IN VIVO
THE BUSINESS & MEDICINE REPORT

Medical Devices

WIRELESS MEDICAL DEVICE TECHNOLOGY – STILL SECURE ENOUGH?

Medtech manufacturers and users need to be ever alert to the risk of theft of intellectual property, regulatory violations, and loss of proprietary information assets. Security should be a top priority for executives thinking of entering the market with innovative medical devices, according to Miri Halperin Wernli, PhD, VP, deputy head global clinical development, global head business and science affairs, Actelion Pharmaceuticals Ltd., and Boaz Ganor, PhD, of the Tel Aviv-based International Institute for Counter-Terrorism (ICT), who addressed these issues at the ICT's *14th International Conference on Counter-Terrorism* in Herzliya, Israel last year.

It's not as though industry and government are not aware of the issues. Last fall, the FDA organized a gathering in Arlington, VA, for public and private sector experts to exchange points of view and question each other about the current state of play and possible solutions. Many good thoughts came out of that meeting (*See "Legacy Devices The Weak Link In Cybersecurity Fence"* — "The Gray Sheet," *October 24, 2014*), but stakeholders are behind the curve. Collective recognition of the IT security problem is a necessary first step toward a solution. Given the rapid expansion of software-reliant medical devices, many know that industry is in the "too little, too late" mode, and desperately needs to change.

Numerous medical treatments would not exist if not for the software component of devices, which enables wireless monitoring and remote reprogramming. It facilitates greater communication between clinician and device, from device to device, and between device and a variety of health care administrative functions.

A typical hospital setting has hundreds of computers classified as medical devices, many operating with out-of-date software, without anti-virus protection, and often compromised by malware inadvertently embedded by vendors.

The problem is so extensive that in July 2013, the FDA warned hospitals to take action to close the security gaps in their computers, smartphones, and tablets. The warning focused on the failure to provide timely security software updates, the continued use of legacy operating systems such as Windows XP, and the ongoing issue of inadequate password control. (*See "FDA Proposes New Cybersecurity Submission Standards For Devices"* — "The Gray Sheet," *June 17, 2013*.)

Of the three categories of software-reliant medical devices – peripherals, independent, and networked – the most serious hacking concerns relate to the latter two. Both types, which include implantable medical devices (IMDs), are increasingly subject to wireless control for adjustments, calibrating connections with other devices, and data collection.

> **Given the rapid expansion of software-reliant medical devices, many know that industry is in the "too little, too late" mode, and desperately needs to change.**

Global pacemaker sales are forecast to total $5.1 billion by 2018, meanwhile, the ICD (implantable cardioverter defibrillator) market is predicted to total $10.5 billion in 2015. Drug pump and neurostimulator sales also are on the uptick. Although currently small in number, it's only a matter of time before new wireless IMD nanotechnologies will be entering the market in the shape of smart pills, brain implants, a variety of subcutaneous sensors, and "smart" orthodontia, among others.

To frame the picture in terms of current usage, more than 50% of IMDs in the US use software and communicate via radio waves. A pacemaker may require as much as 80,000 lines of code; drug infusion pumps as much as 170,000 lines. Some of this programming controls how the device functions; other programming allows the device to connect to EMRs and billing computers. What could possibly go wrong?

In 2010, an automatic software update by web security giant MacAfee went awry causing health information technology devices worldwide to be off-line. Almost half of the 6,000 computers in Upstate University Hospital in Syracuse, NY, were affected. One-third of Rhode Island's hospitals had to postpone elective surgeries and stop treating non-traumatic ER patients.

Between 2005 and 2010, the FDA received reports of 710 patient deaths linked to problems with infusion pumps, including incorrect entry of data dosage and software malfunctions. One issue described by agency officials was defective software interpreting a single keystroke as two separate presses of the key. This resulted in 22 medication units being dispensed instead of two. Reports in the media at the time suggested the agency's officials believed the number of deaths to be higher.

Elsewhere, a programming issue involving an infusion pump resulted in a bolus being delivered in 20 minutes instead of the intended 20 hours.

MALWARE

There are two significant malware-associated risks. The biggest is widespread unavailability of patient care. Imagine the havoc when hundreds of infusion pumps in a hospital setting stop working! The other is compromised functioning of medical sensors resulting in inappropriate clinical decisions due to receipt of inaccurate data.

One possible remedy to these and other forms of malware interference is a system that would monitor power consumption. Changes in power consumption rates may indicate that malware is at work.

MALICIOUS ATTACKS

Malware is a serious nuisance, but it pales next to the very real threat of malicious attack. No longer just the realm of fiction, real criminals are hacking in to steal personal information and to cause harm. Computer network security expert Jay Radcliffe put this issue in the public spotlight. A diabetic, he found that the wireless connection of his insulin pump was vulnerable to letting hackers manipulate insulin levels, with possible fatal results.

