Commentary

Collaborating to Achieve a Mutual Cybersecurity Advantage

Bill Hagestad and Aleksandar Straumann

About the Authors

Bill Hagestad is a senior principal cybersecurity engineer at Smiths Medical in Plymouth, MN. Email: bill.hagestad@smiths-medical.com

Aleksander Straumann is an engineer I at Smiths Medical in Plymouth, MN.

Challenges and threats to key decision makers in the boardroom regarding cybersecurity are affecting the way hospitals and medical infusion pump manufacturers mutually conduct business. Deterring and defeating the cyber- and physical threats that affect patient safety are key among these mutual challenges. Other challenges that must be considered include reputational damage, litigation, and impact to the bottom line.

The technical dilemma includes several layers and encompasses 20th century product design. The continued use of legacy medical equipment built before 2000, such as infusion pumps, indicates that many medical device manufacturers are stuck with 1990s-era design-development processes. Given today's ubiquitous Internet of Things (IoT) network environment, medical device manufacturers must now consider the issues of legacy device connectivity in the 21st century. The IoT provides a mandate for key stakeholders, including healthcare authorities, medical infusion manufacturers, the Food and Drug Administration (FDA), The Joint Commission, and the Centers for Disease Control and Prevention, to provide a collaborative roadmap for the cybersecurity of connected devices.

Given today's ubiquitous Internet of Things network environment, medical device manufacturers must now consider the issues of legacy device connectivity in the 21st century.

Infusion pump manufacturers are faced with environmental challenges. Patient care depends on technology, and delays to the delivery of care are unacceptable, including for cybersecurity issues. Medical devices are becoming more connected and dependent on technology, while many hospitals treat medical infusion pumps as yet another device to connect to their infrastructure. Achieving information assurance within traditional and wireless networked infrastructures is now mandatory. As devices become more connected and the push for interoperability becomes more urgent, the risk for vulnerability becomes both more shared and more inevitable.

Most medical infusion pumps are seeing institutional use and utility in excess of a single decade or even longer. To ensure patient safety, medical device manufacturers must deliver medical infusion pumps with a temporal security advantage. The concept of a "temporal advantage" means that medical device manufacturers must adapt to emerging cyberchallenges. Yet, this cybersecurity issue encompasses more than staying ahead technologically. Organizations should have the capability to uncover and react to a cybersecurity vulnerability.

FDA Cybersecurity Guidance

On June 13, 2013, the FDA issued a safety communication aimed at medical device manufacturers, hospitals, facilities that use medical devices, health information technology (IT) staff, procurement staff, and biomedical

engineers.[1] In it, the agency recommended that medical device manufacturers and healthcare facilities work to reduce the risk that a device would fail due to a cyberattack.

"Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches. In addition, as medical devices are increasingly interconnected via the Internet, hospital networks, other medical devices, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates," the FDA wrote.[1]

Anyone with enough aptitude, ability, skill, motive, and opportunity can pose a negative cybersecurity threat to both hospitals and medical device manufacturers.

The agency sought awareness of several cybersecurity vulnerabilities and associated field experiences that contribute to potential effects on medical devices or hospital network operations. These vulnerabilities included the following five noteworthy items requiring awareness and possible remediation:

1. Network-connected/configured medical devices infected or disabled by malware
2. The presence of malware on hospital computers, smartphones, and tablets that targets mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices
3. Uncontrolled distribution of passwords, disabled passwords, and hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel)
4. Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices)
5. Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plaintext or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL (structured query language) injection[3]

The Threat Landscape

The digital battlefield that hospitals and medical device manufacturers operate in is an ever-evolving threat landscape. TrapX Security first reported evidence of medical devices affected by malware backdoors that breached a healthcare network in 2015[2] and again in 2016. During the 2015 investigation of three separate hospitals in the United States, TrapX reported an "extensive compromise of a variety of medical devices, which included X-ray equipment, PACS (picture archiving and communication systems), and blood-gas analyzers."[3] In the 2016 TrapX investigative reports *Anatomy of Attack, MEDJACK* and *Anatomy of Attack, Hospitals Under Siege* TrapX examined security threats with wireless connectivity as well as traditional LAN.[2,3] Primary, secondary, and tertiary compensating controls were reviewed, offering opportunities for effective remediation of potential cybersecurity threats to medical infusion pumps. Tangible courses of action were designed and offered for ensuring patient safety through the selection, procurement, fielding, and decommissioning process of medical infusion pumps in the face of nefarious cyberactors across the known cyberthreat taxonomy.

Both hackers and information security researchers maintain that having an early-warning system for potential common vulnerabilities and exposures and their impact to the collective information assurance, physical security, and cybersecurity of medical device manufacturers is helpful. However, anyone with enough aptitude, ability, skill, motive, and opportunity can pose a negative cybersecurity threat to both hospitals and medical device manufacturers. Vulnerabilities are numerous enough that novice hackers can easily obtain the tools to compromise a hospital network or a medical infusion pump.[4] Hospitals, medical device manufacturers, and the federal government (including the Federal Bureau of Investigation, Department of Homeland Security, and the FDA) must all develop an effective and enduring response to mutually secure the healthcare cyberlandscape.

Medical Device Manufacturer Challenges

Medical device manufacturers face cybersecurity challenges in large part due to legacy designs, which were developed with the assumption of an innocent world without risks. Today, engineering must take into account new challenges to design, particularly in regards to cybersecurity. The threat landscape now includes the concepts of the IoT, where every device is connected and thus vulnerable to potential compromise. In a 2014 article, Derek Brost categorized nine vulnerabilities associated with medical device security[5]:

1. Clinicians use same medical device components for accessing the web, mail, surfing, etc.
2. Lack of regular security patching
3. Device encryption unavailable
4. Use of antivirus and antimalware not considered or validated
5. Original designs no longer have support for operating systems
6. Open communication ports not secure by design
7. Standard password complexity rules not adhered to
8. Use of Microsoft software that is not patched per manufacturer security bulletins
9. Medical devices inherently viewed as insecure and thus a prime target for compromise by hackers

Another resource is the Integrating the Healthcare Enterprise (IHE) cybersecurity best practices document.[6] In it, IHE describes vulnerabilities about which the medical device world needs to maintain awareness: fundamental terms; known and unknown vulnerabilities related to access and authentication (e.g., administrator and/or user accounts); information (e.g., configuration settings, patient data); applications (i.e., the custom application that provides the device's functionality); device and hospital infrastructure (firmware hardware, information networks); and platforms (commercial off-the-shelf components, [e.g., database and operating systems]).[6] The IHE best practice guide further states that "the larger system of devices and supporting components (workstations, servers)" including implied "security dependencies between" these systems indicates that a medical "device can become a security risk to the system and vice versa, that system components can become a security risk to the device."

Healthcare Cybersecurity Challenges

During a December 2013 event of the Information Systems Security Association, Kevin McDonald, director of clinical information security at the Mayo Clinic, identified device security issues posed by medical device manufacturers, calling "vendors generally clueless" when it came to securing their devices.[7] McDonald also stated that medical device manufacturers had either given no consideration to the security of their devices or worse yet viewed "security as an afterthought."

To validate Mayo's collective concern regarding the lack of cogent medical device security, they conducted penetration testing and vulnerability assessments of a variety of devices during a month-and-a-half evaluation period. McDonald and his team both confirmed awareness of vulnerability issues with medical device security and a worst-case scenario developed regarding what has been procured and placed on Mayo's network infrastructure.

According to Craig Hanson, CISSP, information security manager for Hennepin County Medical Center in Minneapolis, MN, the biggest challenge for cybersecurity in the healthcare industry is the need to overcome an overwhelming technology and expertise gap related to information security (C. Hanson, personal communication, July 2016).

"The main focus in healthcare is quality care and treatment of patients, and rightfully so," Hanson said. "However, when the majority of the available resources go into buying the biggest and best magnetic resonance imaging (MRI) machine, along with technicians to operate the beast, that relegates IT to an afterthought that's fighting for leftover cash. In an industry where the operating costs are so high, financial decisions are made based on return on investment. It's near impossible for IT, specifically information security, to compete against the dollars from pumping 100 patients each week through an MRI. With many years of basic neglect of IT in health-

care, we have been forced to survive on a budget that is typically only able to keep the lights on."

Infusion pumps are specifically vulnerable to cyberthreats, Hanson said, in part because a hacker with malicious intent can override safety protocols and reconfigure the pump to operate in a manner that could harm the patient. Hanson called on manufacturers to allow for certificate-based wireless authentication, such as Protected Extensible Authentication Protocol.[8] "I have seen far fewer WEP-only authentication devices lately, however they seem to be moving more towards a WPA-PSK authentication. It is a step in the right direction, but still behind the times," Hanson said.

What may be considered best practices in the cybersecurity domain for enterprises can also apply to securing medical infusion pumps by design and thus the hospital infrastructure where they are installed.

Unsecure protocols such as FTP and TELNET should be shut down, Hanson said, and anonymous SNMP connections closed off. "It comes down to using only the needed services, and making sure those services are secure in nature," Hanson said. It is important to have mechanism to easily and remotely manage devices on the network. In this world where vulnerabilities pop out of the woodwork faster than we can imagine, it is critical to be able to update devices quickly to minimize the downtimes that affect patient care."

