to understand the cybersecurity vulnerabilities that are already present in their networked medical devices, including the potential exposure of sensitive information and the associated privacy issues. The second step is to embed cybersecurity protection into the design and development processes of medical device manufacture. Standards revision and new national guidance is currently addressing this objective. The third step is to establish accountability for medical device cybersecurity, using standards, to assist manufacturers and implementers, together with regulatory oversight to ensure compliance. Finally, medical device industry advocacy must assist in promoting increased awareness of cybersecurity and privacy issues.

To ensure the future protection of medical devices in a networked world, a coordinated proactive approach that includes standard cybersecurity assessment and control, together with specific medical device data and workflow considerations, is needed. In the interim, there will inevitably be adverse outcomes for patient safety while a clear, workable process is developed, awareness of cybersecurity vulnerabilities in medical devices is enhanced, and a shift in perception is implemented.

Disclosure

Williams PAH is a member of the ISO 80001 standard and Joint Working Group 7 revision task force. The authors have no other conflicts of interest to disclose in this work.

References

1. Craigen D, Diakun-Thibault N, Purse R. Defining Cybersecurity. *Technology Innovation Management Review*. 2014;4(10):13–21.
2. Critical Infrastructure Protection. *Cybersecurity and Critical Infrastructure Protection*. Lewis JA; 2006. Available from: http://cip.management.dal.ca/publications/Cybersecurity%20and%20Critical%20Infrastructure%20Protection.pdf. Accessed June 9, 2015.
3. SANS Institute. *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon*. Filkins B; 2014. Available from: http://www.sans.org/reading-room/whitepapers/firewalls/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735. Accessed June 9, 2015.
4. US Food and Drug Administration. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. US Food and Drug Administration; 2014. Available from: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf. Accessed June 9, 2015.
5. US Food and Drug Administration. *FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework*. FDA, FC, ONC; 2014. Available from: http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf. Accessed June 9, 2015.
6. US Food and Drug Administration [homepage on the Internet]. MDDS Rule. FDA Federal Register; 2011(76 FR 8637). Available from: http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/MedicalDeviceDataSystems/ucm251897.htm. Accessed June.
7. US Food and Drug Administration [homepage on the Internet]. Is The Product A Medical Device? FDA; 2014. Available from: http://www.fda.gov/medicaldevices/deviceregulationandguidance/overview/classifyyourdevice/ucm051512.htm. Accessed June 9, 2015.
8. International Medical Device Regulators Forum. *"Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations*. IMDRF Software as a Medical Device (SaMD) Working Group; 2014. Available from: http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf. Accessed June 9, 2015.

