When Healthcare Hacking Turns Deadly

November 30, 2015 â€“ You may not realize it but if you or a loved one is walking around with an implanted medical device â€“ such as a pacemaker â€“ there is a good chance that the device has wireless networking capability. You may not have given this much thought since your doctorâ€¦ or the doctor of your loved oneâ€¦ probably told you that wireless connectivity would be used to program the device and make adjustments to it. But what if it was hacked? What then?

An article published this last Thursday in the National Law Review provided a startling statistic. It said, â€œin a span of six months, hackers attempted to log into MRI and defibrillator machines over ten thousand times and attempted to download malware approximately 300 times. Had these hackers been successful, they could have accessed patientsâ€™ personal information or reprogrammed the defibrillators to deliver deadly jolts of electricity to patientsâ€™ hearts.â€•

While that article was primarily focused on liability issues for medical device manufacturers, it raises the issue of cybersecurity to a new level for tens of thousands of people just trying to live out their lives in peace. Hacking of this type can lead to a lot more than ID theft. It could cost them their lives.

The article goes on to explore the motivations for this type of hacking. â€œAccording to Dr. William Maisel, â€˜[m]otivation for such actions might include the acquisition of private information for financial gain or competitive advantage; damage to a device manufacturerâ€™s reputation; sabotage by a disgruntled employee, dissatisfied customer or terrorist to inflict financial or personal injury; or simply the satisfaction of the attackerâ€™s ego.â€™ Medical data can be worth ten times as much as a credit card number. Added to that, the medical device market was a $25.2 billion industry in 2012 and is expected to be a $33.6 billion industry by 2018. Thatâ€™s a vast market of potential victims.â€•

To the list of motivations, we can add one other. Someone with a networked medical device could actually be individually targeted for injury or death. That could result in a crime almost impossible to trace or to prove.

As with other forms of hacking, this is no longer a matter of â€œifâ€• but a rather, a matter of â€œwhenâ€•. Based on the statisti last year, it is already clear that attempts to hack medical devices are well under way. The only thing we can hope for is that manufacturers use the best forms of encryption available and that they make regular updates so that patients are protected. If, on the other hand, they simply rely on actuarial tables to calculate their liability costs associated with a hacking death, versus the cost of keeping their products up to date, anyone walking around with one of these devices may be in trouble. You just better hope that nobody out there really dislikes you.
byJim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS