COMBATING CYBERTHREATS TO MEDICAL DEVICES

Remediation strategies to reduce patient care risk

SPONSORED BY: American Hospital Association™ | PHILIPS

COMBATING CYBERTHREATS TO MEDICAL DEVICES

Remediation strategies to reduce patient risk

Breaches of medical devices can cause an interruption in data flow or result in the inoperability or malfunction of the device, which can impede care and threaten a patient's safety. There is rising concern about the potential vulnerability of network-connected and network-capable devices that communicate with the electronic health record (EHR) and are integral to the entire hospital network. Cyber-risks are changing daily because of new threats. Implementing an effective cybersecurity plan and continuously assessing an organization's enterprise cybersecurity posture can help mitigate risk of attacks that not only could impact patient care, but also cause financial and reputation damage to a hospital or health system. ●

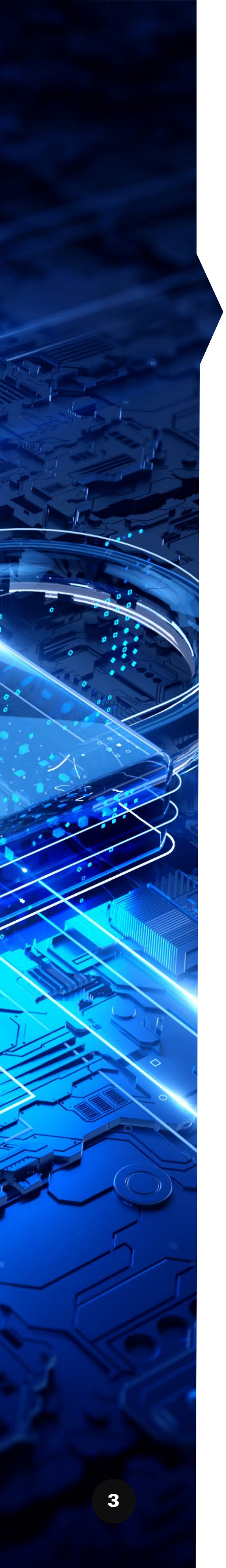
KEY FINDINGS

1 Translate cyber-risk as an **enterprise risk and patient safety issue** to executive leaders and boards. Communication strategies to inform executive leaders could include providing a cyber-risk and vulnerabilities scorecard, the potential impact of the vulnerabilities to patient safety and data or a report on the increased costs of cyber insurance and daily revenue loss if the organization's IT systems were disabled as the result of a ransomware attack. Determine who has designated and delegated authority to make time-sensitive critical decisions during a cyberattack. For example, who has the authority to disconnect the hospital from the internet during a cyberattack? Is that authority and process documented in the incident response plan (IRP) and has there been an analysis of what the clinical impact would be on care delivery and to medical devices if that were done?

2 Develop a proactive plan to address cyberthreats by **identifying potential medical device system vulnerabilities,** reporting and acting upon these cybersecurity risks and implementing a remediation-management plan to prioritize items requiring the most immediate response. Special attention should be given to network capable life-saving and life-support medical devices. Medical-device vendors need to provide software patches and guidance on how to apply the patches and secure devices.

3 Have plans in place for **how to continue care when medical devices go offline.** There is an expectation by staff that equipment will work properly. Staff should be trained in downtime procedures to work around technology and perform operations manually, wherever possible, in the event medical devices such as drug infusion pumps and ventilators become inoperable during a cyberattack. Downtime procedures should be thoroughly tested in advance.

4 Use **metrics to assess vulnerabilities** and implement remediation-management processes. Clinical engineering and information security teams need to work together to maintain a dynamic inventory of medical devices, regularly patch and test for vulnerabilities and perform annual internal audits to identify remediation priorities. Again, constant monitoring for potential vulnerabilities in health care providers' most mission-critical life support and life-saving devices is an essential process to preserve patient care and protect patient safety.



PARTICIPANTS

Mike Canfield

VICE PRESIDENT AND CHIEF INFORMATION OFFICER

AUGUSTA HEALTH | FISHERSVILLE, VA.

Nancy Drews, R.N.

PRIVACY OFFICER AND CLINICAL INFORMATION DIRECTOR

ADVENTIST HEALTH | SONORA, CALIF.

