By Anthony J. Montagnolo

Cybersecurity: It's Clinical, Too

Connected medical devices bring new risks. Trustees can help manage them.

Imagine this text message shows up on your smartphone: "Dear John, we have complete control of your pacemaker software. Please remit $10,000 to our offshore bank immediately or we will drain your battery."

Some might say this is a bit far-fetched. But many in health care must consider possibilities along these lines every day. With ransomware attacks such as WannaCry — which hit Britain's National Health Service — frequently in the news, and with hospitals' clinical technology becoming more and more connected to information technology systems, the cybersecurity risks associated with medical devices are constantly growing. So, while connected medical devices provide numerous ways to better coordinate patient care, with all of its benefits, those connections simultaneously expose us to new risks, which we now must manage.

With increased exposure, experts worry a hacker could connect remotely to a hospital network and the medical devices connected to it. We must all better understand these risks so we can reduce their possible effect on our patients.

Connected risk

In many ways, this risk has been building over the past 20 years as medical devices have incorporated software and software systems into their design. More recently, though, the risks have escalated as more devices connect to hospital networks, outpatient networks and even home networks. More technology means more risk. And more connected technology means more connected risk.

In today's hospital, according to our research, there are approximately 15–17 devices per bed, and about one-quarter of those bedside devices are networked. With more medical devices like physiologic monitoring systems connecting via hospital networks to electronic health records and other information systems, medical device cybersecurity vulnerabilities extend beyond the patient bedside. These connected devices could serve as entry points into a hospital's network, placing operations, medical information, and patient identity and financial information at risk. Older devices can bring more risk: Many medical devices

TRUSTEE TALKING POINTS

- Medical devices increasingly are connected to hospitals' and health systems' information technology systems.
- With this, the threat of hacking and cybersecurity risks become more severe.
- Trustees have a role to play in helping management decide which medical devices are most important or vulnerable and take steps to protect them.
- Continuing education and adaptation are prerequisites for cybersecurity.

IMAGES FROM GETTY IMAGES

have long lifespans and, consequently, these systems may have older operating systems that are more vulnerable.

We should also note that while the Food and Drug Administration is acutely aware of medical device cybersecurity and has issued guidelines and recommendations, it does not test devices for these vulnerabilities. The FDA describes the perception that it does so as a ‘myth’ in a fact sheet it published. ‘The FDA does not conduct premarket testing for medical products,” the sheet reads. “Testing is the responsibility of the medical product manufacturer.” We have a robust medical device industry with thousands of manufacturers, however, and many are relatively small, with limited resources for making their devices secure.

Governance oversight

As trustees, then, what should you keep in mind to help health care management address the device cybersecurity risk? We recommend some basic but important steps.

PRIORITIZE: As a first step, make sure you consider medical device cybersecurity in the context of other cybersecurity risks in your organization. While no patient harm has occurred to date as a result of hacked medical devices, several facilities have experienced loss or ransom of financial information and/or identity, often through relatively simple email phishing scams. Then, work with management to prioritize which types of connected medical devices need attention first. For example, make sure you are protecting patients by focusing on life-critical devices over less risky devices. And protect your organization’s information by focusing on devices and systems that contain “Protected Health Information” under the Health Insurance Portability and Accountability Act.

IDENTIFY: Now that your management team knows which device types to start with, step two requires that your organization create an inventory of all equipment in the device types. This inventory should include key information such as the exact software version, network configuration settings, and which information systems or devices they are routinely connected to. Without knowing exactly what software is running and what connections exist, it is impossible to establish and maintain good cybersecurity practices.

PROTECT: Step three is the active practice of maintaining and improving your medical device cybersecurity. Work with vendors to make sure your organization is getting updated software to patch identified vulnerabilities. Make sure your wired and wireless networks are using appropriate security methods and that your networked devices can support them. Use safeguards like firewalls or private networks around less-secure equipment to reduce its risk, or plan for its replacement.

Collaboration and growth

While medical device cybersecurity gives us all reason to worry, two additional key questions for trustees to ask can help mitigate risk: (1) Who exactly are the people responsible for medical device cybersecurity in our facility? And (2), what type of ongoing medical device cybersecurity educational training are those team members receiving?

These questions are important because medical device cybersecurity requires a blended knowledge of IT and medical technology. The team responsible for protecting patient care and information must have expertise in both.

Often, medical device cybersecurity requires collaboration between any number of departments or functions. These departments may even be working together for the first time. Like any collaborative endeavor, we suggest making sure that there are clear management processes in place. For example, because many medical device cybersecurity risks arise suddenly, each institution must set policy on both responsibility (who is responsible for what aspects of the system) as well as escalation and handoff (how to transfer aspects of a multidepartment issue to the right party) in advance.

Furthermore, because we are suggesting that cybersecurity policies and procedures address the specific threat related to medical devices, not simply IT systems, your organization must build its medical device cybersecurity risk assessment program into the basic IT security program or parallel to it. In particular, the program must not only include a risk assessment but must also create a program of proactive application of manufacturer-validated software patches for medical devices.

Cybersecurity Help

A number of organizations are working to inform and protect the health care field and the public in the area of medical device cybersecurity. Publications, alerts, seminars and tools are available from groups including:

- The Food and Drug Administration (**www.fda.gov**).
- The Association for the Advancement of Medical Instrumentation (**www.aami.org**).
- ECRI Institute (**www.ecri.org**).
- The Healthcare Information and Management Systems Society (**www.himss.org**).

In addition, training must be ongoing because medical technology and IT change so rapidly and malicious actors become increasingly more sophisticated. While the field of cybersecurity for medical devices grows, trustees should help ensure that appropriate personnel, time and money are available for staff to access and participate in the many different organizations trying to keep the health care community informed of potential risks.

Connected technology has obvious advantages, but as with progress in many areas, it brings new risks. If we understand these new cybersecurity risks and take the appropriate steps, we will create a more protected network and a more secure patient experience. The price of connectedness is eternal vigilance, but the value of connectedness is truly better care. So, be vigilant. T

Anthony J. Montagnolo, *M.S. (amontagnolo@ecri.org) is executive vice president and chief operating officer of ECRI Institute in Plymouth Meeting, Pa.*

Reprinted with permission from the July/August 2017 issue of Trustee *magazine, vol. 70, no. 7.*