CYBERSECURITY

A treatment plan for medical device cybersecuirty

Managing U.S. medical device cybersecurity across the product lifecycle

"Connected" not only describes our current lifestyle - it is arguably the greatest contributor to the evolution of 21st century healthcare. From robot-assisted surgery to pacemakers, insulin pumps, and health management apps, connectivity is helping to improve care provided at hospitals, clinics, and even in the home environment. But the increasing adoption of connected technologies also means that safety depends on cybersecurity, now more than ever. Many life-sustaining and life-supporting medical devices reside on hospital networks. Even more are connected wirelessly. All of these devices are vulnerable to cyber-attack, making it all the more necessary to implement cybersecurity measures for medical devices and the networks to which they connect.

The Proliferation of Medical Devices

The growth of the medical device technology market shows no sign of slowing, thanks to its significant role in today's complex and multi-faceted healthcare systems. This market was valued at $521.2 billion in 2017, and estimates show it reaching $674.5 billion by 2022 at a compound annual growth rate (CAGR) of 5.3 percent.[1] Some specific devices are growing at a faster rate.

Cardiovascular devices, for example, are growing by 8.8 percent per year.[2]

Portability is also a defining characteristic of this new era of "connected" medical devices. The portable medical device market is growing by over 15 percent annually, and it is expected to reach a value of $47 billion by 2023.[3] Major factors fueling the demand for these devices include:

- Integration of healthcare with information technology and the internet of things (IoT);
- Aging populations;
- Urbanization; and
- Government support for low-cost medical facilities due to rising healthcare costs.[4]

Why Healthcare is Most at Risk of a Security Breach

While medical devices help support a more cost-efficient, coordinated, and flexible healthcare system, the risks associated with network-connected devices make the healthcare industry vulnerable to cyber- attacks. In fact, healthcare is one of the most targeted industries; an IMB report determined that healthcare was the most targeted in 2015.[5]

[1] BCC Research, Medical Devices: Technologies and Global Markets, March 2018. Retrieved from https://www.bccresearch.com/market-research/healthcare/medical-devices-technologies- and-global-markets-hlc170c.html

[2] Ibid

[3] Knowledge Sourcing Intelligence LLP, Portable Medical Devices Market – Industry Trends, Opportunities and Forecasts to 2023, January 2018. Retrieved from https://www.researchandmarkets. com/research/ml2lqm/global_46_9?w=4

[4] Ibid

[5] IBM, 2016 Cyber Security Intelligence Index. Retrieved from https://www.csoonline.com/article/3136323/leadership-management/healthcare-industry-is-the-bullseye-for-hackers-in-2017.html

"Data in this industry can be monetized"

While 2015 saw significant data breaches, research shows that the number of cyber incidents continues to rise year after year in healthcare – especially in the U.S. In 2017, there were a total of 342 security breaches, 72 more than in 2015.[6]

This trend is why the majority of healthcare organizations report feeling very vulnerable to attacks, with some of this fear stemming from the fact that a multitude of devices are produced and sold by thousands of manufacturing facilities.[7] Ensuring a consistent level of security across these widely available devices used around the world is certainly a challenge.

But why exactly is healthcare targeted so frequently?

Data in this industry can be monetized, which is why patient records are in demand in the black market. The information contained in these records – personal information, health details such as active prescriptions, billing addresses, and credit card numbers – can be used for tax fraud, identify theft, or to order medication to sell on the dark web.[8]

Failing to secure medical devices – and the networks to which they connect – compromises patient information and their safety. Hackers with ill-intent could choose to manipulate the function of a life-sustaining or life-supporting medical device. Malware introduced into medical devices through the supply chain or network can cause the device to operate in an unintended and unsafe manner. Ransomware could also be used to prevent healthcare professionals from accessing important data needed to provide critical care and support decision-making:

"Without quick access to drug histories, surgery directives and other information, patient care can get delayed or halted, which makes hospitals more likely to pay a ransom rather than risk delays that could result in death and lawsuit."[9]

Aside from compromising data and patient safety, failure to implement cybersecurity is also a costly mistake. A 2016 research project conducted by the Ponemon Institute revealed that cost to be $6.2 billion annually in the U.S. alone.[10] Research from Accenture indicates that healthcare providers are at risk of losing $305 billion in cumulative lifetime patient revenue over the next five years due to patients switching providers because of medical identity theft.[11]

The shift towards value-based care is also another risk factor to consider. This model of care depends on collaboration among providers, creating a vast network of organizations that serve the same people. But coordinated care provides attackers with multiple access points as these organizations need to share data. In this environment, providers not only need to ensure cybersecurity compliance within their own four walls, but across their network of partners and vendors – which demands significant direction and management from senior leadership.[12] This in turn puts pressure on medical device manufacturers to provide assurance of their product's cybersecurity.

