CALIFORNIA ASSOCIATION OF HEALTH FACILITIES – DISASTER PREPAREDNESS PROGRAM

Sitting Ducks: How to Prepare for a Cyber Attack on Your Facility

On February 5th, 2016, Allen Stefanek, CEO of the North Hollywood Presbyterian Hospital received an urgent phone call. Earlier that day, anonymous hackers infected his facility's life-saving medical devices with a ransomware device that encrypted all of the hospital's patient health information – and they demanded payment, by an untraceable online currency, before giving him the decryption code.

"The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this," Stefanek said in a public statement, after he sent 40 Bitcoin, the equivalent of $17,000 USD, to the hackers via the Internet.

The case of North Hollywood Presbyterian is not isolated – hacking an outdated, unprotected information system is low-hanging fruit for hackers, and there is a sharp increase in hacking incidents in the healthcare world. According to the Department of Health & Human Services' Office of Civil Rights (OCR), 1 in 10 Americans have been affected by healthcare record breaches; there were 113,000,000 medical records breached in 2015, a tenfold increase since only 2014!

Besides ransomware, in which all devices are locked and inaccessible, hackers can also remain undetected in your network for years, harvesting patients' data and records. According to the OCR, 29% of records are used to obtain healthcare services, 28% to obtain prescription drugs, and 26% to defraud Medicaid/Medicare. These staggering numbers have led to an increased interest in cyber liability insurance, which addresses the fallout of a data breach. There are many ways to take action, however, and subject matter experts recommend a multi-pronged mitigation plan.

<u>To take immediate action:</u>

- Check that the computer networks are configured to minimize unauthorized/outside access.
- Check that the network's physical infrastructure (routers, cables, etc.) are in secure locations.
- Limit wireless access to the network that hosts the information systems – wireless devices are more easily hacked.
- "Clean up" passwords that may be saved on computers that are not regularly used; disconnect from the network those devices, such as printers, that do not have password protection.

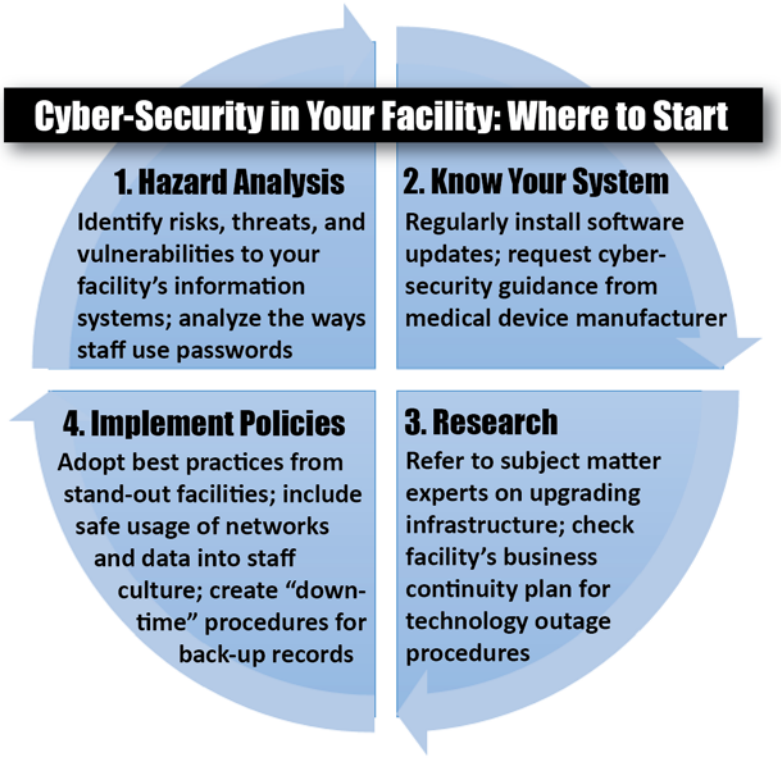
<u>The Food and Drug Administration has released guidelines to medical device manufacturers about cyber security mitigation. The manufacturer may be able to share some of this information:</u>

- Does my device allow different facility roles (administrator, caregiver, nurse) to have varying degrees of access to network information?
- My device has a "hard-coded" password, which is the same for each device in my facility, difficult to change, and vulnerable to public disclosure. Is it possible to change this password, preferably twice a year?
- Does my device have any settings or features that detect security compromises so they are recognized, and addressed swiftly?
- Does my device have the ability to continue to operate, even when the device's cybersecurity has been compromised?

Sitting Ducks: How to Prepare for a Cyber Attack on Your Facility

- Does my device provide methods for retention and recovery of device configuration, by an authenticated privileged user?
- Do you have the hazard analysis, mitigations, and design considerations that address the cybersecurity risks of this device?
- Do you have a summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of this device, to continue to assure its safety and effectiveness?

A cyberattack on a health facility is devastating to both operations and reputation. A multi-pronged plan is the key to success - because hackers target weak links, all of the facility's personnel must buy-in and participate in the new cybersecurity policies at their facility. Cybersecurity is the latest threat to long-term care facilities – however, by updating security policies to apply to the Digital Age, this risk can be prevented altogether.



Sources:

1. Office of the Food & Drug Administration, HHS. "Draft Guidance for Sponsors, Industry, Researchers, Investigators, and Food and Drug Administration Staff: Certifications to Accompany Drug, Biological Product, and Device Applications/Submissions." Biotechnology Law Report 27.4 (2008): 336-37. 2 Oct. 2014. Web. 30 Jan. 2017.

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

2. Office of the Secretary, HHS. "Breach Notification Rule." HHS.gov. U.S. Department of Health and Human Services, 26 July 2013. Web. 30 Jan. 2017.

   https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

3. Office of the Secretary, HHS. "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals."HHS.gov. U.S. Department of Health and Human Services, 26 July 2013. Web. 30 Jan. 2017.

   https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

4. Winton, Richard. "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating." Los Angeles Times. Los Angeles Times, 18 Feb. 2016. Web. 30 Jan. 2017.

   http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html