Trends in Cardiovascular Medicine 29 (2019) 476–480

Contents lists available at ScienceDirect

Trends in Cardiovascular Medicine

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

Are implanted electronic devices hackable?☆

Bryce Alexander, BSc, MD, Sohaib Haseeb, BSc, Adrian Baranchuk, MD, FACC, FRCPC, FCCS*

Division of Cardiology, Queen's University, Kingston, Ontario, Canada

ARTICLE INFO

Keywords:
Pacemaker
Cybersecurity
Implanted electronic devices

ABSTRACT

Medical devices have become increasingly connected in recent years. While this added interconnectivity has provided capabilities for wireless communication and remote monitoring, it has also introduced possible risks for cybersecurity vulnerabilities. Lately, there has been an increased awareness of the potential for cybersecurity breaches in implanted cardiac devices (pacemakers and defibrillators) among patients, healthcare providers, and the media. In this article, we review the current perspective on cybersecurity in implanted medical devices, including a recent high-profile case example of a cybersecurity threat. We outline the actions taken by all the involved stakeholders in response to the disclosure of potential vulnerabilities in medical devices and summarize the positions of major societies in response to these events.

Published by Elsevier Inc.

Cybersecurity and medical devices

Cybersecurity is a broad term that encompasses the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and an organization and user's assets [1]. The past two decades have seen the rise of the Internet of Things (IOT), a vast collection of billions of everyday devices with embedded computers that have the ability to share information via networks. Many modern medical devices now contain embedded computer systems that are increasingly interconnected through networks. These include a wide array of computerized devices such as glucometers, blood pressure and heart rate monitors, pacemakers and insulin pumps to name only a few. There are obvious benefits to these devices, such as rapid clinical information transmittal from patients to clinicians and real-time therapy management that can improve patient care. However, the existence of these networks may put patients at risk for cybersecurity vulnerabilities related to information and device function security. All devices with embedded computer networks within the IOT, not just medical devices, may be vulnerable to cybersecurity breaches. In 2015, the auto industry experienced a major incident when Fiat Chrysler issued a voluntary recall of 1.4 million vehicles in the United States following demonstration by security researchers that it was possible to take control of the Jeep Cherokee remotely using the car's entertainment system [2]. Security concerns have also been identified in the medical industry in a range of medical devices from different specialties that are connected to networks, including devices used to deliver therapy. Recently, in August of 2018, Medtronic issued a security bulletin regarding a family of insulin pumps able to deliver remotely controlled insulin therapy [3]. The insulin pump and remote controller (similar to a key fob) allowed a diabetic patient to self-administer an insulin bolus without physically accessing the insulin pump. An outside security firm identified a method whereby a malicious user could cause the pump to administer an insulin bolus without the patient's knowledge, putting the patient at risk of hypoglycemia. Medtronic responded by issuing recommendations that patients using the affected model disable the remote bolus option on their pumps. In cases where patients wanted to continue the convenience of the remote bolus function, Medtronic recommended that patients only turn the function on when a bolus was needed and recommended that patients always be attentive to the audible pump alert when the remote option was functional.

To date, a total of six product-specific safety communications regarding cybersecurity vulnerabilities in medical devices have been issued by the United States Food and Drug Administration (FDA). Each safety communication was issued in response to reports by independent researchers regarding identified cybersecurity vulnerabilities. The first communication, issued in May of 2015, involved two models of the Hospira LifeCare infusion pump system, a computerized infusion pump designed for continuous de-

☆ **Conflict of interest:** Dr. Adrian Baranchuk has received a $12,000 unrestricted grant from Abbott Laboratories to conduct research in the field of pacemaker cybersecurity.

* Corresponding author at: Cardiac Electrophysiology and Pacing, 76 Stuart St, Kingston General Hospital K7L 2V7, Queen's University, Canada.

E-mail addresses: adrian.baranchuk@kingstonhsc.ca, barancha@kgh.kari.net (A. Baranchuk).

https://doi.org/10.1016/j.tcm.2018.11.011
1050-1738/Published by Elsevier Inc.

livery of anesthetic or therapeutic drugs that can be programmed remotely through a health care facility's ethernet or wireless network. In this case, an unauthorized user with malicious intent using software code would have been able to access the pump remotely and modify the dosage delivered, leading to over-or under-infusion of critical therapies [4]. A second report was issued in July of 2015 identifying similar vulnerabilities in the Hospira Symbiq infusion system. The next series of three communications were issued in response to potential cybersecurity vulnerabilities identified in implantable cardiac devices distributed by St. Jude Medical (now Abbott). The events surrounding this will be discussed separately in upcoming sections. Most recently, in October of 2018, the FDA issued a safety communication regarding potential vulnerabilities in the Medtronic CareLink and CareLink Encore Programmers used with their cardiac implantable electrophysiology devices (CIED). These programmers are designed to work with a wide array of implanted Medtronic devices such as pacemakers, implantable cardioverter-defibrillators, cardiac resynchronization devices and implantable monitors [5]. The programmers allow physicians to obtain device performance data, check battery status, and adjust or reprogram device settings from a CIED. Software updates to the programmer could be obtained either directly via a USB device or could be downloaded from the internet through the Medtronic Software Deployment Network. In this case, an external researcher was able to identify a method by which an unauthorized user could change the programmer's settings during remote download of a software update. Once changed, the programmer could then affect a CIED's settings during either implantation or subsequent follow-up visits. While not impacting the CIED's directly, this vulnerability allowed a method by which the settings of the physically implanted device could be changed, potentially causing patient harm. In response to these events, Medtronic disabled access to the Software Deployment Network, effectively fixing the problem. Medtronic representatives will now update all CareLink 2090 and CareLink Encore 29,901 programmers manually via the secured USB device [6]. Physicians can continue to use the programmers, however they no longer have the ability to remotely update the software.

In each case described above, there have been no identified instances of patient harm. However, due to the critical nature of medical devices and their ability to impact patient health, the potential for harm in a cybersecurity breach makes any vulnerabilities identified in this field concerning. Electronic medical devices that are implanted within the patient's body are of particular concern because unlike the external devices described in detail above, patients must undergo an invasive procedure in order to have one installed. The location of the device within the patient's body means that if these devices were compromised to the point of needing replacement, a second, otherwise unnecessary, invasive procedure would need to be undergone. Implanted medical devices include such devices as pacemakers, implantable cardiac defibrillators (ICDs), drug delivery systems and neurostimulators and are useful in managing a wide range of illness such as cardiac arrhythmias, diabetes, and neurological disease [7]. Like any devices in the IOT, they may be vulnerable to cybersecurity breaches. The first reports of vulnerabilities directly impacting implantable devices arose in 2016 and resulted in the first FDA safety communication directed at implantable devices in August of 2017 [8].

The Abbott pacemaker firmware upgrade

In August of 2016, a short-sell report released by an investment firm, Muddy Waters Capital LLC, outlined the potential for an unauthorized user in close proximity to the patient to remotely access several families (Table 1) of St. Jude Medical (now Abbott)

Table 1
Abbott laboratories pacemaker models affected.

Pacemaker models affected
United States
Accent DR RF
Accent MRI
Accent SR RF
Allure RF
Allure Quadra RF
Anthem RF
Assurity
Assurity MRI
Quadra Allure MP RF
Outside United States
Accent DR RF
Accent MRI
Accent SR RF
Accent ST
Accent ST MRI
Allure RF
Allure Quadra RF
Anthem RF
Assurity
Assurity +
Assurity MRI
Quadra Allure
Quadra Allure MP
Quadra Allure MP RF

pacemakers and impact their performance [9]. The report, written in concert with the cybersecurity research firm MedSec (Miami, Florida), detailed two types of potential cybersecurity breaches in several St. Jude Medical pacemaker models: (1) a "crash" attack that could lead to disabling of the device communication or high rate pacing, and (2) a "battery drain" attack [9]. To launch such an attack on a pacemaker, a person would have to be in close proximity (within several feet) of the pacemaker [10]. An attempt to replicate the conditions of one of the attacks by a group of researchers failed to produce any clinical harm. In this case the Muddy Waters report indicated that through a combination of undisclosed radio traffic, pacemakers could, in some cases, be made completely unresponsive to interrogation from the Merlin at Home system, an exploit they termed a "crash attack". They concluded that it was impossible to tell how such devices were functioning and that it was likely that physicians would explant devices that did not respond to the programmer [9]. Ransford et al. attempted to experimentally reproduce the "crash attack" while testing the pacemakers essential therapeutic function through a hard-wired test circuit [11]. They hypothesized that a clinically unusual amount of radio traffic would trigger a battery-saving mechanism in the CIED. After two hours of high-volume radio traffic they found that the pacemaker had indeed stopped sending radio telemetry and failed to establish communication with an interrogation device. However, by moving the pacemaker to a different location within the same room, normal communication was reestablished. Importantly, during the attack conditions, the hard-wired test circuit confirmed that the pacemaker continued to pace at the programmed setting of 60 beats/min and continued to inhibit pacing in response to the experimental cardiac signals. This experiment demonstrated that telemetry could be inhibited under specific conditions; however there was no apparent impact on the therapeutic functions of the pacemaker.

In situations such as these, security researchers typically practice coordinated disclosure, wherein a manufacturer is notified and a remediation is confirmed in advance of any public disclosure [11]. The motivation behind the release of the Muddy Waters report does not appear to have been focused on patient safety or in the interests of coordinated disclosure, as the findings were pub-

licly released without any prior communication with the manufacturer (Abbott, formerly St. Jude Medical) or the US Food and Drug Administration (FDA) [12,13].

In response to these events, the FDA issued a safety communication that outlined the potential vulnerabilities in several St. Jude Medical pacemaker models and informed the public of a software patch developed and validated by the manufacturer [14]. In January of 2017, St. Jude Medical was acquired by Abbott. Shortly thereafter, the FDA deepened its involvement by issuing a warning letter to Abbott that urged prompt action against the potential cybersecurity concerns identified by the Muddy Watters report [15]. In August of 2017, the FDA approved a firmware upgrade designed by Abbott to enhance cybersecurity in pacemakers [16]. Prophylactic removal and replacement of affected devices was not recommended. Although no known reports of an exploit causing actual patient harm had been identified, the upgrade impacted an estimated 465,000 pacemakers in the US with an additional 280,000 pacemakers also affected around the world [16,17].

The issued firmware upgrade is non-invasive and takes approximately 3 minutes to complete. During the upgrade installation, Abbott indicated that the pacemaker may temporarily change its mode of pacing, leaving open the possibility that patients may become symptomatic [18]. Abbott identified other possible risks associated with the upgrade and estimated frequencies of adverse events based on data extrapolated from other circumstances [18]. These additional risks included a complete loss of device function (0.003%), loss of programmed device settings (0.023%), and failure of the update (0.161%) [16]. Although the estimated risks were small and usually transient, a complete loss of device function would require urgent temporary pacing. Therefore, it was suggested that the upgrade be performed in an environment that is equipped with the ability to perform urgent temporary pacing [13,18].

Patient and physician response to Abbott firmware upgrades

The provider instructions in the FDA safety advisory of the Abbott firmware upgrade advised physicians to discuss the risks and benefits of the cybersecurity vulnerabilities and associated firmware update at the next regularly scheduled visit. As part of this discussion, they advised it was important to consider each patient's circumstances, such as pacemaker dependence, age of the device, and patient preference, and provide them with information related to the subject [14]. Given that there have been no known reports of patient harm associated with cybersecurity vulnerabilities in the Abbott pacemakers and a small but real quoted risk of possible complications, it was difficult for physicians to know how to counsel patients with the minimal data existing at the time [10]. Since then, additional data have been collected regarding patient and physician attitudes toward the upgrade and complication rates. Saxon et al. analyzed a population of 10,854 patients with affected Abbott pacemakers who were seen in clinic following the firmware upgrade release [19]. Of these, only 25% elected to proceed with the firmware upgrade. Patient specific factors that were associated with acceptance of the upgrade included a younger age, male sex and a newer date of implant. The authors reasoned that patients with a younger age and a more recent device implant may have been more likely to receive the upgrade due to a greater time-dependent exposure to risk since their expected device life was likely 5–10 years. The proposed reason for pacemaker-dependent patients receiving the upgrade less often was thought to be a concern that essential functions of the device, such as pacing, could be inhibited during the upgrade. Backup mode pacing was observed in 1% of this population and in each case was resolved with reprogramming of the pacemaker. No cases of complete loss of device function were observed. A smaller Canadian population of 155 patients seen in clinic after the firmware release demonstrated an upgrade acceptance rate of only 3.9% after the risk and benefits were explained in a systematic manner endorsed by the Canadian Heart Rhythm Society [13]. In this population, backup mode pacing was observed in one patient (0.6% of the population) (Fig. 1) and no cases of complete loss of device function were observed.

