Trends in Cardiovascular Medicine 29 (2019) 129–130

Contents lists available at ScienceDirect

Trends in Cardiovascular Medicine

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

MY APPROACH

MY APPROACH to cybersecurity for cardiac implantable electronic devices☆

Adrian Baranchuk, MD, FACC, FRCPC, FCCS

Bryce Alexander, MD

Sohaib Haseeb

Medical devices are increasingly becoming connected to the "Internet of things." Although the networking of medical devices has many advantages in terms of convenience and remote monitoring of therapy, it comes with an increased risk of vulnerability to cybersecurity attacks. Medical devices have been the target of cybersecurity attacks for over a decade, and these attacks have focused not only on pacemakers but have included the entire spectrum of medical devices. Recently, in August of 2016, St. Jude Medical (now Abbott) was put in the public spotlight following the release of short-sell report by Muddy Waters LLC outlining two methods by which their pacemaker cybersecurity could be breached in what was termed a "crash attack" and a "battery drain attack." However, an effort by a group of researchers to replicate the attack conditions failed to reproduce any clinically significant harm. The United States Food and Drug Administration became involved and issued a warning letter to Abbott. In response, Abbott issued a firmware upgrade for several of its pacemaker models to fix the vulnerability. Implantation of the firmware upgrade is noninvasive and takes only several minutes to complete. During the upgrade, the pacemaker may temporarily change its mode of pacing, leaving open the potential for patients to become symptomatic. The device upgrade itself is not without risks. Abbot has quoted the following small, but not insignificant, risk of adverse events: complete loss of function (0.003%), loss of device settings (0.023%), and failure of the update (0.161%). Due to these risks, it has been recommended that the upgrade take place in a center with the ability to perform urgent temporary pacing. Importantly, these risks have been derived from other clinical settings, and the true adverse event rate of the upgrade may not be known until many upgrades have been completed.

Physicians are responsible for identifying patients who may be at risk and offering the firmware upgrade. Soon, an additional firmware upgrade for Abbot implantable cardioverter-defibrillators will be released in Canada, which will increase the number of patients affected by this issue. Patients have the right to decide if they wish to proceed with the upgrade and must weigh the theoretical risks of a cybersecurity attack against the small, but very real, risk of adverse events during the upgrade. A systematic method of explaining the risks and benefits of the upgrade is a valuable tool for clinicians in this scenario. In our center, we use recommendations devised by Abbott and endorsed by the Canadian Heart Rhythm Society. Our approach is:

1. to comprehensively explain to the patients both the possibility of a "hack" attack along with probability of a hack attack. We explained that no hack attack has occurred so far, and, to the best of our capacity, what could be the motivations for such a hack attack.
2. to explain in detail the possible risks associated with the firm upgrade. For that purpose, we quote the percentages of complications provided by Abbott. We also tell, after the first 2 months, the percentages of complications found by our

☆ First published on PracticeUpdate on May 1, 2018. Republished with permission.

https://doi.org/10.1016/j.tcm.2018.10.013

group. So far, no serious complication was seen in the 6 patients who accepted the firmware upgrade.
3. to upgrade the firmware, a procedure that takes less than 5 min.

It has been our experience that the majority of patients at our center, when told the risks and benefits of the upgrade in a systematic manner, have chosen to not proceed with the firmware upgrade. This may reflect patient preference to not expose themselves to possible adverse events in exchange for fixing the risk of a theoretical cybersecurity attack.

The firmware upgrade will be soon available for patients with ICDs, significantly increasing the number of patients exposed to these encounters. This has produced a significant burden in our Cardiac Rhythm Device Clinic, as each patient needs to be carefully explained to regarding the pros and cons of upgrading their devices. At the same time, the upgrades need to occur in a safe environment, with the ability to proceed to urgent battery replacement.

So far, cybersecurity has only affected Abbott devices; however, from a "conceptual" point of view, this may not be restricted to a single company and potentially could expand to other companies in the future. Multisectoral stakeholders groups, including experts in cybersecurity safety, IT, electrophysiologists with experience in cardiac devices, and communicators, should work together to explore all possible vulnerabilities of existing and future intracardiac devices. Physicians dealing with patients with pacemakers and ICDs need to be aware of this situation and have to have a plan ready to properly explain to the patients the different alternatives and consequences of their decisions.

Adrian Baranchuk, MD, FACC, FRCPC, FCCS
Bryce Alexander, MD
Sohaib Haseeb
Queen's University, Kingston, Ontario, Canada

E-mail address: barancha@kgh.kari.net (A. Baranchuk)