Malicious attacks of devices can fall into one of three categories:

- **Insider Attacks** – those in which device programmers, the compact machines used to configure programmable digital circuits, are used to obtain protected information. There is no registry of device programmers, and no knowledge of how many exist. Typically, device programmers have few access controls and are not password protected. They can be easily "misplaced" in the health care environment, and can even be built from scratch with cheap and easily available materials. Should a device programmer fall into the wrong hands, there is a strong chance of malicious disruption.
- **Passive Outside Attacks** – those in which the hacker's primary goal appears to be accessing private patient information. Patient data stored on devices generally are not encrypted. This lack of protection makes it possible for the information to be collected, as demonstrated by researchers who have been able to wirelessly tap into medical records.
- **Active Outside Attacks** – those in which a patient's vital signs are illicitly captured, device power is drained, or therapy is turned off or changed, negatively affecting the patient's physiology. In 2008, computer scientists demonstrated how pacemakers and defibrillators can be hacked wirelessly using radio hardware, an antenna, and a PC. They were able to shut down a combination heart defibrillator and pacemaker, and reprogram it to deliver potentially lethal shocks or to drain its battery.

Given their prominent role across the globe and sophisticated use of technology, terrorists must be factored into the equation. Infiltrating device technology fits with the new terrorism model of inflicting fear and anxiety in large populations and magnifying that fear through adept use of new and traditional media.

Disruption of medical treatment has been added to the terrorist armory, and it is only a matter of time before it joins bombings, poisonings, sabotage, and other forms of physical attacks. Eventually, we'll see it in the form of cyberattacks. Seen in this light, and with so many hospitals with very low levels of security, the size of the potential threat is clear. And it won't get any smaller if it remains unaddressed.

WHAT CAN BE DONE?

Clearly, government regulators are interested and involved. The US Congress has investigated the issue, and in 2012 the US Government Accountability Office (GAO) reported that none of the US agencies were studying security and connectivity of medical devices. In October 2014, the FDA confirmed its earlier guidance that device manufacturers need to tighten security and improve their cyber security and risk management planning. (*See "FDA Sticks With Premarket Plans In Cybersecurity Guidance"* — "The Gray Sheet," *October 1, 2014.*)

Unfortunately, regulators, like industry, are in a new frontier. The FDA and EMA are oriented toward medicines and their safety. As to devices, their concerns are with their routine functioning, not security issues linked to software and connectivity. Regulators are not adequately resourced to handle device security research. Given these constraints, the FDA should continue, as it did in October, to facilitate the exchange of information across various sectors.

Industry and regulators should also work with existing resources and infrastructure to achieve what Jay Radcliffe has identified as a "Framework for Security." This consists of five action steps:

- **Process** – Create a process-oriented plan of how a device would be fixed in the event of failure. Models exist in other industries, but are lacking among medical device manufacturers.
- **Responsibilities** – Clarify the responsibilities for device and operating system patches. FDA guidance on this has been inconsistent. 510(k) submissions should include supplemental information about device updates.
- **System** – Protect operating systems by clarifying processes and procedures for patches and updates. Wernli and Ganor recommend a collaborative approach involving the private and public sectors.
- **Buying** – Make security a part of purchasing criteria and decisions. Manufacturers should be required to formally disclose a medical device security statement indicating all security-oriented due diligence.
- **Testing** – Both buyer and manufacturer should retain third parties to provide thorough security testing on devices under consideration for purchase.

Medical device risks increase with medical device complexity, and software and interconnectedness are highly complex. The future of device technology is rapidly changing with a higher risk of intentional interference accompanying greater reliance in wireless and Internet connectivity. Because of this, privacy and security should be added to the standard metrics of safety and efficacy.

Given the increasing recognition that the potential price of doing nothing is too high, the question that stakeholders need to reflect on is: what will it take for industry to change?

Will it be a rash of homicides by hacked devices? Will it be large-scale theft of personal medical data? Or will it be the simple understanding that we are unable to meet the challenges of today with yesterday's solutions, while expecting to be in business tomorrow?

A#2015800026

By Miri Halperin Wernli and Boaz Ganor

Miri Halperin Wernli, PhD (miriam.halperin_wernli@actelion.com) is VP, Deputy Head Global Clinical Development, Global Head Business and Science Affairs at Actelion Pharmaceuticals. Boaz Ganor (ganor@idc.ac.il) is Founder and Executive Director of the Tel Aviv-based International Institute for Counter-Terrorism.