healthsystemCIO.com
helping CIOs improve healthcare

Medical Devices and "Blind Spots": How True Visibility Can Change the Game

05/06/2021 By Kate Gamble

For healthcare organizations, medical device security is undoubtedly a priority. But with breaches continuing to mount, even during the pandemic according to HIPAA, perhaps it's not high enough on the list.


Theresa Meadows, SVP & CIO, Cook Children's Health Care System

In fact, Greg Murphy, CEO of Ordr, believes there's "a huge blind spot" when it comes to device security, and it stems from a lack of visibility as to what's on the network. "It sounds obvious, but you cannot define a security strategy, and you cannot understand your risks, if you don't know what's connected to your network," he said during a recent webinar.

The problem is that many IT and security leaders think they *do* know, and are unintentionally putting their organizations at risk. Fortunately, it's a scenario that can be avoided if the right steps are put into place, noted Murphy, who discussed this critical issue with Theresa Meadows (CIO, Cook Children's Health Care System), Todd Richardson (CIO, Aspirus) and Christopher Kuhl (CISO & CTO, Dayton Children's Hospital).

Know the risks

The first step, according to Meadows, is determining risk, something her team at Cook Children's does before any major project to help prioritize steps. And so, when they conducted an overall security risk assessment that uncovered high risks with medical devices, it raised several flags. "We felt it was important to know where all of our devices are, what versions of the software are running on those devices, what types of security programs we have in place," she noted. "It became clear that we needed to manage things better."

Greg Murphy, CEO, Ordr

Those findings aren't rare, according to Murphy, who revealed that many organizations are way off the mark when it comes to asset inventory. It's a safe bet that the configuration management database is going to be wrong — "it's just a question of how inaccurate it is," he noted, adding that some still use spreadsheets to track devices. And although no inventory system is going to be perfect, Ordr has identified "gaping holes" where some organizations could only reconcile 60 percent of its assets. "There are devices in the asset inventory that are nowhere to be found on the network, and there are devices we're seeing on the network that weren't in the inventory."

To say that's problematic is putting it mildly, said Murphy, who is encouraged that organizations like Cook Children's and Aspirus are taking steps in the right direction.

"We work very closely to identify risks," said Richardson, whose team conducts annual audits. "We know that it might expose something we may not necessarily be proud of, but if we don't know it's there, we're putting the organization in a far worse spot."

Taking ownership

One of the biggest challenges, he said, is determining which department owns medical device security.

At Dayton Children's, keeping a clean inventory is a shared responsibility in which the asset management team works with biomedical engineering and medical imaging to ensure "what we have is accurate for anything new coming in, as well as anything being decommissioned out of the organization," said Kuhl. Therefore, it was important for all of those groups to participate when they met with Ordr so they could "compare notes" before moving forward.

However, like many healthcare IT projects, what works for one organization may not work for another, according to Meadows. "It's a matter of how you structure a program." Whether the onus falls on clinical engineering or biotech, for example, depends on the maturity of the security program, as well as budget concerns.

One thing leaders want to avoid is a "hot potato" scenario in which accountability for asset management is either passed around from one department to another, or dropped, noted Richardson. What's most important is ensuring that whoever is in charge has a solid understanding of security and networking. "At the end of the day, it's not about who 'owns' it," he said. "But the buck has to stop somewhere, and it usually stops with IT security. We have the best knowledge and are best equipped to do it." And while biomed and clinical engineering certainly have responsibility for maintaining devices, the accountability rests on IT and security. "If it smells, looks, or sounds like anything related to IT, we get involved. Our information security officer has to review it."

Todd Richardson, SVP & CIO, Aspirus

“It’s a team sport”

And although that may be true for many organizations, other departments still need to be involved, as early as possible in the process, said Murphy. “It’s critical to bring others into the conversation,” and avoid mistakes like sending out a memo mandating that certain devices will be removed from the network if standards aren’t met.

“You need to make sure those discussion take place in advance, that people understand what’s happening, and that they have an opportunity to engage,” he noted. Not only can it help avoid bad blood, it can also help build buy-in.

Meadows concurred, adding, “We all need to appreciate and understand that this is a team sport. Clinical engineering is responsible for ensuring that the device is functioning appropriately, but the security team is responsible for ensuring that device — and the rest of the organization — is protected,” she said. “Everyone has their responsibilities.”

It isn’t always easy, said Kuhl, but for information to be kept safe, teams have to “play nicely together in the sandbox.” By inviting multiple teams to the table, leaders can prevent adversarial relationships from developing and ensure it’s a collaborative effort.

Visibility up front

Finally, it’s essential that organizations build visibility into the budget, rather than waiting until a breach happens, at which point it’s too late, noted Richardson. “You have to do the reconnaissance. To put something in place without having visibility into it is reckless,” he said. When budgeting for an acquisition, he teams factors in what it will take to do the discovery and the migration, and to have an understanding of the process.

It’s a strategy that Murphy highly recommended. “The last thing you want to do is discover that your asset inventory is inaccurate when you have a breach,” he noted. “The cost of not having that asset inventory can be extraordinarily high.” By obtaining a detailed and granular understanding of what’s in place, organizations can take the next steps.

And of course, it’s important to realize that this “isn’t a short-term problem,” he added. “You have to get visibility. Only when you have that can you start putting plans in place to improve. And that’s a journey and a path you’ll be on for the months and years to come.”

To view the archive of this webinar — Unlocking Medical Device Value With Visibility, Security and Automation (Sponsored by Ordr), please click here.