9. Halperin D, Heydt-Benjamin TS, Ransford B, et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. Paper presented at: Security and Privacy, 2008. SP 2008. IEEE Symposium; Oakland, California, USA; May 18–22, 2008.
10. Kramer DB, Baker M, Ransford B, et al. Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLoS One*. 2012;7(7):e40200.
11. Maisel WH, Kohno T. Improving the Security and Privacy of Implantable Medical Devices. *N Engl J Med*. 2010;362(13):1164–1166.
12. Kune DF, Backes J, Clark SS, et al. Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors. Paper presented at: Security and Privacy (SP), 2013 IEEE Symposium; San Francisco, California, USA; May 19–22, 2013.
13. Burleson W, Clark SS, Ransford B, Fu K. Design challenges for secure implantable medical devices. Proceedings of the 49th Annual Design Automation Conference; 2012; San Francisco, CA. June 03–07, 2012
14. spectrum.ieee.org [homepage on the Internet]. Peck ME. Medical devices are vulnerable to hacks, but risk is low overall. IEEE Spectrum; 2011. Available from: http://spectrum.ieee.org/biomedical/devices/medical-devices-are-vulnerable-to-hacks-but-risk-is-low-overall. Accessed June 9, 2015.
15. livescience.com [homepage on the Internet]. Lewis T. Medical Devices Vulnerable to Hackers, New Report Says. Live Science; 2013. Available from: http://www.livescience.com/39889-medical-devices-vulnerable-to-hackers.html. Accessed June 9, 2015.
16. Seymour DM. *Medical device security as part of overall risk management*. *ISC2 Congress Strengthening Cybersecurity Defenders; 2014*. Available from: https://congress.isc2.org/sites/default/files/Session2145-MedicalDeviceSecurityAsPartOverallRiskManagementProcess.pdf. Accessed June 9, 2015.
17. Archimedes Ann Arbor Research Center For Medical Device Security [homepage on the Internet]. Improving Medical Device Security; 2015. Available from: http://secure-medicine.org/. Accessed June 9, 2015.
18. wired.com [homepage on the Internet]. Zetter K. It's Insanely Easy to Hack Hospital Equipment; 2014. Available from: http://www.wired.com/2014/04/hospital-equipment-vulnerable/. Accessed June 9, 2015.
19. healthcareinfoseurity.com [homepage on the Internet]. Anderson H. Medical device security raises concerns. Healthcare Info Security; 2011. Available from: http://www.healthcareinfosecurity.com/medical-device-security-raises-concerns-a-3644. Accessed April 11, 2015.
20. US Federal Bureau of Investigation Cyber Division. *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*. FBI Cyber Division Private Industry Notification; 2014. Available from: https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf. Accessed June 9, 2015.
21. Coles-Kemp L, Williams PAH. Changing Places: the Need to Change the Start Point for Information Security Design. *Electronic Journal of Health Informatics*. 2014;8(2):e13.
22. Williams PA. When trust defies common security sense. *Health Informatics Journal*. 2008;14(3):211–221.
23. Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*. 2001;21(6):11–25.
24. Curfman GD, Redberg RF. Medical Devices – Balancing Regulation and Innovation. *N Engl J Med*. 2011;365(11):975–977.
25. Kramer DB, Xu S, Kesselheim AS. Regulation of Medical Devices in the United States and European Union. *N Engl J Med*. 2012;366(9):848–855.
26. Healthcare IT News [homepage on the Internet]. Maliard M. Safety demands better device integration. *Healthcare IT News;* 2013. Available from: http://www.healthcareitnews.com/print/61021. Accessed March 31, 2015.
27. Medical Device and Diagnostic Industry [homepage on the Internet]. FDA Guidance on Wireless Devices: What You Need To Know. MDDI; 2013. Available from: http://www.mddionline.com/article/fda-guidance-wireless-devices-what-you-need-know. Accessed June 9, 2015.
28. cnet.com [homepage on the Internet]. Mills E. Conficker infected critical hospital equipment, expert says. CNET; 2009. Available from: http://www.cnet.com/news/conficker-infected-critical-hospital-equipment-expert-says/. Accessed June.
29. Kshetri N. Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. *Electronic Commerce Research*. 2013;13(1):41–69.
30. Langner R. Stuxnet: Dissecting a cyberwarfare weapon. *Security and Privacy, IEEE*. 2011;9(3):49–51.
31. Hampson N. Hacktivism, Anonymous and a new breed of protest in a networked world. *Boston College International and Comparative Law Review*. 2012;35(6):511.
32. reuters.com [homepage on the Internet]. Finkle J US Government Probes Medical Devices for Possible Cyber Flaws. Reuters; 2014. Available from: http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022. Accessed June 9, 2015.
33. spectrum.ieee.org [homepage on the Internet]. Hsu J. Feds Probe Cybersecurity Dangers in Medical Devices. IEEE Spectrum; 2014:1. Available from: http://spectrum.ieee.org/tech-talk/biomedical/devices/feds-probe-cybersecurity-dangers-in-medical-devices. Accessed June 9, 2015.
34. Haffejee J, Irwin B. Testing antivirus engines to determine their effectiveness as a security layer. Paper presented at: Information Security for South Africa (ISSA); 13th International Information Security for South Africa conference; Johannesburg, South Africa; August 13–14; 2014.
35. McCauley V, Williams PAH. Trusted interoperability and the patient safety issues of parasitic health care software. In: Williams PAH, editor. *9th Australian Information Security Management Conference*. Perth: secau-Security Research Centre, Edith Cowan University; 2011:189–194.
36. healthcareinfoseurity.com [homepage on the Internet]. Anderson H VA Addresses medical device security. Healthcare Info Security; 2011. Available form: http://www.healthcareinfosecurity.com/interviews.php?interviewID=1163. Accessed April 11, 2015.
37. Clark SS, Fu K. Recent results in computer security for medical devices. International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth); Kos Island, Kardamena, Greece; October 05–07, 2011.
38. Deloitte Center for Health Solutions. *Networked Medical Device Cyber Security on Patient Safety: Perspectives of Healthcare Information Cybersecurity Executives*. 2013:16. http://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-networked-medical-device-11102014.pdf. Accessed March 1, 2015.
39. Dark M. Thinking about Cybersecurity. *Security and Privacy, IEEE*. 2015;13(1):61–65.
40. Whitman M, Mattord H. *Management of Information Security*. 3rd ed. Boston, Mass: Course Technology, Cengage Learning; 2010.
41. US Food and Drug Administration. *Understanding Barriers to Medical Device Quality*. FDA; 2011. Available from: http://www.fda.gov/downloads/AboutFDA/CentersOffices/CDRH/CDRHReports/UCM277323.pdf. Accessed April 11, 2015.