National Health Information Sharing and Analysis Center

NH-ISAC Monthly Newsletter May 2016

Dare to Share!

We all are bombarded daily by myriads of blogs, abstracts, white papers, op-eds and straight out advertising touting current security threats and trends.

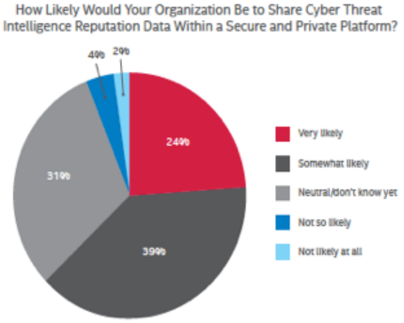
A report from Intel/McAfee Labs, *"McAfee Labs 2016 Threat's Predictions Report",* published in November 2015, which focused on the topic of Cyber Threat Intel (CTI) caught my eye.

Intel security interviewed close to 500 security practitioners to explore views, predictions and forecasting cyber threats into 2016.

Two "takeaways" I feel are still relevant in Q2 of 2016:

1. The lack of awareness or ability to capture CTI. The HITECH act of 2009, coupled with the 2009 Federal HIT Stimulus drove a buying frenzy in Healthcare IT - at the expense of the requisite investment in cybersecurity. This created enterprise vulnerabilities because already tight budgets lacked appropriate security resourcing.

2. Inexplicably, the laggard adoption rate of CTI sharing.
63% of McAfee's respondents claimed they are "Very Likely to Somewhat Likely" to share CTI within a secure and private platform. (See Pie Chart)



With the obvious havoc that recent ransomware attacks such as "Locky" rendered on various community hospitals and a large regional health plan, it seems the willingness to share CTI should be 100%. In theory, CTI sharing is a non-budget line item and it can occur with little or no associated cost.

If you have colleagues or friends who are not currently engaged in information sharing, please do them a favor. Give them our website address to begin the dialogue.

Tell your friends, it's not about membership fees. We are a member driven non-profit organization and *community*. As you know it's about gaining access to NH-ISAC's over 800 security analyst network, who are all watching out for each other and who are sharing information around threats, vulnerabilities, incidents, mitigation strategies and best practices. Together let's help the sector to help all of us!

By Steve Hunter, Director of Marketing, NH-ISAC

We hope you are looking forward to a dynamic, information packed summit!

LET'S TALK. LET'S SHARE. LET'S NETWORK.

Top 10 Health Related Cyber Events Summary

Computer Virus Possibly Exposes PHI in Healthcare Data Breach

More Hospitals Affected by Healthcare Ransomware Attacks

Personal Laptop, Possibly Containing Data On 5M Patients, Stolen from HHS Facility

Einstein Health Suffers Possible Patient Data Breach

Health Care Agency Owner Accused of Stealing Clients' Personal Information

American College of Cardiology Breach Affects 1,400 Institutions

Unsecured Database Leads to Potential Healthcare Data Breach

Alabama CVS' Patient Information at Risk After Laptop Stolen

Pain Treatment Centers of America Notifies 19,397 Patients of Bizmatics Breach

2,400 members' info stolen, Kaiser Permanente says

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

Medical Device Workshop at Stanford Health Care

The NH-ISAC, MDISS and Stanford Health Care hosted a Medical Device Security Workshop on April 7, 2016. The workshop was held at the Quadrus Conference Center in Menlo Park, CA. The event was kicked off the night prior to the workshop with a social event that included hors d'oeuvres and beverages hosted by Stanford Health Care. Ms. Monica Gupta, Associate CIO, Stanford Health Care; Ms. Denise Anderson, President, NH-ISAC; and Dr. Dale Nordenberg, Executive Director, MDISS provided opening remarks. The workshop began at 9:00am and concluded at 4:30pm. The topics at the workshop included:

- Current Threats in the Medical Device Landscape
- Patient Harm? Analyzing Cyber Security Vulnerabilities for Patient Safety Issues
- Bill of Materials – Role of Manufacturers and What is Needed
- Driving Security Throughout the Medical Device Life Cycle
- Public Key Infrastructure – Security Solution for Connected Medical Devices
- NH-ISAC: A Case for Information Sharing
- Medical Device Information Sharing Programs: Operations Optimization and Critical Infrastructure Protection
    - MD-Risk Assessment: Crowdsourcing for Efficiency, Quality and Safety
    - MD-Vulnerability Sharing and Threat Intelligence

Mr. Harvey Fortune, Assistant Director, Clinical Technology & Biomedical Engineering, Stanford Health Care provided closing remarks. Many workshop participants met at Joya restaurant to continue networking after the conclusion of the workshop. The networking, interaction and exchange was fantastic. Plan to attend the upcoming workshop(s) today.

MEDICAL DEVICE WORKSHOPS:

- Kaiser Permanente June 8 (Denver, CO)
- Texas Health - July 19 (Dallas/Ft. Worth, TX)
- Hospital Corp. of America August 16 & 17 (Nashville, TN)
- Mayo Clinic - September 26 & 27 (Rochester, MN)

Registration Now Open for our next Medical Device Workshop:

Wednesday, June 8, 2016
8:30am – 4:30pm (MT)

Breakfast and Lunch Included

Be sure to join us for a no host dinner the night before on Tuesday, June 7.

Details to be sent upon registration.

Kaiser Permanente
6560 Greenwood Plaza Blvd
Greenwood Village, CO

Click Here to Register

NH-ISAC is starting a Provider Special Interest Council.

The goal is to create a group to share ideas and generate white papers as well as new solutions to address the new technology within the provider community.

- Establish (or adopt) a minimum standard for cyber security
- Establish best practices for the latest technologies such as tele-health technology and smart hospitals.
- Assist with supporting the smaller provider organizations
- Increase the share of methods for cyber security and data protection
- Develop patient/employee friendly cyber security approaches
- Assist with training and awareness campaigns

This collaboration will help the community improves its overall cyber security posture and improve its interaction with patients.

The inaugural meeting of the Providers Special Interest Council will be at the Spring Summit in Orlando. For more information, please email contact@nhisac.org.

NH-ISAC Analyst Calls…..

If you are not already participating, the NH-ISAC hosts a member analyst call every month. Usually scheduled for the last Wednesday or Thursday of the month, this call is an open forum for all NH-ISAC Members to be able to speak to other analysts and share information and ideas. A calendar invite is sent out about a week before the event via the NH-ISAC email list.

Currently, we have a small team who help create a rough agenda each month to guide the discussion.

The March analyst call started with an overview of Cyber Health world events, a CyberStorm review and as always, allowed our members to discuss events they have been seeing within their own organizations, including ransomware, current events and malicious activity.

If you are interested in joining this group, please email contact@nhisac.org to discuss.

We are looking forward to hearing from you on this month's Analyst Call.