Coming to Grips With Cyber(in)security

To the uninitiated (i.e., myself—a recent addition to the AAMI staff), forays into the realm of cybersecurity can conjure up paranoiac-inducing ponderings of a soon-to-be future in which implantable technologies are compromised according to the fiendish pursuits of some nefarious malefactor. And perhaps more terrifying: These fears have merit. As Tim Gee, one of our roundtable participants (page 8), points out, although malicious hacks have not occurred “in the wild,” their feasibility has been demonstrated in laboratory settings by “white hat hackers.” Indeed, donning this “professionally evil”—a term used by Kevin Johnson during his interview (page 54)—cap, researchers have demonstrated the ability to hack into wireless, implantable devices, such as pacemakers and neurostimulators, and reprogram them in ways that could harm patients.

After we get beyond the allure of these science-fiction-cum-science-fact realities and delve into the articles presented here, we quickly realize that security experts and engineers, researchers, regulators, manufacturers, and healthcare professionals are facing equally pressing concerns grounded in the here and now. As Kevin Fu and James Blum point out in their article (page 38), “If you watch television crime dramas, you may be duped into thinking that hacking of medical devices is the number one risk for public health today. You would be wrong. The most pressing risks are much less sexy: the unavailability of patient care and the lack of health data integrity.”

This is where we find the cyber-rubber meeting the security road—with issues such as medical device standardization and interoperability. As Krishna Venkatasubramanian describes in his article (page 19), “Failure-free operation of interoperable medical devices can be viewed as satisfying both safety and security.” Researchers, he notes, are striving to design architectures that enable safe interoperability, leading to “better performance, reduced false alarms, automatic decision/diagnosis support, and medication interaction checking in real time.”

Clearly, as Anthony Coronado and Timothy Wong write (page 26), “Cybersecurity risk management is a huge responsibility.” Use of protected health information is an extremely sensitive area—one that is governed by HIPAA and the HITECH Act—and substantial fines have been levied on healthcare facilities failing to comply with the security and privacy requirements of the HITECH Act. The authors note the importance of devising a cybersecurity risk management plan, including clearly defining the distribution of cybersecurity duties among facility personnel, ensuring that devices have strong safety features and that the manufacturer will provide continuing support, and establishing a procedure for reporting cybersecurity events.

Further down in the nuts and bolts of cybersecurity, we find invaluable work being done by security engineers such as Steven Baker (page 42) and Jonathan Knudsen (page 48). Their articles deal with the crucial role played by fuzz testing (i.e., fuzzing) in the development and validation of software. As Knudsen points out, fuzz testing can reveal vulnerabilities that allow device manufacturers to “better understand their risk profile, determine the most effective course of action to manage the inherent risk, and bring that risk to a level that is acceptable to all stakeholders.”

As medical device technology continues its trend toward greater sophistication, the benefits to patient care also will grow exponentially, as will the threats to information, device and healthcare facility functionality, and potentially even to patient health. While our fears may be justified, as the articles presented in this issue of Horizons demonstrate, we’ve got too much work to do to get bogged down in them—work to improve collaboration and communication among stakeholders, work to achieve a standardized or best-practices approach to implementation of devices, and work to stay ahead of the mounting threats.
Get Involved
Shape the future of healthcare technology!

Spread the Word: Write for AAMI Publications or the AAMIBlog
E-mail AAMI at communications@aami.org to get started!

Be Heard: Participate in Standards Development
Visit www.aami.org/standards for more information!

Join the Conversation: Participate in AAMI’s Networking Communities.
See the full list of communities at www.aami.org/communities

Sharpen Your Skills: Register for an AAMI Training Session
Sign-up for an in-person training or webinar today at www.aami.org/meetings/courses

Find your Local Society: Network with Regional Peers
See the full list of regional biomedical societies at www.aami.org/communities/societies to connect with the one closest to you!

Not a member? Join AAMI Today!
Join your peers and move your healthcare technology career forward!
Visit www.aami.org/membership to join AAMI today.