The FDA acknowledges that it is important to balance device cybersecurity with the need to avoid patient anxiety and minimize the risks associated with the update process [20]. Data reported to the FDA by Abbott indicate that no serious adverse events have been observed with the pacemaker firmware upgrade. A report issued by the FDA showed that 0.62% of the devices upgraded experienced an incomplete firmware update and remained stuck in backup pacing mode, which was later resolved. In addition, 0.14% experienced diaphragmatic or pocket stimulation or discomfort when their device was in backup pacing mode. In no cases of a firmware upgrade have there been reports of complete loss of device function to date [5].

Like any therapeutic product, no medical device, whether connected to the IoT or not, is entirely without risk. Given the possibility of adverse events with both accepting and not accepting the firmware upgrade, each encounter should be judged on its own merit with active participation by the patient. To help guide physician-patient encounters in the cybersecurity arena, several major Cardiology societies have issued position papers on the subject of CIED security; these position papers are reviewed in the following section.

Position of major societies

The American College of Cardiology's Electrophysiology Council provided a recent perspective on the issues concerning cybersecurity in CIEDs and what can be done to make improvements in a multidisciplinary manner [12]. The council states there is a need to pursue a comprehensive, proactive, and robust protection system for CIEDs [21]. To achieve this goal, an approach is encouraged where cybersecurity needs are reviewed in both the pre- and post-market settings [12]. The FDA currently utilizes this approach to characterize and assess cybersecurity risks and vulnerabilities in medical devices [20]. They also encourage well-informed and shared decision-making. Clinicians who manage patients with CIEDs are encouraged to learn about the possible cybersecurity risks, regularly review security updates, and be aware of the current issues at hand. Furthermore, clinicians are encouraged to establish a systematic approach to communicate updates in this area to the rest of the clinical team, with the patients actively engaged in the conversation [12].

The Heart Rhythm Society's recent leadership proceedings statement made recommendations focused on patient-centered communication strategies for healthcare professionals, government, and industry [22]. Healthcare professionals are encouraged to weigh the risks of the cybersecurity vulnerabilities and the firmware upgrade prior to implantation and engage in routine conversations with patients regarding this subject matter. If a specific vulnerability is identified, healthcare professionals are encouraged to have an individualized conversation with patients regarding the options to mitigate the risks, consequences for the CIED, and potential long-term solutions to eliminate the vulnerability. The best practice model for patients was suggested to be ongoing software updates at the time of face-to-face visits with healthcare providers. For industry and regulatory bodies, it is encouraged that cybersecurity considerations be implemented into early stages of product manufacturing, with proper infrastructure in place to mitigate specific vulnerabilities as they arise. The education of patients and healthcare providers, as well as increased collaboration between

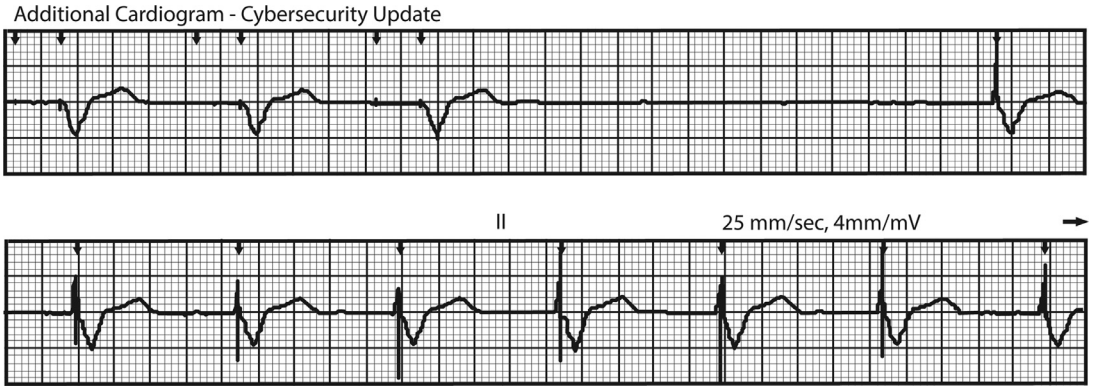

Fig. 1. A transient 3-second pause during a sudden switch to unipolar ventricular pacing during a firmware upgrade. *From: Baranchuk A, Alexander B, Campbell D, Haseeb S, Redfearn D, Simpson C,* et al. *Pacemaker Cybersecurity. Circulation. 2018 Sep;138(12):1272–3.* https://www.ahajournals.org/doi/abs/10.1161/CIRCULATIONAHA.118.035261.

