Dynamic Blog

Home / Validation & Testing Solutions / 5 Cybersecurity Strategies for Medical Device Management

5 Cybersecurity Strategies for Medical Device Management

From pacemakers and implanted defibrillators to drug infusion pumps, MRI machines and more, the healthcare industry is heavily dependent upon medical devices, and, as with virtually any technology, there is a degree of inherent risk involved with the security of these devices. With so many different products and corresponding avenues for potential cyberattacks, medical devices must be free from any gaps or vulnerabilities in efficiency, effectiveness and especially cybersecurity. Medical device manufacturers have the responsibility to ensure all their devices are highly secure and meet regulatory requirements.

Some of the reasons these devices are at risk are because many medical devices run on old operating systems with well-known vulnerabilities and rarely have software updates. Likewise, hospitals themselves typically cannot update software or install security patches.

Here are five strategies for improving security in medical devices.

1. Implement an ITAM program.

If you can't keep track of all the medical devices within a hospital, for example, that is cause for concern and automatically poses a significant risk. An IT asset management (ITAM) program can help with keeping a record of all device inventory as well as their purposes, when they were last updated, where in the hospital system they are located, etc. Visibility into all connected devices is essential for developing a concrete plan to manage them, as well as preventing lost or stolen devices with which hackers can easily tamper.

2. Build security into devices from the beginning of product design.

Medical device manufacturers need to prioritize baking security into product design, in its infancy, as opposed to thinking about it further down the road and tacking on security measures that aren't as effective and will most likely cost more. Building security in from the beginning provides a critical first layer of defense, allowing security customization for each device and ensuring that a firewall is not the sole form of security. Additionally, this allows devices to meet FDA security guidelines. Engineers must consider how much a security failure would cost — not just monetary but social, environmental and economic cost as well — weighing the potential risk of attack against the price of implementing a security solution.

3. Manage and review vendors regularly.

Having clear insights into vendors' plans for their devices, including risk management, is essential in determining whether to work with them, trust their devices and allow them to access such sensitive data and information. Healthcare systems must be knowledgeable about how often vendors' medical devices receive security updates, as well as what potential vulnerabilities may correspond with such devices. This type of information is key to deciding whether to proceed with a vendor and rely upon their devices.

4. Reduce the quantity of data on connected devices.

Using the minimum amount of data helps simplify security processes and ultimately leaves a smaller amount of information susceptible to attacks. Firewalls and other network-based protection also help protect end-user devices.

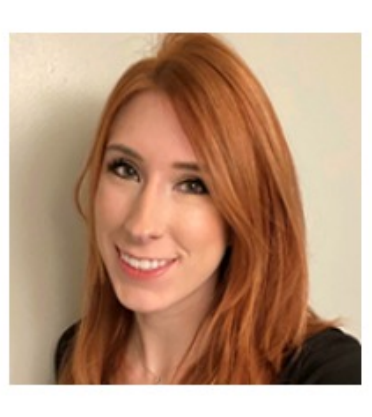
5. Focus on network segmentation.

With so many types of disparate technologies in the healthcare industry, a large portion of them is not secure. Network segmentation is cited in the National Institute of Standards and Technology (NIST) SP800-125 as an important part of maintaining cybersecurity in medical devices, and it means that a network is broken into sections, grouping devices with similar security requirements together into one segment and subsequently restricting any network traffic that attempts to cross those segments. For example, all devices that are shared — such as MRI and CT machines — might be placed in one segment, which is separated from the rest of the connected medical devices. These devices can also be segmented by floors in a hospital, or hospital-owned devices vs. patient- and employee-owned devices. This helps ensure that, if someone were to gain access to one of the network's devices, they would not be able to reach the overall network as well. To implement successful segmentation, cybersecurity teams first must analyze all devices connected to the network for their current security statuses. Then, they must choose whether to utilize physical, on-premise segmentation or virtual segmentation. On-premise is the most expensive segmentation type and takes the longest to fully put in place, but it can also be the most secure. Moving devices to the cloud is another option, and it's easier than physical segmentation, but it is not as effective. Consistent monitoring of segments and network usage is also critical, and it allows cybersecurity teams to detect anomalies and unusual behaviors in devices.

A common misconception is that the FDA tests all medical devices for vulnerabilities. In fact, it is the responsibility of device manufacturers to ensure that their devices meet all requirements. This places significant responsibility on the shoulders of medical device manufacturers, and it is essentially up to them to ensure that their devices are designed to withstand cyberattacks and security vulnerabilities before sending products into production.

Have Questions?

Dynamic offers support for all your connected medical devices. Contact us at 866-399-1084 or info@dccit.com to find out more.



Rachel Zachar
Content Manager

Search

CATEGORIES

Technology Supply Chain Management
Validation & Testing Solutions
Complex Technical Configuration
Technology Asset Lifecycle Management
Thought Leadership
Company News
Uncategorized

SUBSCRIBE TO OUR POSTS

Email*

Subscribe

RECENT POSTS

Just-In-Time Inventory Management May No Longer Be Viable. What's Your Strategy Now?
June 14, 2021

Managing the Lifecycles of Medical Device Workstations
June 2, 2021

Dynamic Computer Corporation Changes Brand Name; Will Operate as Dynamic Technology Solutions^SM
May 13, 2021

Looking for help with your next project?

LET'S TALK

DYNAMIC TECHNOLOGY SOLUTIONS

Dynamic is recognized as the leader in sourcing, testing, configuring and End-of-Life transitions for electronic technology within highly regulated industries. We deliver asset and lifecycle management services as an integrated solution that is compliant, consistent and controlled. Over the past 40 years we have applied a customer-focused approach that has served as the cornerstone of our success.

23400 Industrial Park Court
Farmington Hills, MI 48335

866-257-2111
248-473-2200

Dynamic Technology Solutions is a Service Mark of Dynamic Computer Corporation.

Certified WBENC Women's Business Enterprise

9001 ISO 13485

MBE

SBA WOSB Woman Owned Small Business

Contact Us

First Name
Last Name
Email
Message
Send

Subscribe to Our Blog Posts

Email
Send