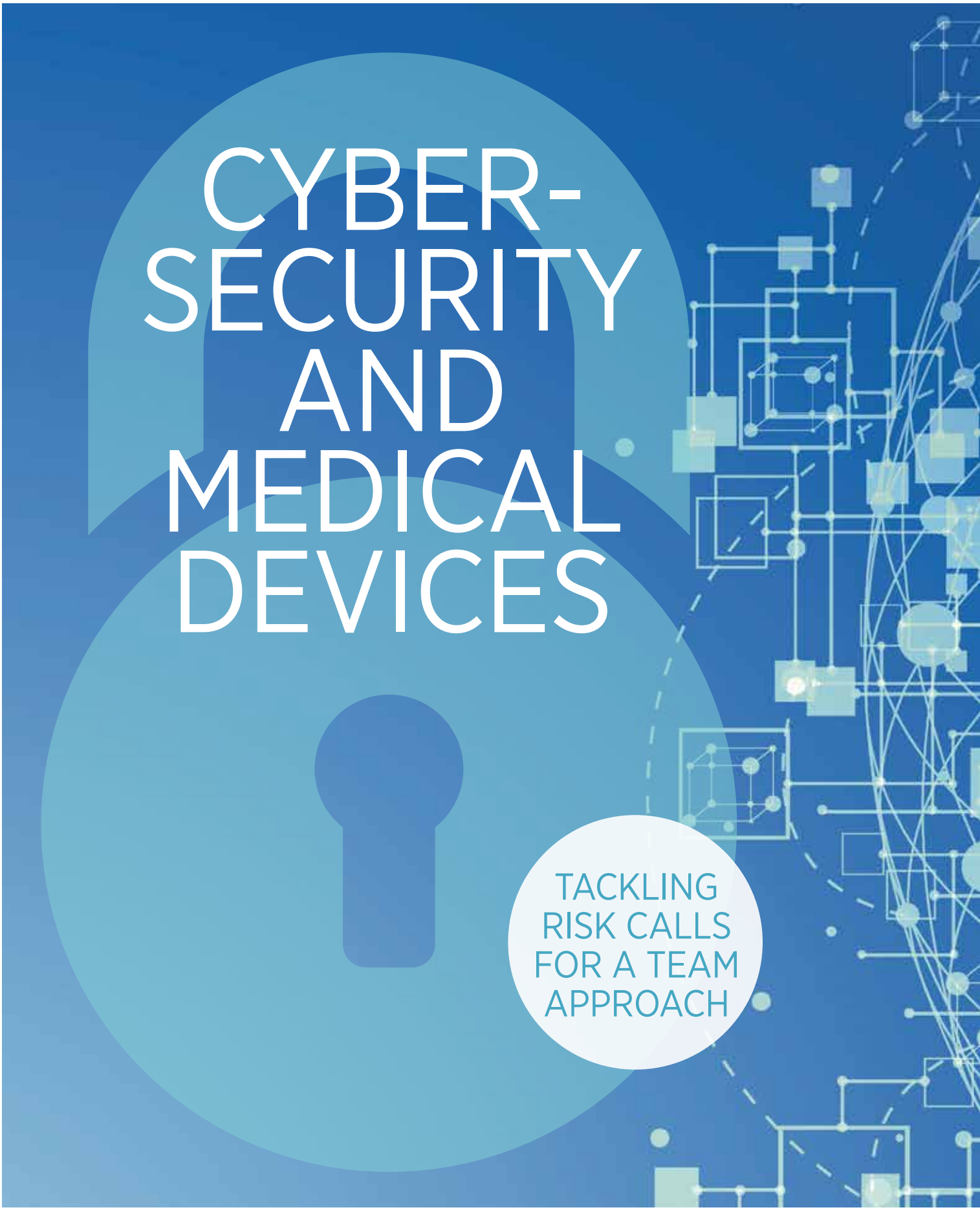

CYBER-SECURITY AND MEDICAL DEVICES

TACKLING RISK CALLS FOR A TEAM APPROACH

When we think about hackers breaking into an insulin pump or pacemaker, it probably seems more like a plot from a cable TV drama than an actual threat. But with the U.S. Department of Homeland Security investigating roughly two dozen cases of suspected vulnerabilities in medical devices, it's clear hospitals can't ignore the risks.

Addressing these threats is a complex task, and not just because a compromised device looks identical to a functioning one. In fact, the problem goes beyond the devices themselves—it's also how people use them that creates risk. Fortunately, there are steps healthcare organizations can take to reduce vulnerability around medical devices and equipment, and the supply chain department is growing more cognizant of cybersecurity risks when considering potentially vulnerable devices. The trick is getting everyone to the table—and that's where supply chain can play an important role. Since they work with both departments, supply chain professionals may be integral in bridging IT and clinical silos when it comes to this emerging challenge.

SECURITY GAPS

According to Reuters, the federal government's investigation includes an infusion pump from Hospira Inc., as well as implantable heart devices from Medtronic Inc. and St. Jude Medical Inc. Even though these devices are being investigated for potential flaws, the fact remains there have been no actual cases of cyber attacks reported to date.

Kevin Fu

"It's not all gloom and doom," says **Kevin Fu**, Ph.D., a researcher from the University of Michigan whose work centers on cybersecurity in medical devices. He stresses putting the problem in context, understanding that patients prescribed medical devices are typically safer using them than not.

"It would be a real tragedy if patients stopped using devices out of fear rather than logic," he says. "It's not a question of do we use these devices or not, but how do we make them better?"

Several different types of flaws can impact medical devices and equipment, and not always in the expected ways. For instance, there's the accidental breach, in which a piece of malware inadvertently gets transferred to a device.

"In this case, it's not intentionally trying to cause harm," says Fu. "It doesn't necessarily hurt anyone; you just might not be able to use the device."

He says devices most at risk are those running outdated operating systems like Windows XP. Since security updates are no longer available, Fu says more recent malware five to 10 years old has no trouble getting in.

And while the U.S. Food and Drug Administration (FDA) provides guidance to help manufacturers reduce vulnerabilities, Fu points out this does nothing to prevent usage problems in the hospital setting.

"It begins with good hygiene," he says. "Any clinician knows how to properly wash his or her hands, but when it comes to cybersecurity, there's a lack of awareness about how things spread."

Fu uses the example of plugging unverified USB drives into medical devices, a common practice that provides an easy entry point for malware.

"You can do all the work you want on a medical device, but it doesn't mean a thing once people start plugging them together," he says.

With no guarantee medical devices are free of vulnerabilities, it's up to hospitals to enact additional controls. Flawed medical devices, improper use and even network vulnerabilities have the potential to compromise not only patient health, but also the organization as a whole.

WHO'S ACTUALLY RESPONSIBLE?

Unfortunately, cybersecurity isn't necessarily top priority for all manufacturers. It's definitely on their radar, Fu says, but their primary aim is to sell devices.

"Some manufacturers are completely unaware," he says, noting smaller companies often fall into this category. "I do know some small companies that invest time and effort in security at the design phase, but many don't get it because it's hard to explain in economic terms."

Frank Platt

With no guarantee that medical devices are free of vulnerabilities, it's up to hospitals to enact additional controls. Flawed medical devices, improper use and even network vulnerabilities have the potential to compromise not only patient health, but also the organization as a whole.

Just ask **Frank Platt**, a Nashville-based information security consultant and Certified Information Security Systems Professional (CISSP).

"If there's a breach, and personal health information gets out, you've now got a serious HIPAA violation. That can mean huge fines and criminal penalties, even jail time," he says.

Cybersecurity around medical devices is still an emerging issue, and as a result many organizations don't know who should be actively managing it. The IT department understands security, but not necessarily medical equipment. Biomedical staff understand the equipment, but not always the security side. The fact that healthcare organizations are composed of multiple silos doesn't help.

"Siloing is a huge stumbling block when it comes to security," Platt says. "People don't always want to give up information, and it becomes an issue because not everybody is forthcoming about what they're trying to accomplish."

WHAT HOSPITALS CAN DO

Several groups offer guidance to help hospitals proactively mitigate cybersecurity risks in medical devices. In 2014, the National Institute of Standards and Technologies (NIST) released its "Framework for Improving Critical Infrastructure Cybersecurity," which resulted from President Barack Obama's directive on the issue.

The Medical Device Innovation, Safety and Security Consortium (MDISS) also provides a tool called the Medical Device Risk Assessment Platform, or MDRAP, that helps providers evaluate device security as part of their procurement practices.

Continued on page 34

Continued from page 32

In addition, the Healthcare Information and Management Systems Society (HIMSS) publishes a form called the Manufacturer Disclosure Statement for Medical Device Security (MDS2), which lets device manufacturers disclose security features to providers.

HIMSS is clear, however, that the MDS2 form alone isn't enough. Instead, hospitals should use it as part of a larger risk assessment, something Platt says is key to ensuring an organization fully addresses these threats.

In fact, HIPAA guidance directs hospitals to use the risk management framework set forth in NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. This type of high-level risk assessment is important because it brings all relevant parties to the table, ensuring everyone is working toward a common goal.

"To truly mitigate the risk, organizations need several layers of technical, operational and management controls around assets containing vital information," Platt says. "It's what we call a defensive depth approach."

Management controls include things like planning and risk assessment, a crucial part of identifying vulnerabilities. Operational controls, on the other hand, help ensure internal procedures contribute to overall security.

Platt uses an example of how human resources policies can create risk for an organization. If there's no process informing IT of role changes or terminations, hospitals can easily end up with a whole list of outdated login accounts that haven't been accessed for months.

"If I'm a hacker, the first thing I'm going to do is figure out how to access that list and take over one of those accounts," Platt says. "And there's no technology in the world that's going to tell you it's happening, because it's a legal account they're using."

Not surprisingly, technical controls include measures such as access control and systems protections. Platt points to some hospitals now using physically separated networks to control all Wi-Fi devices connected to medical equipment, systems and devices.

"It's a pretty expensive control. It doesn't necessarily eliminate the ability to get into a specific medical device, but it does protect patient information," he says.

Platt suggests avoiding those point solutions where someone's trying to sell a security product as a silver bullet, noting there are less expensive, common-sense approaches. "They don't require a lot of money, but they do require somebody focused on the bigger picture."

Ultimately, experts say hospitals will still have to manage legacy devices, many designed over a decade ago without security considerations in mind. Fu says in some cases, that will mean having to live with detection of security breaches rather than prevention of them.

"Just like there are certain viruses we don't know how to cure, simply being aware can lead to smarter thinking and actions," he adds. **S**