

Medical Design & OUTSOURCING

THE U.S.-CHINA TRADE WAR:



Here's what it means for medical device industry suppliers

**8 MEDICAL DEVICE
INDUSTRY SUPPLIER
INNOVATIONS YOU
NEED TO KNOW**

**THE TOP 10
MEDICAL
DEVICE STATES**

CUSTOM + ONE-WAY CHECK VALVES • SMARTPRODUCTS.COM



How to avoid having your medical device hacked

Leaving a medical device vulnerable to hacking is just too risky. Medtech manufacturers can take several steps to lessen the likelihood of such attacks.



Stephanie Van Ness |
Integrated Computer
Solutions |

From pacemakers to light scopes to infusion pumps, today's connected medical devices not only appeal to clinical users but cybercriminals as well. The potential for security breaches should alarm device manufacturers and users, as breaches can put patients' lives, customers' sensitive data and companies' financial futures at risk. Meticulous, security-conscious development can be the antidote to cyberhacking.

A growing menace

Thanks to the rise of the Internet of Things (IoT) and the push for greater connectivity, more devices — and more-sensitive devices — are susceptible to malicious hackers. In the U.S. there are 10 to 15 connected devices per hospital bed, many

of which are vulnerable to cyberattack, according to a report by Alpine Security.

Medtronic made news in March 2019 when it disclosed a security flaw in some of its implantable defibrillators that allow for remote monitoring. This disclosure was made after the Dept. of Homeland Security flagged a critical cybersecurity weakness in one of the company's cardiac devices, rating the weakness 9.3 on a 10-point vulnerability scale. The flaw, present in the device's Conexus wireless communication protocol, could allow unauthorized access and changes to the settings of the device and at-home monitors.

In 2017, the FDA recalled 465,000 radio-controlled implantable cardiac pacemakers made by St. Jude Medical. The reason: too much potential for cybercriminals to hack the devices. For instance, hackers could run down the batteries or alter the patient's heartbeat, both worst-case scenarios that could result in the death of the patient. Affected patients did not have to have the devices removed. Instead, Abbott, which owns St. Jude, issued a firmware update in 2018, incorporating more stringent security.

Certainly, networked devices allow physicians and other professional caregivers access to expansive data, which can lead to better patient outcomes. In fact, Medtronic suggested the remote monitoring feature of its flagged defibrillators delivers substantial-enough benefits to outweigh the potential security risks. Still, it's clear that stringent security measures are necessary when developing and using connected medical devices, especially given the number of device makers looking to leverage these devices' capabilities.



Critical steps for building connected devices

- Build security into IoT applications and devices during the design phase.
- Prevent unauthorized users from gaining access.
- Limit data collection to information required for the device to operate as intended; only keep data for the shortest amount of time necessary.
- Design products to ship with unique credentials, or require users to set new credentials the first time they use the device.
- Monitor the health of devices and provide patches as soon as vulnerabilities are identified


Last year, the U.S. Dept. of Health & Human Services recommended that device makers and the FDA conduct pre-submission meetings to better address questions regarding networked-device cybersecurity. The FDA asked manufacturers to provide the information below in their submissions:

- Hazard analysis listing the cybersecurity risks considered and the cybersecurity controls incorporated into the device.
- Traceability matrix linking the actual cybersecurity controls to the risks that were considered.
- Manufacturer's plans for validating and updating device software.
- Description of controls in the software supply chain.

For healthcare organizations, designing security measures in their systems from the outset should be fundamental, as is addressing security at the network and application levels. On the network level, that may involve guarding against an imposter device sending incorrect information that could corrupt application data. Regarding the application layer, which includes web, mobile or cloud-based applications connected with the device, security must be addressed during both design and development phases, as well as during testing. Penetration testing of embedded and connected devices can help confirm they're secure.

For devices users, whether that's the nurse or physician in a clinical setting or a patient or non-professional caregiver in a home setting, the key is to remain vigilant by addressing basics like changing default passwords when setting up a device. According to IBM, most consumers don't change factory settings, yet many IoT devices are shipped with default usernames and passwords that can be found with a simple Google search.

Shared responsibility

It's impossible to build a 100% secure device — hackers are simply too skilled and too motivated, and increasingly sophisticated technologies are continuously emerging — but the consequences of a malicious medical device hack can be devastating. All stakeholders, including device manufacturers, healthcare organizations, care providers and patients, must be responsible for cybersecurity. Cybersecurity experts and the FDA should also do their part to ensure that using these devices does not pose an unacceptable level of security risk. 

A Pressing Need, A Unique Event

The combination of innovative research, powerful, low-cost enabling technology, and the support of business, government and academic leaders, would seem to bode well for the commercial prospects of healthcare robotics.

But despite the monumental potential of healthcare robotics technologies and obvious need, commercial development of healthcare robotic products has been relatively slow. What is required is a new class of event specifically constructed to provide engineers and engineering management with the technical information and guidance they need to more quickly and easily design, develop and manufacture the next generation of commercial class healthcare robotics systems. That event is the **Healthcare Robotics Engineering Forum**.

Healthcare Robotics Engineering Forum tracks:

- Enabling Technologies Track
- Tools and Platforms Track
- Design and Development Track
- Management and Opportunity Track

DECEMBER 9-10, 2019
SANTA CLARA CONVENTION CENTER
SANTA CLARA, CA



healthcareroboticsforum.com

EXHIBIT AND SPONSORSHIP OPPORTUNITIES
For more information, contact Mike Emich 508.446.1823, memich@wtwhmedia.com,

PRESENTED BY:

THE **ROBOTREPORT**

PRODUCED BY:

WTWH
Media LLC