Trends in Cardiovascular Medicine 29 (2019) 481–482

Contents lists available at ScienceDirect

Trends in Cardiovascular Medicine

journal homepage: www.elsevier.com/locate/tcm

Editorial commentary: Cybersecurity of cardiac implantable electronic devices – role of the clinician

David Slotwiner, MD

Weill Cornell Medicine, 56-45 Main Street, Flushing, NY 11355, United States

Computers and networking are now essential tools of health care. Health care providers have come to appreciate that medical devices are not immune to cybersecurity vulnerabilities. Clinicians are being required by circumstance to both understand their role in minimizing cybersecurity vulnerabilities and, for electrophysiologists, have had to advise patients on how to respond to cybersecurity vulnerabilities of implantable cardiovascular electronic devices (CIEDs) [1]. This is foreign and uncertain territory for most health care providers. As clinicians, we are trained to assess and advise patients about the potential risk and benefits associated with pharmaceuticals, surgical and invasive procedures, or medical device-based therapy such as CIED. Cybersecurity vulnerabilities are inherently different. Clinicians do not have the expertise to independently evaluate the evidence presented regarding a potential threat or even an understanding of which agencies are responsible for working with manufacturers to evaluate and substantiate potential cybersecurity vulnerability. Nevertheless, patients turn to their health care provider in times of uncertainty and expect us to be able to give informed guidance [2,3]. Therefore, physicians play a critical role in translating potential vulnerabilities to patients and working with them to develop patient-centered interventions to minimize risk. A first step in this process is understanding the infrastructure, processes and personnel in place to both evaluate and minimize cybersecurity threats.

In this issue of Trends in Cardiovascular Medicine, Alexander et al provide an overview of the 6 medical device cybersecurity vulnerabilities that have been identified to date and resulted in U.S. Food and Drug Administration (FDA) Safety Communications [4]. Four of the 6 vulnerabilities have been related to CIEDs, while the first 2 affected computerized anesthesia infusion pumps. Importantly, there are no reports of any patients being harmed by cybersecurity breach of any of these vulnerabilities. In their review, the authors explain each vulnerability with enough detail that a non-technical audience such as health care providers can appreciate the risks and put those risks in perspective. The first vulnerability claims were of St. Jude (now Abbot) pacemakers. In August 2016 the Investment Firm Muddy Waters LLC and the cybersecurity research firm MedSec (Miami, Florida) claimed to have identified 2 types of vulnerabilities in several models of St. Jude pacemakers: a "crash attack" that could disable communication with the pacemaker and alter the pacing rate; and a "battery drain" attack [5]. Alexander et al summarize the subsequent attempts by others to validate these claims and rightly point out that a person would need to be within a few feet of the pacemaker in order to execute the attack. In addition, simply by moving the pacemaker to a different place in the room, telemetry communication was reestablished, and evidence indicated no change in pacing rate had occurred [6]. Thus, the likelihood of the vulnerability being exploited was remote, and the consequences if it was exploited turned out to be minimal, with no clinical impact to the patient. More recently, in October 2018, Medtronic confirmed the existence of a cybersecurity vulnerability in their CareLink Programmers [7,8]. Cybersecurity researchers notified Medtronic that they had identified a vulnerability that could be exploited while the programmer was downloading software updates. The researchers were able to change the programmer settings during the download of the file. Once these settings are changed, the programmer could then affect a CIED's settings upon subsequent interrogation. Medtronic, in response, disabled access to the Software Deployment Network and now requires updates to be installed via a USB drive, eliminating the opportunity for exploiting the vulnerability.

It's important for clinicians to understand why Medtronic was able to announce a strategy to mitigate the risks of its cybersecurity vulnerability at the same time the vulnerability was made public as opposed to Abbott for whom there was a 1 year time lapse, from August 2016 when the Muddy Waters released its claim to August 2017 when Abbot confirmed the findings and released a firmware patch [9]. Most cybersecurity vulnerabilities are identified by cybersecurity researchers who then notify the manufacturer, Department of Homeland Security's National Cybersecurity and Communications Integration Center and the U.S. FDA [2]. This allows the manufacturer to validate the claim, develop a strategy to mitigate the risk, and work with the FDA for any necessary regulatory approvals. This process, known as coordinated disclosure, allows experts to work together and present a unified approach to the public once the claim has been validated and once a strategy to minimize the vulnerability has been agreed upon. When a potential vulnerability is announced directly to the public, as was the case with the Muddy Waters disclosure, there will unavoidably be a period of uncertainty and confusion as patients and health care providers wait for the manufacturer, the FDA and any other required expertise to evaluate the claim and develop a risk-mitigating strategy. Fortunately, most

E-mail address: djs2001@med.cornell.edu

https://doi.org/10.1016/j.tcm.2019.01.003

vulnerabilities are identified by cybersecurity researchers whose careers are built by responsibly disclosing their findings and working under the coordinated disclosure model. But there is no way to prevent individuals or groups from going straight to the public, causing fear and uncertainty. When this occurs, such as it did when Muddy Waters released its claim directly to the public in August 2016, patients and health care providers should consider potential ulterior motivating factors by the individual or group as they evaluate the claim and consider what approach to take.

