MEDTECH INSIGHT
CITELINE COMMERCIAL

17 Jun 2022 | **Analysis**

The Pace Of Cyberattacks Is Accelerating. Can Regulators Keep Up?

by Brian Bossetta

Cybersecurity expert Scott Trevino tells *Medtech Insight* that a major challenge US regulators must confront in securing medical devices and hospitals is playing offense, not defense, against hackers who are becoming increasingly brazen and sophisticated in their ability to shut down systems and steal valuable data.

As cyberattacks across the US health care sector increase, regulators face the daunting challenge of staying out in front of the rapidly growing threat. That's because falling behind can be catastrophic, says Scott Trevino, senior VP of cybersecurity at Indianapolis-based clinical asset management company TRIMEDX.

Hospitals are one of the most targeted segments of the nation's critical infrastructure, Trevino told *Medtech Insight*, adding that breaches on hospital systems have gone up significantly over the last few years and there's no sign of them abating.

But what does a cyberattack on a hospital look like?

Unlike a physical attack, the fallout from a cyberattack is invisible, but that doesn't mean it can't be destructive and result in loss of life.

As Trevino pointed out, a cyberattack on a hospital could delay service or treatment to a patient. And while that might just result in the inconvenience of having to reschedule a procedure – it could also mean putting off that procedure for many months or perhaps indefinitely.

And in some cases, waiting to have surgery or a diagnostic exam could result in a drastically worse outcome for the patient.

Trevino also painted a potential worst-case scenario for a patient being transported in an

ambulance to an ER that's been attacked: "If you need to get to a level one trauma center and have to be rerouted to another facility because of a ransomware attack, that can mean life or death. Minutes count here."

Data

But perhaps the most immediate risk, Trevino said, is to data and personal health records, such as the April attack on Kaiser Permanente and Yuma Regional Medical Center in Arizona, in which the medical records of some 70,000 patients might have been stolen by hackers who were able to access the hospital's emails.

Shields Health Care Group in New England also reported a potential breach on the data of 2 million patients, which the company said was discovered in March.

And the US Cybersecurity and Infrastructure Agency (CISA), which is part of Homeland Security, recently issued a cybersecurity alert to Illumina software.

> *"With cybersecurity, it's always been a catch-up kind of approach."*
> *– Scott Trevino*

"Successful exploitation of these vulnerabilities may allow an unauthenticated malicious actor to take control of the affected product remotely and take any action at the operating system level," the CISA warns in its alert. "An attacker could impact settings, configurations, software or data on the affected product, and interact through the affected product with the connected network."

And in 2021, the Department of Health and Human Services reported data breaches from 578 health care organizations, impacting 41 million individuals. The HHS also cited the *HIPAA Journal*'s 2020 Healthcare Data Breach Report, which says the health care industry in 2020 had the third-largest number of data breaches on record since 2009.

These attacks, Trevino said, not only expose one's personal health data, but Social Security numbers and all the information needed to steal an identity and other sensitive information that could have enormous reputational and personal implications.

So what is being done to stop this threat?

FDA Response

The Food and Drug Administration in April issued its much anticipated guidance on medical device cybersecurity, replacing the agency's 2018 guidance with a document, in Trevino's view, that better addresses the emerging and dynamic cybersecurity threat.

Though by no means a panacea, Trevino said the latest guidance "is encouraging and a step in the right direction," and puts the government in a better position to get ahead of hackers, which is crucial considering how quickly technology is evolving and that attacks are not only increasing in frequency but doing so at a speed that's often faster than that of regulators.

"With cybersecurity it's always been a catch-up kind of approach," Trevino said.

Suzanne Schwartz, director of the Office of Strategic Partnerships and Technology Innovation within the FDA's device center, told *Medtech Insight* in April that the latest guidance reflects an evolution in the agency's thinking and its ability to adapt to the changing cyber landscape. (Also see "*FDA's Schwartz Says New Draft Cybersecurity Guidance Addresses Emerging Threats*" - Medtech Insight, 12 Apr, 2022.)

For example, the guidance asks manufacturers to consider cybersecurity as essential to the FDA's Quality System Regulation – which requires device makers to establish and maintain procedures for validating a device's design – and recommends that firms establish a Secure Product Development Framework to reduce the number and severity of product vulnerabilities to better hit QSR benchmarks.

Further, the Software Bill of Materials can help manage risks to supply chains and monitor software used in devices, which is becoming more prevalent. The SBOM can also mitigate cybersecurity vulnerabilities throughout the software stack and includes components developed by a third party, such as a company that makes software to support another firm's device or system – a "critical aspect" of the guidance, according to Schwartz.

> ***"Health centers save lives and hold a lot of sensitive, personal information. This makes them a prime target for cyberattacks." – Bill Cassidy***

One area that falls short, in Trevino's view, however, is remediation. "There's no requirement to provide access to remediations or to provide them in a timely manner. And that points to some of the challenges today," he said, adding the current requirements for manufacturers to monitor

their devices for safety problems in the postmarket space are basically the same as those for product recalls or other safety issues.

“But the reality is, most cybersecurity issues do not rise to the level of required remediations,” Trevino said.

Industry’s Part

But the onus to advance cybersecurity and patient safety in general is not just on government. Industry also has a central role to play.

For example, TRIMEDX, Trevino said, is a founder member and current active member in the Alliance for Quality Medical Device Servicing and the Medical Device Servicing Community, and an active member of the Association for the Advancement of Medical Instrumentation.

“We also actively engage with FDA and other government agencies, legislators and industry organizations on various topics, activities and initiatives,” he said, adding that industry participation is another significant step individual companies can take to advance patient safety and security.

Legislation

Along with the FDA’s current initiatives, Trevino said he’s also optimistic about the bipartisan effort to address cybersecurity on the Hill.

For example, the US House of Representatives on June 8 approved a bill requiring the FDA to ensure cybersecurity throughout the life cycle of medical devices and that manufacturers meet minimum cybersecurity requirements set by the agency.

The legislation, sponsored by Rep. Anna Eshoo, D-CA, passed with overwhelming support from both sides of the aisle in a 392-28 vote.

And Sens. Todd Young, R-IN, and Jacky Rosen, D-NV, introduced the Strengthening Cybersecurity for Medical Devices Act, which would require the FDA to review and update medical device cybersecurity guidelines and offer suggestions to ensure devices are protected from possible hacks.

“Medical devices are increasingly connected to the internet or other health care facility networks to provide features that improve the ability of health care providers to treat patients,” Young said in press release.

And in March, Rosen, along with Sen. Bill Cassidy, R-LA, introduced the “Healthcare Cybersecurity Act,” which, according to a release from Cassidy’s office, would direct the CISA

and the HHS to collaborate on how to improve cybersecurity measures in hospitals and other facilities, and would authorize training to health care personnel on cybersecurity risks and ways to mitigate them.

“Health centers save lives and hold a lot of sensitive, personal information. This makes them a prime target for cyberattacks,” Cassidy said.

Then there’s the pending Protecting and Transforming Cyber Health Care (PATCH) Act, introduced in April by Cassidy and fellow senator Tammy Baldwin, D-WI, which would make the FDA the final authority on device cybersecurity and aims to ensure the security of devices before they go to market. Companion legislation to the PATCH Act has been introduced in the House by Reps. Michael Burgess, R-TX, and Angie Craig, D-MN.

Though glad to see lawmakers act, Trevino said he would like for them to be quicker about it.

“The urgency needs to be there based on all the trends we’re seeing daily in the news,” he said. “Because it pertains to the safety for patients, our hospitals, and the health system as a whole.”