Collaboration and Recommended Actions

If the cybersecurity environment and collaborative domain affect both medical device manufacturers and hospitals, what are the recommended best practices and courses of action to mitigate the security risks posed by ubiquitously interconnected and less-secure medical devices?

The onus is not only to design security into the device, but to build the functional capabilities into the organization. Leadership from the front is necessary. It emphasizes the importance of cybersecurity as a necessary strategic position—more than just a tactical issue to be dealt with by information security professionals. It is no longer optional to design security into medical devices.

The challenge for hospitals and healthcare regulatory authorities is significant. They must begin to demand that medical device manufacturers deliver products with security designed in, rather than as an afterthought.

The challenge for hospitals and healthcare regulatory authorities is significant. They must begin to demand that medical device manufacturers deliver products with security designed in, rather than as an afterthought.

To reestablish mutual cybersecurity trust, medical device manufacturers must assess and evaluate legacy product designs by completing the following actions.

1. Conduct thorough risk and vulnerability assessments of every current and in-development infusion pump. The methodology should be based on what is recommended by the FDA guidance *Cybersecurity for Medical Devices and Hospital Networks*[1]; AAMI TIR57, *Principles for medical device security—Risk management*[9]; the Forum of Incident Response and Security Team's CVSS (Common Vulnerability Scoring System) Version 3.0; and the National Standards Institute's Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*.[10]
2. Field medical infusion pump models that were examined through a rigorous and independent offensive security review.
3. Conduct regular periodic defensive and offensive security reviews as noted in the items above.
4. Build and staff cyber-knowledgeable people into the organization.

Do consistent industry cybersecurity standards need be developed so there is consistency in how security controls are fielded across all device families? (For example: all infusion pumps support a best practice for the cybersecurity of both wired and wireless devices; compensating controls such as the Security Technical Implementation Guides supported by the Defense Information Systems Agency.[11]) Best practices for medical infusion device security manufacturers would enable a positive and

mutually beneficial goal of sustained patient safety and include cybersecurity design considerations in both traditional wired and wireless networked infrastructures.

During a July 2016 medical device security workshop convened by the National Health Information Sharing and Analysis Center, changes in the healthcare industry cybersecurity stance were apparent. Recommendations to the medical device industry by healthcare authorities in attendance included the following requests, which should be considered as mandatory requirements for the cybersecurity of all medical devices:

- Ensure that software is digitally signed by the medical device manufacturer.
- Deliver timely tested security patches authoritatively and proactively.
- Treat medical infusion pumps as networked devices. In today's IoT world, medical infusion pumps are viewed as computers. Manufacturers need to treat them as such in their initial design and security.
- Establish the ability for medical infusion pumps and other devices to join the hospital's active directory domain, which enables centralized deployment of updates.
- Encourage medical infusion device manufacturers, common operating system manufacturers, and antivirus vendors to support efficient, ongoing maintenance and upgrades.

A revised network topology, consisting of segregating the device network from the hospitals in order to protect against network credential loss, would allow for better monitoring of traffic as well as better delegation of connections in the system.

As medical technology is welcomed into IoT, certain required steps are needed to protect our systems from nefarious individuals. From a network standpoint, it would be a good idea to revise the topology, change the way routing is done in your local area network, and alter how your IP (Internet protocol) addresses are delegated. Alongside networking comes authentication, which needs to be handled on both the physical and digital level in order to provide the best security possible.

With the above-mentioned steps, we must further look into what it means to implement these changes. A revised network topology, consisting of segregating the device network from the hospitals in order to protect against network credential loss, would allow for better monitoring of traffic as well as better delegation of connections in the system. Alongside that, there are two options that can be executed to prevent and remediate a multitude of basic attacks against such devices. One option is the use of static IP addresses and ARP (address resolution protocol) tables. This would allow protection from spoofing and possible man-in-the-middle attacks. The second option is the use of network address translation (NAT). NAT would prevent against unwanted amounts of request or data being sent to these devices. NAT allows an individual to map multiple devices to one IP address using only ports to delegate what packets of data go where, with the added benefit of allowing packets of data to only go to devices that are awaiting this information. Block chain methodologies can also be utilized to deter ransomware in hospital environments. An example of block chain may be a master registry of inventoried model and serial numbers validated against MAC (media access control) addresses within the hospitals networked infrastructure. In addition, investigate best practices focused on hardening requirements for the specific hospital database architecture.

Authentication of medical infusion devices on a hospital network is a huge cybersecurity issue. Many of them are implemented without authentication, as this is the least of the medical device manufacturer design concerns. The implementation of top-level security with product design engineering is a requisite cybersecurity condition and characteristic.