Table 2
Abbott laboratories cardioverter defibrillator (ICD) and cardiac resynchronization therapy defibrillators (CRT-D) models affected.

ICD and CRT-D models affected
Current
Ellipse
Fortify
Fortify Assura
Promote
Promote Quadra
Quadra Assura
Quadra Assura MP
Unify
Unify Assura
Unify Quadra

all stakeholders, are emphasized in the evolving landscape of cybersecurity in CIEDs.

Future directions

In April of 2018, the FDA approved an additional firmware upgrade intended for certain Abbott implantable cardioverter defibrillators (ICDs) and cardiac resynchronization therapy defibrillators (CRT-Ds), further increasing the number of patients that were affected by this issue [23]. In May of 2018, this high-voltage firmware upgrade was also approved in Canada. The upgrade was designed to address a software-related battery performance alert and additional cybersecurity concerns across Abbott's radiofrequency enabled ICDs and CRT-Ds. As before, clinicians are tasked with the responsibility of identifying patients that are affected by the advisories, and as experience with both firmware upgrades accumulates, clinicians are encouraged to have risk-benefit discussions with their patients in a systematic manner. Due to the packaging of the battery performance and cybersecurity update, the FDA has taken a stronger stance than during the pacemaker advisory and recommends the upgrade for all eligible patients [5]. As before, prophylactic removal and replacement of the device is not recommended. This firmware upgrade includes increased security against unauthorized access to the devices, and also includes the battery performance alert for devices affected by previously issued lithium battery cluster advisory from 2016 [24]. The advisory applies to devices manufactured between January 2010 and May 2015 and includes several device families (Table 2). Similar to the pacemaker firmware upgrade, the upgrade process takes approximately 3 minutes to complete. During this time, the device will operate in back-up mode (VVI pacing at 67 ppm) with high voltage therapy disabled. Abbott quotes the following risks to be associated with the device upgrade and acknowledges that it is possible that additional adverse events may occur:

- discomfort due to back-up VVI pacing settings,
- reloading of previous firmware version due to incomplete upgrade,
- inability to treat VT/VF while in back-up mode given high voltage therapy is disabled,
- device remaining in back-up mode due to unsuccessful upgrade, and
- loss of currently programmed device settings or diagnostic data.

No estimation of the frequency of these risks has been reported at this time, though it is likely that the rate of adverse events will be similar to those experienced during the previous pacemaker upgrade process. Abbott recommends consideration of patient specific issues such as pacemaker dependence, frequency of high voltage therapy, age of device, and patient preference be given.

The Canadian Heart Rhythm Society has communicated the following recommendation: "As this upgrade for the high voltage devices includes the battery performance alert for advisory devices, we recommend this upgrade strongly for those devices. Given the very low risk of permanent loss of function from the upgrade, it is reasonable to consider this for all devices."

It is likely that there will be a higher rate of implementation of the high voltage firmware upgrade than the previous pacemaker firmware upgrade due to the bundling of the cybersecurity upgrade and the battery upgrade in one release. There is a need going forward for more information pertaining to the true risks and benefits of performing these firmware upgrades in order to effectively counsel patients.

Are implantable electronic devices hackable?

The short answer seems to be yes, although only in specific cases of extremely narrow and difficult to reproduce circumstances that are unlikely to lead to patient harm so far. Despite hundreds of thousands of devices being affected by the existing cybersecurity breaches, no reports of patient harm have ever been recorded. Most implantable electronic devices have a lifespan measured in years and with the fast pace of the cybersecurity industry it is likely that vulnerabilities will be discovered in the implanted lifetime of many devices [10]. Despite increasing attention to cybersecurity issues by manufactures and regulators it is probable that more of events such as the ones described above will occur in the near future. It is important for physicians to be knowledgeable about the risks in this field, as well as the steps that can be taken to mitigate these risks, so they can provide effective and accurate advice to their patients.

References

[1] ISO/IEC. ISO/IEC 27032:2012(E) information technology - security techniques - guidelines for cybersecurity. Geneva, Switzerland: ISO/IEC; 2012.

