Cybersecurity Standards Are Standing Up to the Bad Actors

Wil Vargas

It seems like every day there are news reports of a data breach in another industry: banking, retail, government, medical—wait, medical? How can that be? Bad actors, as they are called, have decided that that nothing is sacred, not even when it may harm people in need of care. Healthcare delivery organizations (HDOs) and their devices are at risk just like every other sector and electronic consumer product. That's a rather terrifying thought.

AAMI's Device Security Standards Working Group was established in 2013 to develop standards and technical reports on device security as it relates to the producers of medical devices. That's not to say that manufacturers weren't making their devices secure. However, the industry needed a cohesive way to address the attack vectors being exploited by these bad actors. There had to be a better way.

The committee decided to look at device security as a risk management problem and got inspiration from two foundational documents regarding risk management: the standard ANSI/AAMI/ISO 14971, *Medical devices—Application of risk management to medical devices,* and National Institute of Standards and Technology SP 800-30, *Guide for Conduction Risk Assessments*. We asked, "What if we utilized the fundamental concepts of risk management established in 14971 and looked at it through a device security lens?" To make this effort useful, the output should be informative and not constitute another burdensome process. This guidance document should help a manufacturer incorporate device security measures through examples that can be folded into their existing 14971 processes.

Thus, AAMI TIR57, *Principles for medical device information security risk management* was born. Published in July 2016, this technical information report provides guidance on methods to perform security risk management for a connected medical device in the context of the safety risk management process required by 14971. TIR57 expands risk management found in 14971 by considering security in risk management and ANSI/AAMI/IEC 80001-1, *Application of risk management for IT Networks incorporating medical devices—Part 1: Roles, responsibilities and activities*, by incorporating the same key properties of safety, effectiveness, and data and systems security as well as providing examples of best practices.

The Food and Drug Administration (FDA) recognized TIR57 less than a month after its publication, and the TIR was quickly identified as a critical element for manufacturers in the journey to facilitate medical devices that are better able to address current security risks. Strong positive feedback on TIR57 from the industry inspired the Device Security Working Group to develop a companion standard.

In the standards development world, typically a standard is developed and then a guidance document follows to facilitate its use. In this case, we approached device security in reverse. That's because a TIR can be developed faster and the industry desperately needs solid guidance on the matter. This led to the initiation of AAMI SW96/Ed. 1, *Medical devices—*

About the Author

Wil Vargas is a director of standards at AAMI in Arlington, VA. Email: wvargas@aami.org

Application of security risk management to medical devices. The working group was approved to begin developing the standard in February 2017. SW96, scheduled for publication in 2020, will provide the required steps and processes expanded upon in the guidance of TIR57.

These documents won't completely solve the global challenge of protecting ourselves from every bad actor. But, as a collection, they represent the beginnings of a portfolio with solid and useful [cybersecurity] approaches.

In addition, the AAMI Device Security Working Group is developing a new guidance document, AAMI TIR97, *Principles for medical device security—Post-market security management for device manufacturers*. This TIR provides guidance for addressing postmarket security management within the risk management framework defined by 14971. TIR97 will apply to any healthcare product that requires postmarket management of security. In other words, where TIR57 helps a manufacturer develop a product with security in mind, TIR97 will provide guidance on how to address device security issues once the product is out in the field. TIR97 is expected to help manufacturers manage and process postmarket device security interactions internally and in association with the HDOs. It will also provide recommendations on methods to manage medical device software patching. TIR97 is scheduled for publication in 2019.

It's certainly an exciting time for the members of AAMI's Device Security Working Group. These documents won't completely solve the global challenge of protecting ourselves from every bad actor. But, as a collection, they represent the beginnings of a portfolio with solid and useful approaches to reducing the overall likelihood and severity of the cybersecurity threats that are troubling medical devices and affecting those that need medical care.

The AAMI Device Security Working Group values additional input from all parts of the medical device and healthcare industry. For more information regarding the committee's work or to join the committee, please contact me at **wvargas@aami.org**. ■

Available AAMI Device Security (and Related) Standards

- AAMI TIR57/Ed. 1, *Principles for medical device information security risk management*
- AAMI/ANSI/ISO 14971, *Medical devices—Application of risk management to medical devices*
- AAMI/ISO TIR24971/Ed.2, *Medical devices—Guidance on the application of ISO 14971*
- AAMI/IEC 80001-1, *Application of risk management for IT Networks incorporating medical devices—Part 1: Roles, responsibilities and activities*
- AAMI/IEC 80001-2-2, *Application of risk management for IT-networks incorporating medical devices—Part 2-2: Guidance for the communication of medical device security needs, risks and controls*
- AAMI/IEC TIR80001-2-8/Ed. 1, *Application of risk management for IT-networks incorporating medical devices—Part 2-8: Application guidance—Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*
- AAMI/IEC TIR80001-2-9/Ed. 1, *Application of risk management for IT networks incorporating medical devices—Part 2-9: Application guidance—Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities*

Standards are available for purchase at **www.aami.org/store**.

AAMI FOUNDATION

The AAMI Foundation thanks all of its industry partners for making the work of the Foundation possible!

DIAMOND

BD

Connexall®

icumedical human connections

Johnson & Johnson

Masimo

Medtronic Further, Together

PLATINUM

Baxter
B. Braun
GE Healthcare
Ivenix
Malinckrodt
Nihon Kohden
Philips
Smiths Medical

GOLD

Bernouilli
Cerner
Crothall
Draeger
EarlySense
Mindray
Sotera
Spacelabs
Vocera

BRONZE

Fresenius Kabi
Safen Medical Products
VitalSims
ZynoMedical