Med-tech trade group launches online cybersecurity tool

March 15 2019, by Joe Carlson

Credit: CC0 Public Domain

Cybersecurity events like 2016's NotPetya ransomware attack tend to arrive in bursts of confusion and concern, but the hard work of mitigating cybersecurity risks in health care technology is embedded in the daily grind of the medical technology industry, insiders say.

The Food and Drug Administration requires medical device companies

to plan for cybersecurity at the earliest stages of design, and to monitor for new vulnerabilities long after devices have been shipped to customers. But industry insiders say companies are uneven in their abilities and willingness to address the issue and talk about it openly, which can hinder progress.

Now the Washington-based medical technology trade group AdvaMed is creating a new communication tool for med-tech companies known as an "information sharing and analysis organization," or ISAO (pronounced "I-sow") that will allow technical-minded med-tech experts to trade tips and analysis of ongoing problems.

News of the ISAO's impending creation comes as the FDA is finalizing an update to its five-year-old guidance on the things that device makers need to do on the cybersecurity front before asking for permission to market their devices in the U.S.

Known as the "premarket" submission guidance, the 24-page draft of the new rules spells out specific tasks and goals, like working to prevent unauthorized access and protect sensitive data. (Public comments on the guidance before it's finalized are due on Monday.)

"These documents ... don't merely convey 'guidance' that a manufacturer may choose to follow," Zach Rothstein, vice president of technology and regulatory affairs at AdvaMed, said in a conference call with reporters Thursday. "A manufacturer cannot choose to ignore the documents. If they were to do so, FDA would likely not review the premarket submission, or in the post-market setting FDA could take enforcement action."

Participating in an ISAO is one way a med-tech company can show regulators and the public that it is serious about cybersecurity.

The FDA's post-market cybersecurity guidance, enacted in 2016, says manufacturers should fix uncontrolled cybersecurity vulnerabilities as quickly as possible, and report them to the FDA. However, if the manufacturer remediates the problem, discloses it to its ISAO, and the vulnerability has not led to death or serious health problems, then the company can avoid reporting the problem to the FDA, under the 2016 rules.

Rothstein said the AdvaMed ISAO will be like a regular online forum, except it will have strong security and its users will be restricted to experts in cybersecurity who've agreed to not share confidential information outside the forum.

The group will help experts compare notes in real time. But it will also serve an important function for smaller companies who may have a hard time affording the cybersecurity competence they need.

"It's probably no surprise to hear that the smaller the med-device company, the harder it is for them to hire, retain and pay for cybersecurity expertise," Rothstein said. "Part of what we are using the ISAO to do is to provide that type of education (for) our midsize, smaller-sized companies."

©2019 Star Tribune (Minneapolis)
Distributed by Tribune Content Agency, LLC.