[6] HIPAA Journal, Largest Healthcare Data Breaches of 2017, January 2018. Retrieved from https://www.hipaajournal.com/largest-healthcare-data-breaches-2017/

[7] Douglas Bonderud, "FDA Rolls out New Action Plan for Medical Device Cybersecurity," in Security Intelligence, April 2018. Retrieved from https://securityintelligence.com/news/fda-rolls-out- new-action-plan-for-medical-device-cybersecurity/

[8] Ryan Francis, "Healthcare Records for Sale on Dark Web," in CSO Online, April 2017. Retrieved from https://www.csoonline.com/article/3189869/data-breach/healthcare-records-for-sale-on- dark-web.html

[9] Kim Zetter, "Why Hospitals are the Perfect Targets for Ransomware," in Wired, March 2016. Retrieved from https://www.wired. com/2016/03/ransomware-why-hospitals-are-the-perfect- targets/

[10] Ponemon Institute, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016. Retrieved from https://www.ponemon.org/blog/sixth-annual-benchmark-study-on- privacy-security-of-healthcare-data

[11] Accenture, The $300 Billion Attack, October 2015. Retrieved from https://www.businesswire.com/news/home/20151014005121/en/Cyberattacks-Cost-U.S.-Health-Systems-305-Billion

[12] Gerard Nussbaum and Roey Moran, Value-Based Care Makes Cybersecurity Even More Critical, February 2017. Retrieved from http://www.ecgmc.com/thought-leadership/blog/value-based- care-makes-cybersecurity-even-more-critical

"manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices."

Key Standards and Regulations for Medical Device Cybersecurity

Although cybersecurity for medical devices is still evolving, numerous standards, guidance documents, and regulatory frameworks offer manufacturers and healthcare providers a foundation on which to build to better protect themselves from cyber-attack.

European and International Standards

In Europe, three directives set out the security requirements for medical devices and their required essential performance levels, based on device type:

- 93/42/EC for medical devices
- 98/79/EC for in vitro medical devices
- 90/385/EEC for active implantable medical devices

A number of harmonized standards outline the requirements for incorporating cybersecurity within these directives. For example, IEC/EN 62304 addresses medical device software, requiring manufacturers to prepare a problem report for each problem detected in the software, with information that may aid in developing a solution.

ISO/EN 14971 outlines risk management requirements for medical devices. The Association for the Advancement of Medical Instrumentation (AAMI) produced a guidance document to complement the ISO standard, focused specifically on cybersecurity. AAMI TIR57 helps manufacturers and other users of the ISO standard to:

- Identify threats, vulnerabilities, and assets associated with medical devices;
- Estimate and evaluate associated security risks;
- Control security risks; and Monitor effectiveness of controls.[13]

Building on ISO/EN 14971, a joint working group under ISO and IEC developed the IEC 80001 standard. It took the concepts from the earlier standard and expanded them into the full lifecycle of connected medical devices. This helps healthcare delivery organizations apply risk management to their IT networks that incorporate medical devices.

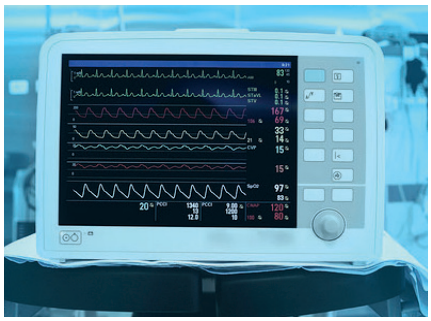
Another international standard, IEC 60601-1, outlines requirements for identifying known and foreseeable hazards, including those that impact data security and the IT network's ability to support the programmable electrical medical system (PEMS) in achieving its basic safety and essential performance. The standard also includes requirements for identifying the causes of hazardous situations associated with IT networks, testing methods for PEMS validation, and instructions from the PEMS manufacturer on connecting PEMS to IT networks that they have not validated.

U.S. Guidance

Given the impact of cyber-attacks to the American healthcare industry, the Food and Drug Administration (FDA) has produced guidance documents that address the following issues related to medical devices:

- Pre-market submissions - offers manufacturers direction on how to address cybersecurity throughout the design and development process, leveraging best practices set by international standards such as IEC 62443 and IEC 80001. Product submission documents from manufacturers should contain information such as hazard analysis, updates and patches, risk controls, and other relevant instructions.
- Networked medical devices containing off-the-shelf (OTS) software - confirms that device manufacturers using OTS software in the device bear the responsibility for its continued safe and effective performance, including the performance of the software.

13 Association for the Advancement of Medical Instrumentation, AAMI TIR57: Principles for Medical Device Security—Risk Management, June 2015. Retrieved from http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729



"Manufacturers find themselves in a constantly changing environment of safety, conformity, and market access requirements"

- Postmarket management of medical device cybersecurity - provides a risk - based framework to help assess when changes to medical devices for cybersecurity require reporting to the FDA. It also emphasizes that manufacturers should "monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices."[14]

In addition to these guidance documents, the FDA is rolling out a new action plan that focuses on "software transparency, mandatory patching, and the creation of an investigative body" to act as the go-to team for device attack investigations.[15]

Following Best Practices with Support from Third-party Testing Agencies

To keep up with advances in technology and IoT, and to compete in a highly competitive and complex market, healthcare organizations and medical device manufacturers must evolve to support and reflect this rapid pace of innovation. Ensuring that these systems and devices are safe for usage by both trained medical professionals as well as inexperienced home users is critical to business success and public safety. As a result, manufacturers find themselves in a constantly changing environment of safety, conformity, and market access requirements – an environment in which they cannot afford to fall behind.

When it comes to cybersecurity, the nature and evolution of network-connected products and systems demand a more holistic, multi-layered *"Defense in Depth"* strategy. This approach helps to protect all assets while recognizing all of the interconnections and dependencies. But it is a challenging strategy to implement.

For manufacturers, this involves protecting:

- Their product IP;
- Their IT networks through regular monitoring and patch updates so that medical devices can be remotely accessed in a safe manner; and
- Personally identifiable information (PII) or personal health information (PHI), which they collect.

This level of protection can be supported through the following activities that align with major regional and international standards:

- Gap analysis – this determines the overall areas of cybersecurity weakness in the product or process, as well as necessary improvements.
- Security Development Lifecycle (SDLC) – a process that helps manufacturers address security threats early in the product lifecycle, before committing to production.
- Embedded Device Security Assurance (EDSA) – a service that provides third- party assurance of the security of embedded devices and their features, as well as the device supplier's development process.
- Bench testing – evaluation techniques used to identify weaknesses and vulnerabilities, as well as necessary security controls.

Recognized third-party testing agencies can help manufacturers comply with cybersecurity standards and other best practice frameworks. CSA Group®, with a long history of working with emerging technologies in the medical space and its cybersecurity evaluation service, offers tailored cybersecurity solutions to medical device manufacturers. The service helps identify potential issues and security measures to provide seamless protection through security testing verification and security assurance certification & attestation.

14 Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, December 2016. Retrieved from https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf

15 Douglas Bonderud, "FDA Rolls out New Action Plan for Medical Device Cybersecurity," in Security Intelligence, April 2018. Retrieved from https://securityintelligence.com/news/fda-rolls-out- new-action-plan-for-medical-device-cybersecurity/

Class I

These devices present minimal potential for harm to the user and are often simpler in design than Class II or Class III devices. Examples include enema kits and elastic bandages. 47% of medical devices fall under this category and 95% of these are exempt from the regulatory process.

Class II

Most medical devices are considered Class II devices. Examples of Class II devices include powered wheelchairs and some pregnancy test kits. 43% of medical devices fall under this category.

Class III and IV

These devices usually sustain or support life, are implanted, or present potential unreasonable risk of illness or injury. Examples of Class III devices include implantable pacemakers and breast implants. Approximately 10% of medical devices fall under this category.

SOURCE: Food and Drug Administration. Retrieved from https://www.fda.gov/MedicalDevices/ResourcesforYou/Consumers/ ucm142523.htm

For medical devices that require a premarket approval (PMA) from the FDA, the premarket guidance for cybersecurity is an important consideration when crafting regulatory submissions. However, even devices which are exempt from the PMA process should also have, at a minimum, a security risk management as a part of the product design outputs to help assure that the risks due to cybersecurity are identified and mitigated. In addition, the information in the FDA postmarket guidance on cybersecurity should also be considered for all connected devices regardless of classification, and the management of postmarket security should be addressed.

Custom training workshops can also help provide practical solutions for beginning or expanding your organization's security assurance know-how. Sample topics for workshops include:

- Introduction to Cybersecurity
- Security Risk Analysis (Threat Modeling)
- Quality Management and Supply Chain Considerations
- Security Assurance
- Specific Standards for Cybersecurity

Cybersecurity as Part of the Treatment Plan

To help deliver quality care through the use of medical devices, cybersecurity evaluation must become part of the plan. The high risk of a breach to health networks and medical devices makes it critical to work with a recognized third party early in the product development cycle to meet cybersecurity standards. Securing these devices against advanced threats and meeting the required standards helps protect the device's functionality, personal information, and more importantly, the patient's health and safety.

Contact Us

Put CSA Group's industry-leading knowledge and experience to work for you.

866 797 4272
certinfo@csagroup.org
csagroup.org