Berkleylifesciences
a W. R. Berkley Company

Cyber Security Considerations in Integrated Medical Devices

Many were shocked when they saw a recent episode of the television show *Homeland*, where an attack on the Vice President was conducted by hacking into his pacemaker, taking control of the device, and bringing on a heart attack.[1] This plotline seemed far-fetched but the reality is that medical devices are becoming more digitally interconnected with each other and with information networks. Although an event like this has not yet happened, the possibility is very real.

Medical devices fall under the authority of the Food and Drug Administration (FDA) and recently, cybersecurity in medical devices has been given tighter scrutiny by the FDA due to these devices becoming more interconnected. Last year, the FDA issued its final guidance on this topic entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." [2] These digital connections create a new threat of cybersecurity breaches. Such threats include both controlling the devices themselves as well as using the devices as portals to broader digital information networks. This paper provides a review of what makes medical devices vulnerable, the outcomes that could happen if breached, and what practices stakeholders should take to protect themselves against these vulnerabilities. This is the second in a series of papers focusing on cyber security in the life sciences space.

Understanding the vulnerabilities

Medical devices have been found to be a target of cyber-criminal activity since they can be the gateway to a digital network such as that found in a hospital. As reported by TrapX, a deception based cybersecurity firm, the recent malware virus MEDJACK compromised three separate hospital systems after accessing the systems through medical devices like x-ray systems, blood gas analyzers, and diagnostic equipment.[3] The breadth of use of digitally connected medical devices has created many stakeholders, all of which must be involved to ensure that these medical devices are adequately protected from cyber breaches. Depending on the device use and the stakeholder involved, there are different vulnerabilities and outcomes. The following table helps to understand how each stakeholder could be affected:

Stakeholder	Vulnerability	Outcome
Medical device manufacturer	Out of date software; device access; malware	Compromised device functionality, device or network breach, data loss (such as intellectual property)
Medical professional	Network access	Network breach, data loss
Hospital	Out of date software; device access; malware	Compromised device functionality, device, privacy, or network breach
End user	Device access	Compromised device functionality

When vulnerabilities are exposed in medical devices and the digital networks they are connected to, both of these can be breached. There are three principal ways that this could happen. The first one is from malware. The FDA defines malware as "…software designed with malicious intent to disrupt normal function, gather sensitive information, and/or access other connected system."[2] Malware can infect digital networks by using the medical device as the entry point. Once a digital system is infected with malware, it is easily breached by letting the hacker take control of the network and taking the data that he wants. The second way is from devices or networks not getting its software updated. Lack of updated software with necessary patches or fixes leaves the devices or networks more vulnerable for attacks from malware. The third way is uncontrolled devices or networks. If devices or networks do not include the proper access controls or authentication processes, then it is much easier to gain unauthorized access into these devices or networks and steal data. All of these vulnerabilities can lead to outcomes where the device itself, the network or data housed on the network is compromised or lost.

Below are a series of questions about the medical device and the digital information network through which it can connect for the stakeholder to consider when evaluating potential vulnerabilities:

1. What type of data is being sent and received by the device and how is it being encrypted?
2. What are the possible adverse outcomes of a device hacking (including impact to the patient)?
3. Does the medical device create an opening for a cybercriminal to penetrate the digital network that the device is connected to?
4. How will the medical device manufacturer be notified of potential cyber security breaches surrounding their products?
5. What types of controls are in place to protect against incursions?

Risk Management Resources to Mitigate This Exposure to Cyber Security

There are many ways that a medical device stakeholder can begin to understand his or her potential cyber vulnerabilities. The recommendation from the National Institute of Standards and Technology (NIST) is to take the following steps to mitigate cyber security exposures:

1. Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. Protect – Develop and implement the appropriate safeguards to ensure delivery or critical infrastructure services.
3. Detect – develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. Respond – develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.[4]

By following these steps, a medical device stakeholder can conduct a gap assessment of their cyber activities and start to create practices and procedures to close these gaps. Depending on what type of stakeholder you are, the practices to be implemented are different. The following are examples of practices by stakeholder

1. Medical device manufacturer:
    a. When designing a medical device, cyber security issues should be considered. The FDA now requires that as part of the premarket submission, information related to the cybersecurity of the medical device needs to be included. [3] These include but are not limited to:
        i. Description of the advanced authentication process and encryption for the device and its data.
        ii. Description of fail-safe modes – how does the device react once breached?
        iii. Adverse event or risk monitoring of their product in the marketplace
    b. Once the medical device is in the marketplace, software updates should continue to be developed and dispatched to the stakeholder to prevent gaps in cyber protection.
2. Hospital or medical professional:
    a. When choosing medical devices, be informed about the cyber security controls that the device has in place and what support the manufacturer will give for software updates and patches when known issues are identified.
    b. Create cyber security controls for the users of devices as well as the digital networks that they are connected to. These controls should include, at a minimum, rules for device access to be limited to only trusted users.
    c. Create policies and procedures around the access and use of the medical devices including:
        i. How to respond to a cyber-incident with the device?
        ii. How often to perform virus scans?
        iii. How often to check and, if applicable, install software or patch updates?
        iv. Who will have access to the devices and digital network?

d. Report any adverse events that occur with medical devices, following the FDA medical device reporting regulations (MDR).
e. Conduct audits of the effectiveness of cyber controls, such as fuzzing, a testing technique for locating unknown vulnerabilities and other defects by sending malformed and unexpected inputs to software.

3. End user:

   Understand what type of device will be used and how the medical professional or hospital ensures that the device's software is up to date and functioning properly.

Cyber criminals will continue trying to find ways to infiltrate digital networks at hospitals and medical device manufacturers that hold sensitive information like personal data and intellectual property Ultimately, it is up to the stakeholder to protect themselves against these criminals by keeping their cyber security controls up to date to prevent any infiltration of their digital network via the medical devices they produce, distribute or utilize.

Sonia Weiss, ARM, CIH, MBA, MPH, Senior Life Science Risk Management Specialist

Sonia Weiss has over 10 years of experience working in the environmental, health and safety ("EHS") professions, specializing in providing EHS services and advice to the academia, manufacturing, and biotechnology sectors. At Berkley Life Sciences, her focus is on helping her life science clients understand and manage their overall risk, with a particular focus on cyber security risk. Prior to joining Berkley Life Sciences in 2013, Ms. Weiss was the Safety Health and Environmental (SHE) Manager for Genencor, where she was responsible for workplace safety, regulatory compliance, risk assessments, and industrial hygiene. Ms. Weiss has a Bachelor of Arts degree in Biochemistry and Environmental Sciences from Northwestern University, a Master in Public Health in Environmental Health Sciences from the University of California, Berkeley and a Master in Business Administration from Presidio Graduate School.

1 http://www.forbes.com/sites/singularity/2012/12/06/yes-you-can-hack-a-pacemaker-and-other-medical-devices-too/
2 FDA Guidance for Industry and FDA Staff: Content of Premarket submissions for management of cyber security in medical devices.
3 http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html
4 NIST National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cyber security, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf