



NH-ISAC

DARE TO SHARE



Are you taking advantage of all NH-ISAC Services?

Your days are busy, so you most likely missed an email from us about a new Service offered through NH-ISAC. As a member, these services are free or reduced in price, we hope you take advantage of them to better assist your security posture.

- A. **Email Lists** - Both of these email lists available to members - Members list for daily briefings and alerts, Amber List for member to member communication. Please email us to be added to either list.
- B. **Soltra Automated Information Sharing** - Receive a data feed of intel directly into your SIEM or local STIX based tool. Data feeds consist of NH-ISAC Member, DHS and US-Cert, Australian Cert, and our intelligence partners data sets. You can email us directly to get access.
- C. **Perch Security** - A Managed Service that allows our members to view, detect, and share the threats. View more information on our website - <https://nhisac.org/perch/>
- D. **Digital Stakeout** - Free IP/Domain range monitoring service. Collect, enrich, and analyze digital data sourced from social, surface, deep, and dark web, and proprietary sources. More information can be found on our website: <https://nhisac.org/digital-stakeout/>
- E. **CYBERFIT** - a selection of services that can improve and facilitate your security operations, risk assessment, benchmarking, and legal and regulatory policy analysis. <https://nhisac.org/cyberfit/>
 - ◇ **Security Operations Service** - Services supporting your organization's security capabilities. Incident Response and Malware Analysis, Penetration Testing, Web Application Testing, Vulnerability Assessment, Vulnerability Management.
 - ◇ **Risk Assessment** - A shared risk assessment platform and vendor monitoring service for NH-ISAC Members
 - ◇ **Benchmarking** - Free online 83 question survey focused on 6 sections: spend, organization, operating model, strategy and tools, user education, open text.
 - ◇ **Legal and Regulatory Newsletters** - Free monthly newsletter focusing on updates in health care-specific regulation, legislation, and current key court rule changes in health care cybersecurity and privacy.

Top 10 Health Related Cyber Events for October:

[Community Memorial Health System In Ventura Suffers Data Security Breach](#)

[ShadowBrokers are Back Demanding Nearly \\$4m and Offering 2 Dumps Per Month](#)

[Ransomware Attack May Impact 19K Oncology Hematology Patients](#)

[Smiths Medical to Patch Serious Flaws in Syringe Infusion Pumps](#)

[The Equifax Breach: What You Should Know](#)

[ICS-CERT Reports Medfusion Medical Device Vulnerabilities](#)

[CCleaner targeted top tech companies in attempt to lift IP](#)

[SMART Physical Therapy hacked by TheDarkOverlord](#)

[Deloitte hit by cyber-attack revealing clients' secret emails](#)

[73 Percent of Medical Professionals Share Passwords for EHR Access](#)

Did you miss this webinar?

Intel Security Readiness Program

NH-ISAC hosted David Houlding of the Intel Security Readiness Benchmarking service. Our members participated in a 1-hour online workshop that walked them through 42 questions.

You can still participate - and the best part - there is **zero cost**. Members can view the webinar at this link - <https://attendee.gotowebinar.com/recording/4967780835859406339>. If you care to read more about the program, please visit Intel.com/SecurityReadiness, or you can email David Houlding directly at david.houlding@intel.com.

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



Business Email Compromise Workshop

Registration - <https://nhisac.org/events/nhisac-events/business-e-mail-compromise-workshop/>

Business Email Compromise (BEC) has become a significant threat to U.S. businesses and individuals.

Since October 2013, the Federal Bureau of Investigation has identified victims from 131 countries and a global monetary exposure of over \$5 billion dollars as a result of BEC fraud.

Business leaders, please plan to join us for this important opportunity to learn about a very real & proliferating cybersecurity threat. Cybersecurity experts from the FBI, US Secret Service and private sector will be sharing their experiences & expertise around BEC, why you should be concerned and how you can protect against becoming the next victim.

Workshop Topics:

- Describe BEC
- Current threat landscape
- Tactics, techniques & procedures used by the criminals
- Discuss why situational awareness & information sharing are important
- Offer strategies to help protect your organization from BEC attacks

Locations: San Francisco, CA; Seattle, WA; Kennedy Space Center, FL; Akron, OH; Phoenix, AZ; Denver, CO; Nashville, TN; Kansas City, MO; Boston, MA

Registration - <https://nhisac.org/events/nhisac-events/business-e-mail-compromise-workshop/>

Event presented by

The FBI, United States Secret Service, Multi-State Information Sharing and Analysis Center (MS-ISAC), National Health Information Sharing and Analysis Center (NH-ISAC), Research and Education Network (REN-ISAC), Retail Cyber Intelligence Sharing Center (R-CISC), and Symantec

Mark Your Calendars For the Upcoming Workshops:

Biotech/Pharma Security Workshop at MSD

Tuesday, November 7, 2017
Workshop: 8:30am – 5:30pm
(local time)

Breakfast and Lunch Included

MSD

**Na Valentine 3336/4, Prague 5,
Czech Republic**

[**Click Here to Register**](#)

October:

Health IT Summit - Sheraton
Raleigh, NC, October 19

Business E-mail Compromise
(BEC) Workshop - Foster City,
October 13

November:

Health IT Summit - Beverly Hills
Hotel Los Angeles, CA,
November 9

The Education Committee is working on the following two activities that will help boost NH-ISAC membership and add value for existing members:

- A scholarship program starting in 2018, initially targeted at recruiting new tier 1, non-profit organizations, offering a year of membership and attendance at one of the summits
- Monthly security master class webinars where members present on emerging or in demand technology and security topics to help advance knowledge sharing. The very first one in the series will be on October 13th at 2pm EST. Please go to <https://attendee.gotowebinar.com/rt/7432292170023761921> to register



Cyber Rodeo

Plan to Arrive Early!

Cyber Outbreak

An Exclusive Cybersecurity Tabletop Exercise
Monday, November 27, 2017 2-5 pm

NH-ISAC is officially launching a new sector-wide exercise series, *Cyber Outbreak*. The first exercise in the series will take place in person on the afternoon of Monday, November 27 in advance of the NH-ISAC fall summit.

The exercise scenario will examine potential threats to the manufacturing processes in the Pharmaceutical and Medical Device industries and the impacts that might have on patient care.

The table-top exercise will test the sector's incident response and information sharing capabilities. Results will be documented and shared in an after-action report, but individual player contributions will be non-attributable and off the record.

Representatives of companies from all sub-sectors are invited to participate. The first 30 members to RSVP will be registered as players, while subsequent RSVPs will be invited to join the exercise as observing participants.

Deadline to register is November 18, 2017 or until seats are full. If you would like to join the planning team that is developing the scenario, please mail exercise@nhisac.org.

We look forward to seeing you at this exercise and future Cyber Outbreak events!

Hotel Reservations must be made on or before the cut-off date of Tuesday, November 7, 2017 to be eligible for the group rate.