March 3, 2016

OCR Cyber-Awareness Monthly Update

February 2016 Topics:

- Why any Organization Can Suffer a Healthcare Breach, and Tips for Keeping PHI Safe
- NSA's Lesson Learned
- Malware and Medical Devices

Why any Organization Can Suffer a Healthcare Breach and Tips for Keeping PHI Safe

According to Verizon's 2015 Protected Health Information Data Breach Report, industries such as finance, insurance, education, retail, and professional services (i.e. law offices and tax preparers) have had the most data breaches involving personal health information. Further, the report states that some companies are managing their own employee health benefits programs and are becoming custodians of more healthcare information, and "their information security team may not even realize that they have this kind of information in their organization until it gets breached."

The Report highlights that criminals are finding new ways to monetize health information. Personal health information may be stolen and sold to the uninsured, used to get medical supplies and equipment that can be sold, or used to submit fake insurance claims. As such, this information is often the target of a breach.

An entity must be aware of the information that lives in its organization, as well as how it's processed through its many stages of use and where it goes outside the organization. Also, it must make sure it has controls in place throughout the data lifecycle. If the entity doesn't know where the data lives, it's likely that it has been exposed someplace that the entity doesn't know about.

Quick tips Covered Entities and Business Associates should keep in mind as part of their compliance efforts:

- **Know what data you have--** Identify all the data in the enterprise lifecycle and pay particular attention to the pieces of information that could be considered high risk.

- **Encrypt or De-identify** – Consider the use of encryption to secure sensitive data or de-identifying data to eliminate personal identifiers (e.g., through the use of HIPAA Expert Determination or Safe Harbor de-identification methodologies).

- **Involve teams responsible for defining data –** Know why your entity has certain types of data. Get your teams involved to help understand how the data is being created and used.

- **Strengthen security around data pathways between your entity and your vendors –** Make sure data is identified and protected when it's moving out of your systems to your vendors. Ensure that breaches and security incidents are properly addressed as part of your business associate agreements or service level agreements.

- **Monitor access to data –** Limit access to data only to the users that need the data and only to the amount or type of data required for the user to perform his or her job duties including access by privileged users. Put in place processes to log user activities regarding data access and monitor these logs.

- **Ensure appropriate training –** It is important to provide training for all employees who touch data.

NSA's Lessons Learned

At this year's inaugural Usenix Enigma security conference in San Francisco, the NSA spoke about how nation-state attackers can exploit the smallest vulnerability on your system and provided a compendium of best security practices that should be implemented to mitigate the likelihood of these types of attacks from occurring.

Attackers may gain access to your system by retrieving credentials of network administrators and others with high levels of network access and privileges. Also, attackers look for any hardcoded passwords in software or passwords that are transmitted in the clear.

NSA says no vulnerability is too insignificant and that you should not assume a crack is too small to be noticed or exploited. Temporary cracks such as opening your network over the weekend to allow a vendor to remotely access your network to fix it can be exploited; employees using personal devices, also used by other family members to play games, to connect to the organization's network is another vulnerability; the heating and cooling system and other elements of a building infrastructure can provide unexpected pathways into your network.

NSA notes that it is important to know what applications are running on your network and devices that are connected to your network.

To keep intruders out of your network, Covered Entities and Business Associates should consider:

- Limiting access privileges for information systems to those who really need them.
- Segmenting networks and important data to make it harder for hackers to reach your information assets.
- Patching systems and implement application whitelisting.
- Removing hardcoded passwords and legacy protocols that transmit passwords in the clear.
- Implementing a device that monitors network activity and produces logs that can record anomalous activity.
- Staffing system administrators with the ability to read and decipher network activity logs.

Resources:

National Security Agency: https://www.nsa.gov/index.shtml

Malware and Medical Devices

The biggest danger to medical devices is mundane-but manageable, says the Food and Drug Administration (FDA). Cybersecurity for medical devices has been known to be poor, and according to a group of security researchers called “I Am the Cavalry,” the health care sector is 15-25 years behind banking and retail when it comes to defending against online threats.
Last year, researchers ran “honeypot servers” pretending to be medical devices, including an MRI and defibrillator, and they were infected by malware hundreds of times.

Although the researchers believe that medical devices are not deliberately targeted by malware, a resourceful malware could overwhelm a medical device and cause patient harm. According to Suzanne Schwartz, director of emergency preparedness/operations and medical countermeasures in the FDA’s Center for Devices and Radiological Health, connected/configured medical devices that are infected by malware can disable a device from properly performing its clinical function and could lead to a patient safety concern.

For example, malware could make a medical device unusable, vulnerable to denial of service attacks or silent failures, in which the device remains usable but is not doing what the physician is telling it to do. Also, many medical devices continue to run Windows XP or unpatched versions of Linux, which leaves entire hospitals vulnerable to an infection of malware that could disrupt, injure, and even kill.

FDA is working hard to raise awareness of the issue with a critical step called “Cyberhygiene”. Cyberhygiene is meant to protects patient from the threat of malware infections the same way hand-washing and other sanitary measures protects patients from microbial infection. Further, FDA is requesting that manufactures publish a coordinated vulnerability disclosure policy, which helps independent researchers who aspire to improve device security.

Main security hygiene issues Covered Entities and Business associates may need to consider the following issues.

- Medical devices may ship from the manufacturer with known weak default or hard-coded credentials, including administrative passwords. These passwords or credentials are easily discoverable by downloading the device manual from the manufacture’s website.

- Due to legacy systems and an inability to apply updates or patches on medical devices, various critical old medical devices are running unpatched operating systems that continue to be vulnerable to malware.

- There continues to be a lack of encryption being utilized on medical devices and their supporting systems and applications.

Resources:

Food and Drug Administration (FDA): http://www.fda.gov/MedicalDevices/default.htm