As software develops, manufacturers will inevitably issue many patches or updates to the software and firmware of these devices. It is critical to validate software efficacy on these devices to ensure that they are working as intended. It may be tempting to trust the developers who are issuing the patches and updates with the testing of their software and hardware. However, it is unlikely that medical device manufacturers maintain an environment similar to the eventual hospital

installation environment. Therefore, it is important when software testing to slowly roll out the changes to these providers to ensure compatibility and inherent security. Always make sure to test the updates and patches on a few devices to make sure they will interact well within the healthcare environment after deployment. That is a software engineering best practice.

Data integrity, security, and protection will always be a significant concern with the implementation of medical devices. As anonymous as data may seem at the time of transmission, storage, or receipt, skilled adversaries may be able to deanonymize these data. It should be mandatory to encrypt this traffic to protect against any attempt to deanonymize sensitive information. One must always assume the worst case when considering the possible nefarious uses of sensitive information.

In the End, It's Really Only the Beginning

Many medical devices and manufacturers missed the arrival of the 21st century. However, healthcare regulatory authorities must work to protect the confidentiality, integrity, and availability of their interconnected medical devices and prevent patient harm. Through collaborative cybersecurity consonance and a concerted effort, key stakeholders, medical device manufacturers, and healthcare regulatory authorities can work together to achieve a cooperative cybersecurity advantage. ■

References

1. **Food and Drug Administration.** Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication. Available at: www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm. Accessed Dec. 1, 2016.
2. **TrapX Security.** Anatomy of an Attack: Medical Device Hijack (MEDJACK). Available at: http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf?aliId=1494651. Accessed Dec. 1, 2016.
3. **TrapX Security.** Anatomy of Attack: MEDJACK.2, Hospitals Under Siege. Available at: http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_MEDJACK.2.pdf. Accessed Dec. 1, 2016.
4. **Verma A.** Best Hacking Tools of 2016 for Windows, Mac OS X, and Linux. Available at: http://fossbytes.com/best-hacking-tools-of-2016-windows-linux-mac-osx. Accessed Dec. 1, 2016.
5. **Brost D.** Beware These Nine Medical Device Vulnerabilities. Available at: www.24x7mag.com/2014/08/beware-nine-medical-device-vulnerabilities. Accessed Dec. 1, 2016.
6. **Integrating the Healthcare Enterprise.** Medical Equipment Management (MEM): Medical Device Cyber Security—Best Practice Guide. Available at: http://ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.0_PC_2015-07-01.pdf. Accessed Dec. 1, 2016.
7. **McDonald K.** Medical Device Security in a Connected World. Available at: www.researchgate.net/file.PostFileLoader.html?id=54ed93b1d3df3e15178b4610&assetKey=AS%3A273715474960384%401442270262329. Accessed Dec. 1, 2016.
8. **Riley R.** Wireless security with 802.1x and PEAP. Available at: www.blackhat.com/presentations/win-usa-03/bh-win-03-riley-wireless/bh-win-03-riley-notes.pdf. Accessed Dec. 1, 2016.
9. **Association for the Advancement of Medical Instrumentation.** TIR57, *Principles for medical device security—Risk management*. Available at: www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729. Accessed. Dec. 1, 2016.
10. **National Institute of Standards and Technology.** NIST Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments. Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. Accessed Dec. 1, 2016.
11. **Information Assurance Support Environment.** Security Technical Implementation Guides (STIGs). Available at: http://iase.disa.mil/stigs/Pages/index.aspx. Accessed Dec. 1, 2016.

AAMI
Advancing Safety in Healthcare Technology

AAMI AWARDS

Celebrating Excellence and Leadership

Nominations Due Jan. 13, 2017

www.aami.org/awards

Each year the medical technology community recognizes leaders and innovators whose efforts have moved the industry forward.

Winners will be awarded monetary prizes, a plaque commemorating their achievements, and will be celebrated by their peers at the AAMI 2017 Annual Conference and Expo in Austin, TX in June.

★ NOMINATE YOURSELF—OR YOUR PEERS! ★

AAMI Foundation Awards

- AAMI Foundation's Laufman-Greatbatch Award
- AAMI Foundation & ACCE's Robert L. Morris Humanitarian Award
- AAMI Foundation & Institute for Technology in Health Care's Clinical Solution Award

AAMI Awards

- AAMI & Becton Dickinson's Patient Safety Award
- AAMI's HTM Leadership Award
- AAMI & GE Healthcare's BMET of the Year Award
- AAMI's Young Professional Award
- HTM Association of the Year Award
- The Spirit of AAMI Award

Standards Awards

- Standards Developer Award
- AAMI Technical Committee Award

Nominate leaders in the industry today! Find nomination forms and guidelines at www.aami.org/awards