MEDTECH INSIGHT
CITELINE COMMERCIAL

21 Nov 2022 | **Interviews**

Exec Chat: Cybersecurity Regulations Aren't Burdensome But 'Best Practice'

by Hannah Daniel

Impero senior vice president of products Sam Heiney spoke to *Medtech Insight* about reframing the way medtech and healthcare organizations think about cybersecurity regulations.

Healthcare organizations have struggled with cybersecurity more and more since the beginning of the pandemic, but regulations to protect them from such attacks have been few and far between.

Exceptions include the PATCH Act, which was introduced in the Senate in March, and a recently announcement from the Biden Administration that healthcare cybersecurity guidance should be coming out in the near future. (Also see "*As Cyberattacks On Hospitals Rise, Medical Devices Are Particularly Vulnerable*" - Medtech Insight, 16 Aug, 2022.).

The PATCH Act would provide protection against ransomware attacks, which have hit 82% of hospitals since March 2020. (Also see "*Senators Question User Fee Hike In Committee Hearing*" - Medtech Insight, 5 Apr, 2022.)

Medtech Insight spoke to Sam Heiney, senior vice president of products at Impero Solutions Ltd., about his role providing remote access tools to healthcare organizations to prevent cybersecurity threats. He gave a software company's perspective on cybersecurity legislation for healthcare and medtech organizations.

Q **Medtech Insight: What do you do at Impero?**

A Sam Heiney: I'm the senior vice president of products for Imperial and we are a global technology software manufacturing company that produces secure remote access tools for industry, educational technology, for the [educational technology] sector,

and web filtering and secure internet gateways for all sectors. I come from the position of a product manager and working principally with the secure remote access tool, which is where my background lies.

Q How do healthcare organizations use remote access tools?

SAM HEINEY, SENIOR VICE PRESIDENT OF PRODUCTS AT IMPERO

A Heiney: If you have a help desk or a service desk, [or] if you have a piece of equipment that needs to be monitored, patched, improved, supported, you'll likely use a remote access tool. I think that the ability to monitor network traffic, filter inappropriate websites, isolate browsers, and just kind of the whole concept of a secure internet gateway is getting increasing traction, again, horizontally across all verticals. We anticipate that we'll have more and more interest from our healthcare providers for those products.

Q It seems like a point of interest across industries right now—being able to have a handle on what people are able to see, especially in such sensitive environments like health care.

A Heiney: When you look at modalities of [cyberattacks], people are always where you go, right? That's why spear phishing and phishing attacks are so successful. The weak link is often that people aren't trained. If you can augment that training with tools that isolate their browser activity that prevent them from looking at malicious websites that literally prevent malware before it even gets to the user, then you've gone a long way towards introducing more defense in depth, improving your security posture and protecting your devices, your network, and your people.

Q Turning to regulations, what are your reactions to some of the legislation

coming from Congress and the White House?

A Heiney: We've been tracking and are supporters of the PATCH act, and I know that in terms of industry, there have been some mixed feelings about that. I personally believe that that is a good piece of legislation and I'm supportive of it.

Q **What kind of reactions?**

A Heiney: I think the general impression that I get is one of people being in favor. … The American Hospital Association [and] a variety of large organizations have already come out in favor of the PATCH act. As a software vendor, I can tell you that regulations can be burdensome, and whenever you mandate that something change, you have to invest in change management, you have to then go understand what's going to be needed. You have to change your processes to do that, and there's cost involved in that, so whenever a new regulation comes down it it's a little scary. When we talk about cybersecurity, however, and the just sheer necessity of making these changes, most of my colleagues and peers recognize that what the PATCH Act is trying to accomplish is best practice. Trying to adopt those can be a little painful, but I think most organizations recognize the need for that and are acting appropriately.

Q **What are you looking for from the government to help manage cybersecurity threats?**

A Heiney: The one thing that I always try and reinforce with my customers with my colleagues, my peers, my employees, is that cybersecurity is so valuable and important. When looking at regulations … There's often that fear and burden of regulatory compliance, but cybersecurity is patient safety. Cybersecurity is his healthcare safety, and it really deserves our attention. So, even if we get it wrong with that regulation, moving forward with something is a good idea. We have to do more. I think that's the message I always want to make sure that I get across—We need to do better.