MEDTECH INSIGHT
CITELINE COMMERCIAL

16 Jul 2019 | **News**

Siemens Cybersecurity Expert Says Medtech Industry Has 'Perverse Incentive' To Not Disclose Vulnerabilities – Might A New Law Be The Fix?

by Shawn M. Schmitt

The fear of losing business by being transparent about cybersecurity vulnerabilities means there's "a perverse incentive in some parts of the market that encourages a lack of disclosure," Siemens' Harrison Wadsworth says. But the US FDA's Suzanne Schwartz believes coordinated vulnerability disclosure legislation could "level the playing field."

A few years ago, *Siemens AG*'s Harrison Wadsworth was in the office of his company's product security officer when a customer phone call was patched through.

"The person said: 'How come I keep getting product security bulletins from Siemens about all your security problems when this other vendor we work with has no problems?'" recalled Wadsworth, who is Siemens' director of government affairs, and the firm's cybersecurity expert.

"That's when our product security officer said: 'Well, actually, they do have problems. They're just not telling you,'" he said at a June *Case for Quality* forum in Arlington, VA.

Wadsworth said the customer was so concerned about Siemens' cybersecurity disclosures that they were considering switching to a different vendor.

That fear of losing business by being transparent about cybersecurity vulnerabilities means there's "a perverse incentive in some parts of the market that encourages a lack of disclosure," Wadsworth said.

> *"We may be looking to require coordinated vulnerability disclosure through legislation in order to level the playing field." – Suzanne Schwartz*

That's why the US Food and Drug Administration's Suzanne Schwartz says a new law might be the antidote to companies that willingly hide cybersecurity vulnerabilities to avoid concerning their customers.

"We certainly want to see much broader adoption of coordinated vulnerability disclosure across the entire ecosystem," Schwartz, deputy director of the Center for Devices and Radiological Health's Office of Strategic Partnerships and Technology Innovation, said at the forum.

Coordinated vulnerability disclosure is a process wherein product-makers work with cybersecurity researchers to find vulnerabilities in any software-based product – including medical devices – followed by designing a patch to fix the gap, and then distributing and deploying the patch. (Also see "*FDA Cybersecurity Forum: Manufacturers Explain Coordinated Vulnerability Disclosures* " - Medtech Insight, 1 Feb, 2019.)

There's so much concern at the FDA about a lack of disclosure in industry that "we may be looking to require coordinated vulnerability disclosure through legislation in order to level the playing field," Schwartz said.

After all, "the companies that are demonstrating the kind of behavior that is a role model for all the ecosystem shouldn't take a hit because of their transparency and the maturity that they are demonstrating – while all the other [firms] that do have vulnerabilities and are not disclosing them" go unnoticed, she added.

> *"There's a risk, if fear takes over, that people will become afraid to connect their devices." – Harrison Wadsworth*

Schwartz noted that a *2016 FDA guidance document*, "Postmarket Management of Cybersecurity in Medical Devices," "calls out strong recommendations and encouragement of coordinated

disclosure policies and processes to be adopted through industry, and we recognize the international standards that are specific to those."

In October 2018, a US congressional panel encouraged federal government agencies and private companies to embrace coordinated vulnerability disclosures, pointing to the disclosure advice in the FDA's cybersecurity guidance as a model that could work. (Also see "*US Lawmakers Praise FDA Tips On Coordinated Vulnerability Programs For Device Cybersecurity* " - Medtech Insight, 25 Oct, 2018.)

When it comes to cybersecurity and transparency, "the stakes are really high in safety-critical industries," Schwartz said. "Particularly, think about those patients with implanted devices or devices at home that they rely on for critical life functions, and what it's like to find out that information has not been disclosed in a coordinated manner. It creates a lot of fear, a lot of concern, a lot of anxiety and a lot of hysteria."

Added Siemens' Wadsworth: "There's a risk, if fear takes over, that people will become afraid to connect their devices [and will develop] an overall lack of trust in connected technology and innovation.

"That's the real risk."