Staying Ahead of 'Enormous and Evolving' Cyberthreats Requires End-to-End Collaboration

As a newly appointed member of the AAMI Board of Directors, you have mentioned how your work with MITA, H-ISAC, and AdvaMed can be leveraged to increase awareness of the vision and mission AAMI across a broader constituency in the healthcare domain. From your unique vantage point, what are some ways in which you these organizations can benefit by synchronizing their efforts?

Great examples of how best to leverage the synchronization of organizations often are found within standards consensus. As a member of multiple industry forums on standards, I have the ability to bring common topics and information to these various groups in improving communication horizontally.

In addition, organizational collaboration and synchronization are very helpful when attacking common challenges in need of standardization, such as our communication vehicles (e.g., the MDS2 [Manufacturer Disclosure Statement for Medical Device Security] form and the need to standardize the information inquiry in order to be both comprehensive and effective).

Standardizing a common software bill of materials (SBoM) also is needed. We need to be holistic in our approach to standards and organizationally collaborative across the end-to-end ecosystem. Synchronization and collaboration across organizations will further our mutual goal to strengthen the industry.

At this point, the dangers surrounding cyberthreats are well known, with the ECRI Institute ranking “Ransomware and Other Cybersecurity Threats” as its number one health technology hazard of 2018. What are the most urgent best practices and solutions that need to be implemented to combat this sharply escalating threat landscape?

From my perspective, members of the healthcare ecosystem need to apply best practices to inventory their assets, and that goes beyond the physical to include SBoM. Absent best practice inventory management, defining the threat landscape or establishing the defense, maintenance, mitigation, and remediation necessary to provide comprehensive cybersecurity is not possible. Again, we are a community that needs to be working together on these threats, as I had mentioned in my Oct. 4 opinion piece for the Morning Consult.

I would go further to recommend the development of a comprehensive coordinated vulnerability disclosure program, as well as to reassure customers and consumers that proper procedure and efforts are consistently applied to the repair of all vulnerabilities and prevention of future damage.

What’s one cutting-edge advancement in technology that shows promise in bolstering healthcare cybersecurity?

We see lots of promise within blockchain technology for opportunities (e.g., Keyless Signature Infrastructure) to augment traditional deployment solutions (e.g., Public Key Infrastructure) and reduce the risks of surveillance. A blockchain-decentralized network can definitely play a role in securing sensitive medical data, both at rest and in transit. Blockchain also has the potential to help us reduce human factor vulnerabilities and the risks of single points of failure.

What practical approaches should healthcare technology management professionals be implementing to protect medical devices from cyberthreats?

Identifying your end-to-end inventory assets is at the top of the list. This is foundational. With the defined inventory in hand, we as a community, both manufacturers and healthcare delivery organizations (HDOs), can then tackle the challenges of purging the end-to-end environment of legacy devices that represent enormous vulnerabilities.
You used the term "security ninjas." in a presentation you gave in 2016. What are security ninjas, and how do they factor into the landscape or medical device security?

Security ninjas are our own internal “white hat” hackers. Within our Security Center of Excellence, we have teams of talented cybersecurity professionals dedicated to hardening our products and services via both static and dynamic testing. As a manufacturer, we also fully embrace the external community of researchers. This embrace of external white hats or security ninjas is an important part of a holistic cybersecurity program, in that no one entity in isolation will be able to secure the environment against the evolving threat landscape. It will take the entire community working toward the same results for safety, security, and privacy.

You have asked, "How many believe that responsible 'coordinated' disclosure is a contact sport?" Can you please explain this? In what ways does the culture of disclosure need to change?

My contact sport metaphor relates to seeing some within the community of health technology manufacturers and HDOs taking a defensive posture with researchers. This is based on the incidental frictions that are part of that interactive relationship.

We all need to be open and transparent, recognizing and embracing the importance of external challenges to the security of our products and services; otherwise, we will be vulnerable and put our customers, consumers, and patients at risk.

Researches are our allies in arms against a common enemy; we must embrace their contributions, in order to reinforce our capacity to build a secure medical infrastructure that can deliver safe and affordable healthcare.

As mentioned previously, no one entity in isolation will be able to secure the environment against the evolving threat landscape. If any one player believes they can compete on the “security” of their own offering, they are sadly mistaken.

Cybersecurity threat and defense requires comprehensive transparency and clear communication across the end-to-end ecosystem. Any one device maker or healthcare facility can bring down all systems within and adjacent to its own enterprise business processes for suppliers, shipping, records management, etc. We also need open and honest communication with our regulators and security professionals to establish the capacity to defend against a landscape of perpetrators ranging from "attic room" hackers to organized crime and even nation-states.

The challenges ahead are enormous and evolving; to stay in front, we are dependent on the collaborative cooperation of all—throughout the end-to-end ecosystem.

Any closing thoughts?

I would just like to add my appreciation for the vote of confidence reflected in my recent election to the AAMI Board of Directors. I look forward to contributing, specifically regarding the cybersecurity issues facing the industry and to the more than 50-year legacy of the association’s impact on the development, management, and use of safe and effective health technology.

References

