Cybersecurity experts gather to try to prevent future attacks like WannaCry

20 May 2017, by Joe Carlson, Star Tribune (Minneapolis)

An entire team of experts works at the Mayo Clinic to ensure that 25,000 networked medical devices - everything from digital cameras to proton beam therapy systems - are hardened against cyberattacks like the WannaCry worm that affected hospitals from England to China last week.

It's no easy job, but - knock on wood - there have been no reported successful cyberattacks or malicious outsiders hacking Mayo's systems. Still, the WannaCry worm has infected at least some medical devices in the U.S., and well-funded hospitals like the Mayo Clinic may not be the first medical centers where successful hacking would crop up.

Rather, the public ought to think about the more than 600 financially struggling hospitals in smaller communities that are on the verge of closure. "Those are the people that we need to keep in mind for medical devices, not Mayo," said Kevin McDonald, Mayo's director of clinical information security.

"It costs a ton of money to be able to do this," he said. "Medical devices have now become the weakest link in your enterprise security defenses."

McDonald spoke Thursday morning in Silver Spring, Md., on the first day of the Food and Drug Administration's latest public forum on cybersecurity and medical devices. The two-day event is called "Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis," and is intended to produce a document that will identify potential "gaps" in regulation, product design and basic research in med-tech cybersecurity.

Unlike the previous meetings on med-tech cyber precautions, this week's workshop takes place against the backdrop of a worldwide cyberattack that has affected hundreds of thousands of computers and put government agencies on high alert for another wave.

The so-called WannaCry worm is based on a security vulnerability in older versions of Microsoft Windows, which is still run on many medical devices today. The Windows flaw was discovered by the National Security Agency years ago, and publicized recently after hackers got ahold of the NSA files. The worm is a form of "ransomware" that infects computers and computer networks, locking down critical files until the victim agrees to pay a ransom.

"A few years ago the biggest problem was the breach," which would allow a hacker to steal patient data and sell it on the black market for a profit. "What's really scary is now they've figured out how to monetize the attacks directly," said workshop speaker Todd Carpenter, chief engineer at Minneapolis' Adventium Labs.

No U.S. hospital has yet publicly acknowledged being affected by the WannaCry worm. Nonprofit health care information-security organization Hitrust Alliance said it had seen evidence that devices made by Siemens and Bayer's MedRad subsidiary, along with other unnamed device makers, have been affected by the worm since the news broke last Friday morning that WannaCry had crippled dozens of hospitals in the United Kingdom.

Thursday's FDA meeting was part of the long-running effort in the U.S. to not just raise the profile of med-tech cybersecurity as an issue, but to break through the logjams that have stood in the way of progress. One key question is how to pay for it all.

"Health care institutions do not have the time, money or resources to independently fix the problems," said one of McDonald's slides, under the title "Assumptions We Need to Make." "The costs and effort for securing devices should not, and cannot, be the full responsibility of hospitals."

The Star Tribune reported earlier this week that Hennepin County Medical Center will need to

spend $200,000 to address vulnerabilities raised by WannaCry in a single machine.

But the problem of cybersecurity vulnerabilities in medical devices is much deeper than figuring out who's going to write these large checks.

Ken Hoyme, director of security for product and engineering systems at Boston Scientific, said hospitals sometimes buy expensive equipment whose service life doesn't take into account how long the underlying operating system will be current.

"There is this willingness to accept a device with an expiring operating system, when the buyer knows for certain that they are going to use it for 20 years," Hoyme said at the workshop. "There are certainly research needs for something that would fill that niche (for a durable OS) in a way that is cost-effective and long-term supportable."