Evaluate Vantage

October 26, 2016

Vantage Point – Medtech needs to up its cybersecurity game

Madeleine Armstrong

Worries about medtech cybersecurity are not new, but they have come to a head recently – first with controversial claims of security flaws in St. Jude Medical's implantable cardiac devices and then with Johnson & Johnson's warning that one of its wirelessly controlled insulin pumps could be vulnerable to hacking.

While there is no reason for patients to panic cybersecurity was bound to hit the headlines sooner or later, one expert believes. "We were thinking of it as more of a when than an if," Kevin Fu, associate professor of computer science and engineering at the University of Michigan, tells *EP Vantage*. The topic will become even more important with the advent of more complex devices, he believes, and he urges companies to consider the risks at the very earliest stages of device development.

"10 years from now, if we don't do a better job with security I can imagine patients losing confidence in future technologies like the artificial pancreas," he says. Failing to consider cybersecurity could leave devices vulnerable to attack by computer hackers, for instance, in the worst case putting patients at risk of death.

Risk-benefit

The risk of a security breach needs to be weighed against the benefit of medical technology, as the medtech industry association Advamed points out.

Even hackers who seek to advise industry, and who have found vulnerabilities in devices, often do not recommend that the device company tell patients to stop using them, says Mark Brager, an Advamed spokesperson. "They all agree that the benefits of the technology far outweigh the minimal cyber risk."

Advamed admits that no connected device can be deemed completely safe. To reduce the risk of a cyberattack, companies should follow the FDA's guidance documents, as well as international standards developed by the likes of the Association for the Advancement of Medical Instrumentation (AAMI), says the industry body's associate vice-president of technology and regulatory affairs, Zach Rothstein.

"Following these procedures offers, in today's environment, the best protection available to patients worldwide," he tells *EP Vantage*.

Justine Bone, chief executive of Medsec – one of the groups that raised the allegations against St. Jude – demurs, saying companies should be "going above and beyond basic compliance and certification requirements".

Professor Fu seems less confident that adhering to the rules will stop any potential cyberattack. "There's always more that companies can do, but there is a point of diminishing returns."

Ultimately the issue is not whether a device is hackable, Professor Fu argues, as "anything with a chip in it is hackable". So far, infusion pumps, insulin pumps and implantable cardiac devices like pacemakers have been disproportionately affected by cybersecurity scandals – probably because these support important functions in the body, so the consequences of a potential hack would be serious.

The more important question, according to Professor Fu, is how well the device copes when under attack.

“We’ve advised for years that when a device senses that it’s come under attack it goes into a safe mode, perhaps even turns off secondary functions.”

Indeed, this is what St. Jude said had happened to its device, rather than a crash, as the short seller Muddy Waters Capital claimed. Whether this was actually the case remains unclear – a report by Professor Fu’s cybersecurity company Virta Labs could not conclude whether the allegations against the company had merit or not.

The saga rumbles on, with Muddy Waters making new allegations in October in spite of a lawsuit from St. Jude.

Earlier better

Any medtech manufacturers hoping to avoid a similar fate might be disheartened to hear that it could be too late for products already on the market. “Companies really need to build security in rather than bolt it on after the fact. It’s very difficult to retroactively add security,” says Professor Fu.

It takes 10 years or more to design a new medical device, and cybersecurity has only been on the radar in the last decade – so upcoming devices might fare a little better.

The Swiss blood glucose monitoring specialist Ascensia Diabetes Care agrees that cybersecurity should be considered early, with a spokesperson describing it as a “fundamental” factor when developing its new wireless-enabled devices, recently CE marked in Europe.

“We started the design of our Contour Next One meter and the companion Contour Diabetes App with cybersecurity in mind from the outset, starting with the early design requirements,” the spokesperson tells *EP Vantage*. “We engaged outside cybersecurity consultants to review and test our design, coding and final product.”

The meter and app took around four years to develop, so cybersecurity was already at the forefront at the early stages of development.

Wider responsibility

Medtech companies are not the only ones with responsibilities: hospitals and health centres are also an important part of the cybersecurity chain. “Basically every layer introduces more risk. Imagine you get a medical device that’s difficult to secure, and then you put it in a hospital that’s also difficult to secure,” Professor Fu says.

This vulnerability was highlighted earlier this year when several US hospitals’ IT systems were infected with ransomware and the hackers demanded cash to restore them.

Overall, Professor Fu is optimistic about the long-term cybersecurity of medical devices, but believes that in the short term “there are going to be many dozens if not hundreds of unpleasant stories”.

One recent story involved J&J warning patients that its Animas OneTouch Ping insulin pump was vulnerable after being alerted to the problem by a benign hacker. The fear is that an attack could trigger unauthorised and potentially fatal insulin injections – however there have been no reported incidents, and J&J describes the risk as low.

Similarly, other cases of cybersecurity hitting the headlines have often involved law-abiding hackers, or “white hats”, trying to find vulnerabilities so they can warn companies about potential problems.

Indeed, Professor Fu helped propel cybersecurity into the public consciousness with a 2008 paper on how his group had hacked an implantable cardioverter defibrillator and caused it to emit a potentially fatal shock, with the aim of improving patient safety.

But this has not stopped some from worrying about the possibility of a malicious attack. Former US vice-president Dick Cheney has reportedly had his pacemaker’s wireless capabilities disabled to stop possible assassination attempts.

Professor Fu fears negligence more than a criminal mastermind. “I’m more concerned about the hospital that loses its continuity of operations. That doesn’t necessarily require malice, it does not require a hacker – all it would require is a computer virus that gets into the wrong place at the wrong time.”

He compares cybersecurity with the understanding of the importance of handwashing. “It’s taken over 170 years to get where we are with hygiene in hospitals. We’re at a very early stage in understanding medical device security. It’s really basic hygiene – we’re picking our nose in the operating room.”

“A patient shouldn’t have to ask their physician to wash their hands. And a patient shouldn’t have to ask their physician to secure their medical devices – it should be second nature.”

To contact the writer of this story email Madeleine Armstrong in London at madeleinea@epvantage.com or

follow @ByMadeleineA on Twitter