

Hacking Healthcare

Policy Analysis on Info Sharing

Last week, we started diving deeper into HHS' newly formed Health Cybersecurity and Communications Integration Center (HCCIC). We looked at how it might improve the security of HHS systems themselves. This week let's look at how the HCCIC will work with DHS' National Cybersecurity and Communications Integration Center (NCCIC) and the other government agencies.

For HCCIC to add value to the already crowded government information sharing space, it needs to bring unique skills or capabilities *and* integrate those capabilities into the existing structure. For instance, the HCCIC will not add value if it just seeks to put out additional bulletins that are similar to what the NH-ISAC or NCCIC have already released. The information sharing community is awash in bulletins when new incidents occur. Just look at the recent ransomware and destructive malware attacks as an example.

As always, become a member of the NH-ISAC for full in-depth analysis each and every week.

Next week, we will close out our first look at the HCCIC by discussing how the new center will work with the NH-ISAC itself.

The Week Ahead –

Congressional Activity

- [HHS Appropriations Markup](#) (7/19 - House Appropriations)
- [Hearings to examine an update on FirstNet](#) (7/20 - Senate Commerce)
- [Business Meeting to consider nomination of Christopher Wray as FBI Director](#) (7/20 – Senate Judiciary)
- [Examining Bipartisan Legislation to Improve the Medicare Program](#) (7/20 – House Commerce)
- [21st Century Medicine: How Telehealth Can Help Rural Communities](#) (7/20 – House Small Business)

Conferences

- [2nd Annual Medical Device Cybersecurity Risk Mitigation](#) (7/17-18)
- [Health IT Summit - Denver, CO](#) (7/18-19)
- [Medical Device Coordinated Disclosure Tabletop Exercise TTX](#) (7/19)
- [DHS Active Shooter Preparedness Workshop - Various Dates/Locations](#) (7/19)
- [Black Hat](#) (7/22-27)
- [DEF CON 25](#) (7/27-30)
- [Free GCA DNS Webinar by Global Cyber Alliance](#) (7/26)
- [Basic Best Practices in Cybersecurity – Nebraska](#) (NH-ISAC) (7/26)
- [Basic Best Practices in Cybersecurity – Washington](#) (NH-ISAC) (8/2)
- [SANS Security Awareness Summit – Nashville](#) (8/2-3)
- [Free DMARC Webinar by Global Cyber Alliance: Brand Protection](#) (8/2)

Hot Links –

- [Top 3 Essentials in Preparing for Ransomware Attacks](#) (Health IT Security)
- [Patient Safety Critical Part of Healthcare Information Security](#) (Health IT Security)
- [Applying Healthcare Information Sharing to Data Security](#) (Health IT Security)
- [How Security Pros Can Help Protect Patients from Medical Data Theft](#) (Dark Reading)
- [Only Half of Healthcare Professionals Report Their IT Infrastructure Is Safe from Cyber Attacks](#) (HealthcareInformatics)
- [Hospitals to receive £21m to increase cybersecurity at major trauma centres](#) (The Guardian)
- [Adobe, Microsoft Push Critical Security Fixes](#) (Krebs)
- [Zero-Day Exploit Surfaces that May Affect Millions of IoT Users](#) (DarkReading)
- [Experts in Lather Over ‘gSOAP’ Security Flaw](#) (Krebs)
- [3 things to know about GSA’s proposed CDM SIN](#) (cyberscoop)

Speeches –

- [SEC Chairman Jay Clayton’s Remarks at the Economic Club of New York](#)
 - “As a final comment on enforcement, I want to go back to cybersecurity. Public companies have a clear obligation to disclose material information about cyber risks and cyber events. I expect them to take this requirement seriously. I also recognize that the cyber space has many bad actors, including nation states that have resources far beyond anything a single company can muster. Being a victim of a cyber penetration is not, in itself, an excuse. But, I think we need to be cautious about punishing responsible companies who nevertheless are victims of sophisticated cyber penetrations. Said another way, the SEC needs to have a broad perspective and bring proportionality to this area that affects not only investors, companies, and our markets, but our national security and our future.”

Reports –

- [Machine Learning Raises Security Teams to the Next Level](#) (McAfee)
- [Petya used to destroy evidence of espionage?](#) (BoozAllen)
- [ICS-CERT 2016 Annual Assessment Report](#)
- [Reducing IT Friction Can Boost Government Workforce Productivity](#) (fedscoop + vmware)

Podcasts –

- [Former Estonian President Toomas Hendrik Ilves on Russia, Fake News, and Twitterbots](#) (CipherBrief)

Sundries –

- [DHS sorts through 'mountain' of data on energy cyberthreat](#) (E&E News)
- [Australian companies under 'constant' cyber attack, says security company CrowdStrike](#) (ABC)
- [GCHQ Says Hackers Have Likely Compromised UK Energy Sector Targets](#) (motherboard)

- [UAE orchestrated hacking of Qatari government sites](#) (WP)
- [Dow Jones Inadvertently Exposed Some Customers' Information](#) (WSJ)
- [Elon Musk says preventing a 'fleet-wide hack' is Tesla's top security priority](#) (electrek)
- [Extreme cyber attack could cause \\$120bn in economic damage](#) (FT)
- [Russia, China vow to kill off VPNs, Tor browser](#) (The Register)
- [The Russians Will Be Back. Will We Be Ready?](#) (Politico Mag)
- [South Carolina May Prove a Microcosm of U.S. Election Hacking Efforts](#) (WSJ)
- [Is It A Crime?: Russian Election Meddling and Accomplice Liability Under the Computer Fraud and Abuse Act](#) (LawFare)
- [White House reveals contact info on voters concerned about privacy](#) (SC)
- ['It was always going to happen': Inside the cyber-attack on parliament](#) (bbc)
- [DHS S&T cyber division hitting its stride with research transition, start-up projects](#) (FederalNewsRadion)
- [House extends law streamlining federal IT systems](#) (the Hill)
- [Military cyber operations headed for revamp after long delay](#) (AP)
- [Nations, Even Adversaries, Must Work Out Cyber Issues - Carefully](#) (Cyber Brief)
- [Wyden pushes DHS to adopt DMARC](#) (SC)
- [More on the NSA's Use of Traffic Shaping](#) (Schneier on Security)
 - [Deep-dive](#) (TCF)

(In)Secure Takes –

Jennifer @jfost75 · 20h ▼
 Deadline extended to August 1st!

NH-ISAC @NHISAC
 Call for papers deadline is tomorrow 7/14 for NH-ISAC Fall Summit. Go to nhisac.org/events/cyber-r...
 #NHISACFall17

🗨️ ↻ 1 ❤️ ✉️

Contact us: follow us @NHISAC @flatgard and email us at bflatgard@nhisac.org