David Franklin

DIRECTOR, BUSINESS DEVELOPMENT, CUSTOMER SERVICES

PHILIPS | BRENTWOOD, TENN.

Will Landymore

MANAGER, VULNERABILITY AND RISK

NEW YORK-PRESBYTERIAN HOSPITAL | NEW YORK, N.Y.

Peter Marks, Ph.D.

VICE PRESIDENT AND CHIEF INFORMATION OFFICER

WAKEMED HEALTH & HOSPITALS | RALEIGH, N.C.

Richard Meeks

CHIEF COMPLIANCE OFFICER

EVERGREEN HEALTH | KIRKLAND, WASH.

George Reed

DIRECTOR OF CLINICAL ENGINEERING

WAKEMED HEALTH & HOSPITALS | RALEIGH, N.C.

MODERATOR **John Riggi**

SENIOR ADVISOR FOR CYBERSECURITY AND RISK

AMERICAN HOSPITAL ASSOCIATION | WASHINGTON, D.C.

COMBATING CYBERTHREATS TO MEDICAL DEVICES

Remediation strategies to reduce patient care risk

MODERATOR *(John Riggi, American Hospital Association):* **Knowing that sometimes there's a gap between clinical engineering and cybersecurity teams, which may impede visibility from the information security team, how is your current cybersecurity program structured and how do you assess risks to medical devices?**

PETER MARKS *(WakeMed Health & Hospitals):* At WakeMed, clinical engineering is aligned with the chief information officer and we have adopted the same process that we have for traditional information technology (IT) equipment for security. We have a policy that specifies the cyber expectations, which we share with our vendor partners. For any new technology, our partners complete a document detailing the cybersecurity and infrastructure of their solutions. Every Thursday, all the engineers on the tech side, the clinical engineering side and the cyber side get together to evaluate alignment with our policy protections. If not, we collectively try to figure out if we can mitigate the risk.

If we can't, we go to the vice president in that area and the compliance officer detailing the risk and weighing the reward of the system. Often, the VP of the area decides that the risk is not worth the potential value. Our leadership team supports this approach.

MODERATOR: David, how do you see this in the Philips customer base?

DAVID FRANKLIN *(Philips):* Philips is getting a lot of questions right now. It's really divided into two types of customer questions. Customers are asking what Philips does to ensure that our equipment has cybersecurity and to assess and evaluate it. When Philips produces a new piece of equipment, it has built-in software for the security. A question asked of Philips multivendor services is how we address cybersecurity on non-Philips equipment. Philips is creating a service offering to perform cybersecurity assessments on other medical manufacturers' equipment, because our customers often say that they don't know their current cyber health.

MIKE CANFIELD *(Augusta Health):* We have an outstanding internal clinical engineering team that also reports to me along with IT security. They collaborate well together. Our clinical engineering team has kept some old but stable equipment in use for us, which has been in the patients' and the hospital's best interests. Our approach from a security perspective has been technical isolation and segmentation. We are still relatively segmented in clinical engineering and the EHR. So, our monitors and pumps are not feeding direct data back into our EHR. That segregation strategy is a little easier for us than those that have tight device integration.

MODERATOR: Great points! Significant medical device cybersecurity issues on the manufacturer side are security by design and software bill of materials. That's why at AHA we pushed the manufacturers for lifetime-support devices and security by design. From the provider side, network segmentation of medical devices helps mitigate the cyber-risk they may cause or be susceptible to.

WILL LANDYMORE *(New York-Presbyterian Hospital):* I'm the manager of the vulnerability and the risk teams at New York-Presbyterian Hospital. In our onboarding process, we ask the vendors for certain criteria to be part of our network; it's similar to a high-level risk assessment. But once the devices are onboarded, then it falls to the vulnerability team for penetration testing to assess the risk of these devices. If we find a vulnerability that's extreme, we'll bump it off the network. We do get that because the vendor has not applied patches. There is shared responsibility here. The vendor will need to provide guidance on how to secure these devices when they don't come to us as hardened as they should before becoming part of an enterprise network.

FRANKLIN: For equipment requests for proposal, Philips is receiving RFPs with language from the customers stating, 'Tell me certain key points about software patches, when they're upgraded, how long will Philips provide them, etc.' And Philips is also receiving questions from the customer regarding multivendor services asking, 'What role will Philips perform if a customer incurs a cyberattack; what happens from there?'

NANCY DREWS, R.N. *(Adventist Health):* I'm the clinical information systems director and a privacy officer at our site and we're with an Adventist Health corporate office. We have a screening process for new applications and new equipment. We've rolled out the smart pumps. I'm not convinced, however, that they are totally secure. Every time a physician wants to have a new piece of equipment that has protected health information in it, we look at how secure and safe it is from the privacy side as well as from the cybersecurity side.

MODERATOR: How do you identify vulnerabilities in medical devices across your organization and how are you closing those gaps? Nancy, are there manual overrides on these smart pumps?

DREWS: Yes, but the problem is that nurses are used to things running. We have a good downtime process in place, but it's not perfect. We set up a command center if something occurs that's unplanned. The clinical information staff will round and support the nurses on the floor. You have to be prepared and you need to know what to do to take care of your patients.

CANFIELD: Nancy, as a seasoned nurse, you know how to figure things out and you know when something doesn't look or seem right. In today's busy and stressful hospital work environment, nurses don't always have that kind of situational awareness. There's a huge expectation that technology is going to work correctly. And if a pump malfunctions or a monitor starts reading poorly, nurses' first assumption is that it may be human error or that something else is going on rather than the hardware actually malfunctioning or being controlled by a malicious party. Those are real risks, and I don't know how you alert staff to this reality.

GEORGE REED *(WakeMed Health & Hospitals):* Our emergency preparedness team at WakeMed pulled together all network devices, and we sat with the emergency response team and identified what actions would happen if we were attacked. What would have to go to manual operation and what would be the downtime procedures? We assumed it would be an hourlong discussion, but it ended up taking months of work to develop this plan. Clinicians often become used to things going a certain way, and when they don't, they will develop a workaround. So, we wanted to make sure everybody had a clear understanding of what had to be done.

For example, we had a power outage, but this did not impact the patient monitors, or central stations; all were functional. What we did not notice was damage to a router that prevented patient data flow to Epic for hours. Through that experience, we learned that vulnerabilities do not always present themselves initially and to check the operation of equipment at each location, as well as data flow to Epic and other applications.

> **"In our onboarding process, we'll ask the vendors for certain criteria to be part of our network; it's similar to a high-level risk assessment. But once the devices are onboarded, then it falls to the vulnerability team for penetration testing to assess the risk of these devices."**
>
> — Will Landymore —
> NewYork-Presbyterian Hospital

MODERATOR: What remediation-management processes do you activate once vulnerabilities are identified?

LANDYMORE: It's mostly the vulnerability scanning that happens two weeks or more for all devices. These days, we reach out to the system owners by showing them what has to be done to remediate the problem.

REED: From a clinical engineering perspective, vulnerability scanning is new. It's not something we're used to doing, but it's coming into play. There are companies that are starting to move to the forefront of helping clinical engineers look at this more, but part of the challenge is that we're still trying to figure out how to work with our information security counterparts.

RICHARD MEEKS *(Evergreen Health):* I'm the chief compliance officer at Evergreen Health. Most of our work has involved the FBI alerts — reviewing them and working with the owners of those systems to make sure those vulnerabilities don't exist. I find that a lot of the system operators don't feel empowered to act on the alerts. We end up having calls with the owner, the operator and then information security to come up with a plan to remediate those vulnerabilities. I also serve as the information security officer and ensure that those vulnerabilities actually are mitigated and don't fall by the wayside.

> "If you don't play at the board level and reported cyber vulnerabilities like infection rates, it's not going to get the same attention."
>
> — David Franklin —
> Philips

FRANKLIN: Richard, when you mentioned remediation management, that seems to be one of the biggest challenges that hospitals face. Vulnerabilities exist and they're delegated to individuals in the hospital at different levels. Then the challenge becomes tracking what actions are taken, and what actions remain unaddressed. My analogy is like a nosocomial infection. If you do everything up front, then you're not going to have a nosocomial infection, but you still measure it. You hope it's zero. If you incur no infections, it's because preventive action was taken. I like to talk about cybersecurity in terms of cyber health metrics and suggest that hospital leaders report their cyber posture to the board monthly.