We as health care providers serve a critical role in assisting patients not only in evaluating the alleged cybersecurity risk and mitigating strategy, but also putting in perspective the importance of the underlying device therapy for the individual patient given their underlying indication for the device. Other important factors to discuss include the potential consequences if the vulnerability is exploited, the technical feasibility of exploiting the vulnerability and any risks associated with software/firmware updates.

With enough time and resources, the security of almost any device can be compromised. Medical device manufacturers and regulatory agencies are now acutely aware of the potential risks and are implementing controls and design techniques to minimize vulnerabilities [10–13]. Ultimately, the health care field must reach a point at which occasional software security updates for medical devices are anticipated and expected by patients and clinicians and are considered standard of care. Together, these approaches will substantially reduce potential vulnerabilities and exponentially increase the difficulty required to exploit them. Health care providers will remain a crucial advisor to patients when concerns about a potential threat inevitably occurs. Understanding the infrastructure in place to minimize these risks and to evaluate potential vulnerabilities as they arise should minimize our fear of the unknown and allow us to give informed guidance to our patients.

References

[1] Kramer DB, Fu K. Cybersecurity concerns and medical devices: lessons from a pacemaker advisory. JAMA 2017;318(21):2077–8. doi:10.1001/jama.2017.15692.

[2] Slotwiner DJ, Deering TF, Fu K, Russo AM, Walsh MN, Van Hare GF. Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians—proceedings of the Heart Rhythm Society's Leadership Summit. Heart Rhythm 2018;15(7):e61–7. doi:10.1016/j.hrthm.2018.05.001.

[3] Baranchuk A, Refaat MM, Patton KK, Chung MK, Krishnan K, Kutyifa V, et al. Cybersecurity for cardiac implantable electronic devices. J. Am. Coll. Cardiol. 2018;71(11):24620. doi:10.1016/j.jacc.2018.01.023.

[4] Alexander B, Haseeb S, Baranchuk AM. Are implanted electronic devices hackable? Trends Cardiovasc Med. 2019 In Press https://www.sciencedirect.com/science/article/pii/S1050173818302597.

[5] Researcg MW, MW is Short St. Jude Medical (STJ:US) - Muddy Waters Research: @muddywatersre; 2016 [cited 2018 December 18]. Available from: http://d.muddywatersresearch.com/research/stj/mw-is-short-stj/.

[6] Ransford B, Kramer DB, Foo Kune D, Auto de Medeiros J, Yan C, Xu W, et al. Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. Pacing Clin. Electrophysiol. 2017;40(8):913–17.

[7] Health CfDaR. Safety communications - Cybersecurity Updates affecting medtronic implantable cardiac device Programmers: FDA safety communication [WebContent]. Center for Devices and Radiological Health; 2018. [cited 2018 December 19]. Available from: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm623184.htm.

[8] Medtronic. Security Bulletin CareLink 2090 Programmer and CareLing Encore 29901 Programmer 2018 [cited 2019 January 2]. Available from: https://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/REV-Medtronic-2090-Security-Bulletin_FNL.pdf.

[9] Health CfDaR. Safety communications - Firmware Update to address cybersecurity vulnerabilities identified in abbott's (formerly St. Jude Medical's) implantable cardiac Pacemakers: FDA safety communication [WebContent]. Center for Devices and Radiological Health; 2017. [cited 2018 December 18]. Available from: https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm573669.htm.

[10] AAMI TIR57: Principles for medical device security—Risk management - Products - Association for the Advancement of Medical Instrumentation 2019 [cited 2019 January 2]. Available from: http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729.

[11] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff; Availability 2018 [updated 2018-10-18; cited 2019 January 2]. Available from: https://www.federalregister.gov/documents/2018/10/18/2018-22697/content-of-premarket-submissions-for-management-of-cybersecurity-in-medical-devices-draft-guidance.

[12] Postmarket Management of Cybersecurity in Medical Devices 2016 [cited 2019 January 2]. Available from: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

[13] Health CfDaR. Digital health - Cybersecurity [webcontent]. Center for Devices and Radiological Health; 2018. [cited 2019 January 2]. Available from: https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm.