Cybersecurity Vulnerabilities of Cardiac Implantable Electronic Devices: Communication Strategies for Clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit

Endorsed by the Heart Rhythm Society Board of Trustees

David J. Slotwiner, MD, FHRS,[*,†] Thomas F. Deering, MD, FHRS, CCDS,[‡] Kevin Fu, PhD,[§]
Andrea M. Russo, MD, FHRS,[¶] Mary N. Walsh, MD, FACC,[||]
George F. Van Hare, MD, FHRS, CCDS, CEPS-PC[**]

From the [*]New York-Presbyterian Queens, New York, New York, [†]Cardiology Division, Weill Cornell Medical College, New York, New York, [‡]Arrhythmia Center, Piedmont Heart Institute, Atlanta, Georgia, [§]College of Engineering, University of Michigan, Ann Arbor, Michigan, [¶]Cooper Medical School of Rowan University, Camden, New Jersey, [||]St. Vincent Heart Center, Indianapolis, Indiana, and [**]Division of Pediatric Cardiology, Washington University in St. Louis School of Medicine, St. Louis, Missouri.

TABLE OF CONTENTS

Introduction

Computers, networking, and software have become essential tools for health care. Our daily lives increasingly depend on digital technology, and we are persistently bombarded by the need to secure the systems and data they generate and store from attack, damage, and unauthorized access. Cybersecurity vulnerabilities of cardiac implantable electronic devices (CIEDs) are no longer hypothetical. While no incident of a cybersecurity breach of a CIED implanted in a patient has been reported, and no patient is known to have been harmed to date by the exploitation of a vulnerability, the potential for such a scenario does exist. The public awareness of cybersecurity vulnerabilities in medical devices, particularly devices such as CIEDs on which a patient's life may depend and where the potential for reprogramming or rendering the device nonfunctional exists, is raising questions and fueling fears among patients and the clinical provider community. The Heart Rhythm Society (HRS) has identified a gap in clinician-patient communication about the appropriate balance of the risks of such a potential attack against the benefits of lifesaving medical devices. To address these communication gaps, HRS convened a 1-day summit in November 2017, in partnership with the U.S. Food and Drug Administration (FDA). The goal of the meeting was to develop patient-centered communication strategies for health care professionals, industry, and governmental agencies. Participants included patient representatives, subject matter experts, HRS and the American College of Cardiology leadership, representatives from the FDA, and the Federal Bureau of Investigation and leadership of 5 CIED manufacturers. This proceedings statement is based on the 4 communication themes that emerged from the discussion: when to notify patients, whom to notify, how to communicate with patients, and key elements to discuss with patients.

Landscape

The rapidly changing health care environment and global interconnectivity exposes information technology to increasing

KEYWORDS Cardiac resynchronization therapy; Cardiac implantable electronic device; Computer hacking; Cybersecurity; Implantable defibrillator; Remote monitoring; Shared decision making (Heart Rhythm 2018;■:e1–e6)

Address reprint requests and correspondence: Dr David J. Slotwiner, New York Presbyterian Queens, 56-45 Main Street, Flushing, NY 11355. E-mail address: djs2001@med.cornell.edu.

1547-5271/$-see front matter © 2018 Published by Elsevier Inc. on behalf of Heart Rhythm Society. https://doi.org/10.1016/j.hrthm.2018.05.001

Table 1 Common cybersecurity terminology

Terminology	Definition
Computer hacking	In the context of computer security, this term refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is outside the creator's original objectives.
Denial of service (DoS) attack	A cyberattack in which a threat actor seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. DoS is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[5]
Exploit	Software or a sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or electronic (usually computerized).[3]
Firmware	A specific class of computer software that provides the low-level control for the device's specific hardware. Firmware can either provide a standardized operating environment for the device's more complex software (allowing more hardware independence) or, for less complex devices, act as the device's complete operating system, performing all control, monitoring, and data manipulation functions.[6]
Ransomware attack	An attack utilizing a form of malware in which malicious software code effectively holds a user's computer hostage until a ransom fee is paid. Ransomware often infiltrates a personal computer as a computer worm or Trojan horse that takes advantage of open security vulnerabilities. Most ransomware attacks are the result of accessing an infected e-mail attachment or visiting hacked or malicious Web sites.[4]
Threat actor	An entity typically with malicious intent that is partially or wholly responsible for an incident that affects—or has the potential to affect—an organization's security or a device's security.[2]
Vulnerability	A weakness in computer software code that could be exploited by a threat actor (defined below) to perform unauthorized actions within a computer system.[1]

vulnerabilities. Individuals with nefarious intentions can leverage these vulnerabilities for monetary gain or for causing disruption. The public, regulatory agencies, the health care community, and manufacturers increasingly recognize the urgency of the challenge. By gaining unauthorized access to diagnostic or therapeutic medical equipment, hackers may cause a variety of problems (Table 1). These range from ransomware attacks to denial of service attacks, sensor malfunction, or degradation of device function. CIEDs could potentially be reprogrammed, or their normal function could be degraded or disabled. Remote monitoring of CIEDs that requires frequent communication between a home transceiver and the device using radiofrequency telemetry adds an additional stage that could be vulnerable to a cybersecurity breach.

In some cases, such as the WannaCry ransomware attack, medical equipment can be affected without being the primary target of an attack. WannaCry targeted computers running an outdated version of the Microsoft Windows operating systems of which users failed to install updates to patch known vulnerabilities. The WannaCry actors encrypted user data and demanded ransom payment to release it, affecting, among others, multiple hospitals and health care professionals around the globe. As a result, network-connected medical devices across the United States running on this operating system were affected and taken off-line for remediation. Even equipment not connected to the Internet or internal health system servers is vulnerable to hacking. For example, ventilators and external defibrillators can become infected by malware on thumb drives that are plugged into systems when updating software or transferring data.[7]

Inconsistent cybersecurity prioritization in health care delivery organizations and the broad range of manufacturers supplying equipment to the health care industry (diagnostic and therapeutic medical equipment, electronic health records, billing software, purchasing software, etc) has resulted in significant cybersecurity vulnerabilities. Most modern medical equipment contains hardware and software components. The life cycle of software is often shorter than the product life of the hardware components. Institutions frequently use software beyond the period supported by the developer, and device manufacturers may not provide timely updates to identified cybersecurity vulnerabilities, leaving the software vulnerable to attack and providing an entry point for hackers to gain access across the interconnected information technology environment of a health care organization.

In 2013, President Barack Obama issued an executive order calling on the U.S. federal agencies to work collaboratively with critical infrastructure owners and operators to protect the nation's most sensitive infrastructures, including the health care sector, from cybersecurity threats.[8] The U.S. Department of Homeland Security's (DHS's) National Cybersecurity and Communications Integration Center (NCCIC) is tasked with analyzing and reducing cybersecurity threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities (Figure 1). When an incident occurs or is reported, NCCIC triages and collaborates a response to the incident. FDA becomes involved in the evaluation of a threat if it is deemed possible to result in patient harm. In such an event, the agency's role and responsibilities fall largely in line with non–cybersecurity responsibilities. For example, in the event of a CIED cybersecurity vulnerability, the FDA's Center for Devices and Radiological Health (CDHR) interacts with the manufacturer to assess the vulnerability and develop mitigating and/or corrective action (Table 2). In the event of a cybersecurity breach in which