MEEKS: Regarding remediation, one of our tactics is using the vulnerability software to report the number of vulnerabilities we've identified to our board compliance committee. Once that was reported and IT understood that it was being reported, we saw more remediation work being done, because it is a part of a performance scorecard.

FRANKLIN: We're seeing that more and more, and that's what I'm advising: 'If you don't play at the board level and report cyber vulnerabilities like infection rates, it's not going to get the same attention.'

MODERATOR: What metrics do you use to assess vulnerabilities, measure their risk impact and prioritize the response to these risks? Who in your organization owns those metrics, who closes the loop on this issue and who is the point of contact?

MEEKS: A lot of the vulnerability-management software now assesses the risk impact and informs you which vulnerabilities are the greatest risk. This helps us prioritize the risks because we have limited resources and want to spend time in the right areas. Those risks are always changing based on the landscape and are being exploited by the cybercriminals, which change daily. Our IT department owns the metrics because it has the staff members who do the remediation. While it is not their responsibility, compliance has been trying to advocate for the software and the metrics.

We still have some departmental systems, and if the device has a vulnerability, the cost is the responsibility of whomever owns that device. If they don't have sufficient funds, we go up the chain of command to find those funds.

DREWS: From a corporate level, we were concerned about the increased cost of cyber liability insurance, which has hit us hard. What do we need to do so that our insurance costs aren't so high? We also looked at the IT spending of other large corporations. We learned that we lagged behind in our percentage of funding, so we allocated additional funds, because it is such a risk.

MODERATOR: How do you share the information with senior executives and your board and how do you translate cyber-risk into an enterprise risk issue, as a business risk issue and as a patient safety risk issue?

MARKS: For the last three and a half years, we have an independent agency do a HITRUST assessment, which is a board reportable goal for us. We set our cyber goals with the board of directors each year; it's not solely the responsibility of the CIO nor the compliance officer. It is a shared operational responsibility.

MODERATOR: You're right, Pete. Most boards understand it's a problem. But sometimes they're not certain how to act upon it or where to prioritize and focus their attention. And the point Nancy made about funding — health care is lagging behind other sectors in cybersecurity spend. Financial services will devote 10% to 15% of their IT budget toward information security. The norm in health care is about 3% to 7%. There are a number of reasons for the lag compared with other sectors. For instance, we in health care have fewer resources in general, and as a sector we are less mature in cybersecurity. We've only had digitization of our sensitive records for 10 to 15 years compared with U.S. financial services, which has been protecting data and securing electronic financial transactions since computers first appeared in banks more than 50 years ago.

MEEKS: We've used an internal audit as a mechanism to flag cybersecurity and IT as high risks of the organization. Through those audits, we've been able to accomplish a lot of work on initiatives that hadn't been funded previously because all our internal audit reports go to our board audit finance and compliance committee.

LANDYMORE: Reporting with more tangible proof helps with funding and for people to understand the risks. We'll download hundreds of thousands of samples of malware, and then test them against our next-generation antivirus programs to pinpoint any weaknesses or holes. We have cloud-based Splunk scorecards that we can show executives.

FRANKLIN: Cyber health is ongoing; it's not one and done. From an original equipment manufacturer's perspective, Philips wants to make sure that our customers have products that work. If the networks don't work, then we cannot help you deliver care. Philips wants to provide solutions that identify network vulnerabilities and then prioritize them. Prioritization becomes a challenge because it has both expense and time associated with it, and not every customer can figure out how to prioritize the vulnerabilities that are found. We're all in this cyberattack prevention together with Philips wanting to support our customers as much as possible to develop the best solution for health care organizations to achieve cyber health. ●

SPONSOR

PHILIPS

Philips is a leading health technology company focused on improving people's health and enabling better outcomes across the health continuum from healthy living and prevention, to diagnosis, treatment and home care. Guided and inspired by the purpose to improve 2.5 billion lives per year by 2030, Philips leverages advanced technology and deep clinical and consumer insights to deliver integrated solutions. Headquartered in the Netherlands, the company is a leader in diagnostic imaging, image-guided therapy, patient monitoring and health informatics, as well as in consumer health and home care.

FOR MORE INFORMATION, VISIT:
www.Philips.com/partnership

OR FOLLOW ON TWITTER, LINKEDIN,
YOUTUBE AND FACEBOOK:
#futuretogether