[2] Statement: Software Update [Internet] Available from: http://media.fcanorthamerica.com/newsrelease.do?&id=16849&mid=1.

[3] Security bulletin: MiniMed™ Paradigm™ Insulin Pumps (Vulnerability Summary) [Internet] 2018. Available from http://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/Medtronic-MiniMed-Paradigm_Security-Bulletin_FINAL_080718.pdf.

[4] Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication [Internet] 2015. Available from http://wayback.archive-it.org/7993/20170722144742/https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm.

[5] Cybersecurity Updates Affecting Medtronic Implantable Cardiac Device Programmers: FDA Safety Communication [Internet] 2018. Available from: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm623184.htm.

[6] Security Bulletin: CareLink 2090 Programmer and CareLink Encore 29901 Programmer [Internet] 2018. Available from https://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/REV-Medtronic-2090-Security-Bulletin_FNL.pdf.

[7] Halperin D, Heydt-Benjamin T, FuKohno T, Maisel W. Security and privacy for implantable medical devices. IEEE Pervasive Comput 2008;Vol. 7:30–9.

[8] Kramer DB, Fu K. Cybersecurity concerns and medical devices lessons from a pacemaker advisory. JAMA - J Am Med Assoc 2017;318(21):2077–8.

[9] Muddy Waters LLC MW is Short St. Jude Medical (STJ:US) [Internet] 2016. http://d.muddywatersresearch.com/research/stj/mw-is-short-stj/.

[10] Kuehn BM. Pacemaker recall highlights security concerns for implantable devices. Circulation [Internet] 2018;138(15):1597–8. Available from https://www.ahajournals.org/doi/10.1161/CIRCULATIONAHA.118.037331.

[11] 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. PACE - Pacing Clin Electrophysiol 2017;40(8):913–17.

[12] Baranchuk A, Refaat MM, Patton KK, Chung MK, Krishnan K, Kutyifa V, et al. Cybersecurity for cardiac implantable electronic devices: what should you know? J Am Coll Cardiol 2018;71(11):1284–8 Mar.

[13] Baranchuk A, Alexander B, Campbell D, Haseeb S, Redfearn D, Simpson C, et al. Pacemaker cybersecurity. Circulation 2018 Sep;138(12):1272–3.

[14] US Food and Drug Administration Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication [Internet] 2017. https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm535843.htm.

[15] Warning Letter to Abbott (St. Jude Medical Inc.) [Internet] 2017. Available from https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2017/ucm552687.htm.

[16] Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication [Internet] 2017. Available from https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm573669.htm.

[17] Dyer O. Abbott Laboratories offers fix for 745 000 pacemakers vulnerable to hacking. BMJ [Internet] 2017;358:j4190. Available from http://dx.doi.org/doi:10.1136/bmj.j4190 .

[18] Baranchuk A, Alexander B, Haseeb S. MY APPROACH to cybersecurity for cardiac implantable electronic devices. Trends Cardiovasc Med. 2018.

[19] Saxon LA, Varma N, Epstein LM, Ganz LI, Epstein AE. Factors influencing the decision to proceed to firmware upgrades to implanted pacemakers for cybersecurity risk mitigation. Circulation [Internet] 2018;138(12):1274–6. Available from https://www.ahajournals.org/doi/10.1161/CIRCULATIONAHA.118.034781 .

[20] Paulsen JE, Hazelett MB, Schwartz SB. CIED Cybersecurity risks in an increasingly connected world. Circulation 2018;138:1181–3.

[21] Baranchuk A, Refaat MM, Chung MK, Fisher JD, Lakkireddy D. Reply: cyberattacks and cardiac devices: firmware patches are not vaccinations!. J Am Coll Cardiol. 2018;72(July (1)):127–8.

[22] 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. Hear Rhythm 2018;15(July (7)):e61–7.

[23] Battery Performance Alert and Cybersecurity Firmware Updates for Certain Abbott (formerly St. Jude Medical) Implantable Cardiac Devices: FDA Safety Communication [Internet] 2018. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm604706.htm.

[24] Premature Battery Depletion Advisory. [Internet] 2016. Available from https://www.sjm.com/en/patients/arrhythmias/resources-support/battery-advisory?clset=af584191-45c9-4201-8740-5409f4cf8bdd%3Ab20716c1-c2a6-4e4c-844b-d0dd6899eb3a.