National Health Information Sharing and Analysis Center

NH-ISAC Monthly Newsletter March 2016

A Tale of Seatbelts and Breathing Air Bottles — a Healthcare Analog

The seat belt was invented over 150 years ago and yet seatbelt laws were not prevalent until the mid-1970's. Why so long? To be blunt, in safety system circles the term is "Blood Priority"; nothing gets done until casualties reach a threshold of concern. Then the "tombstone technology" boom explodes. As we have seen, we have gone from simplicity, to the shoulder restraint and airbag. The latest being the Radio/Bluetooth remain inoperative until belts are fastened... Nice Touch!

Conversely, the single greatest reasonable threat to passenger aviation is smoke inhalation during evacuation. We've all had to sit through the exit door drills when we fly. There was serious discussion about placing smoke hoods or air bottles on every flight and might have happened had not reality set in. It would be heavy, expensive, and probably would not work with untrained passengers! And so…

As we are all aware, the ransomware attack at Hollywood Presbyterian Medical Center has now shown non-cyber professionals what we already knew…the risk is credible.

As a matter of patient safety, we might have crossed the Rubicon so to speak. Some surgeries had been postponed and certainly there was a disruption in hospital management. It may be just a matter of time before a cyber-attack leads to healthcare casualties with the inevitable prime time media coverage and pundits. The question then is will the "Blood Priority" arrive with thoughtful processes appropriate to the threat, or will well intended reactionary laws or regulations impact our sector.

Until the day of the magic super cyber fix, our healthcare sector and patient interest is best served by sharing practices and threats in the timeliest manner. NH-ISAC tools such as Soltra and Sentinal help greatly to fill that niche. If we leave it to legislation the fix might be intolerable. Just think how you almost had to practice donning a plastic bag over your head after boarding your flight to DC!

By Edward Brennan, Director of Operations, NH-ISAC

Pharmaceutical Cybersecurity Threats and Solutions

A free interactive forum
Hosted by NH-ISAC and MERCK
in collaboration with SAFE-Biopharma Association and Churchill & Harriman

8AM-5PM (ET), Wednesday, March 23
Merck Corporate Conference Center

Register early!
Seating capacity is limited.

Please join us for a No Host Dinner, Tuesday, March 22

Includes: Breakfast, Lunch and Post-Forum Reception

Top 10 Health Related Cyber Events Summary

Hospital Pays $17,000 Ransom to Get Access Back to Its Encrypted Files
Ransomware Hits Hospitals

Memphis Man Accused of Using Stolen Patient Identity Information to Defraud Banks of $1.6 Million

Judge Allows Some Claims Over Anthem Data Breach to Go Forward

Flint Hospital Confirms 'Cyber Attack,' Anonymous Threatens Action Over Water Crisis

Mont. Facility Reports Healthcare Data Breach Affecting 28K

Centene Discloses Missing Hard Drives Contain Personal Information of 950,000 People

St. Luke's Hospital Reports Possible Data Breach Involving Patients' Info

Berkshire Health Systems plagued by malware; patient, payment data safe

Home Health Provider to Pay $240K in HIPAA Violation Fines

91K Patients' Data Compromised in WA Healthcare Data Breach

NH-ISAC is pleased to publish a monthly member newsletter. The newsletter is designed to bring events and other important ISAC information to your attention. If there is something you would like to see included email:
contact@nhisac.org

Recent Rise in Ransomware

Ransomware has been on the rise in the health sector over the past few months and campaigns with names like "Locky", "CrytoWall", "CrytoLocker", and "SamsamCypt", have been proliferating the news. Ransomware can take many forms, but is essentially similar in style. According to TrendMicro - ransomware is a type of malware that prevents or limits users from accessing their systems and/or data. This malware forces its victims to pay a ransom through certain online payment methods in order to be granted access to their systems, or get their data back. Some ransomware encrypt files, while others use TOR to hide C&C communications. Organizations can be infected via malicious emails with links and/or attachments; or, as with SamsamCypt, infected via a JBoss application vulnerability, that allowed hackers to encrypt system files. Using this web application vulnerability was particularly new to the health sector.

A recent case involved Hollywood Presbyterian Hospital (see top Cyber Event on 1st page), and though few specific details have emerged, the hospital was victimized by malicious ransomware that proceeded to encrypt files on multiple systems, then demand that the organization pay a ransom of 40 bitcoins ($17,000US) to receive the ransom key. The hospital did pay the ransom and the systems were in the process of being restored.

What can you do? There are many steps that can be taken to increase security from these types of malicious activities:

- Provide adequate staff training on correct and secure email usage.

- Backup all systems and make sure they are recent backups. Systems can be restored if infected.

- Patch and update as soon as possible.

- Set proper Admin and non-Admin rights on all systems, and restrict user access

- Filter out macro enabled email attachments - since recent versions of ransomware runs via a macro on an attached file, removing these from emails could prevent infection.

- Apply strong endpoint protection / perimeter defenses.

- It is recommended that organizations initiate a review of web applications in their respective environments and upgrade outdated JBoss versions to 7.x

Finally if you see any malicious activity on your network, share those indicators with NH-ISAC or other members so that they may prevent the same issues on their systems. Want to know more? Visit the recorded webinar NH-ISAC recently hosted on Locky and SamsamCrypt.

MEDICAL DEVICE WORKSHOPS:

- **Stanford Health Care - April 7 (Palo Alto, CA)**
- **Kaiser Permanente June 8 (Denver, CO)**
- **Texas Health - July 19 (Dallas/Ft. Worth, TX)**
- **Hospital Corp. of America August 15 (Nashville, TN)**
- **Mayo Clinic - September 26 & 27 (Rochester, MN)**

MARK YOUR CALENDARS:

NH-ISAC AND AVIATION ISAC SPRING SUMMIT WILL BE ON MAY 11-13 AT
Lake Buena Vista, FL

Early Bird Registration ends March 15th.

Are you on the NH-ISAC Member Listserv?

If you are not already participating, NH-ISAC has a members only listserv-based email system for you to send other NH-ISAC members questions, concerns, notifications, or other items that would benefit the broader membership. Items currently shared include updates to malicious Angler EK-based sites, phishing emails, wire fraud emails, and general questions to the membership. As an NH-ISAC member, anyone is allowed to join the lists that are available. NH-ISAC continues its efforts at creating a secure community for information sharing and collaboration. We look forward to your participation in all of our efforts!
Please email NH-ISAC directly with any questions.

Cybersecurity Post Market Guidance Public Comment Period

The public comment period for the recently released "Post Market Management of Cybersecurity in Medical Devices" (http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf) draft guidance is open. All stakeholders are encouraged to provide comment by April 21, 2016 to the docket of the Federal Register Notice at:

(www.regulations.gov docket number 2016-01172).