Hacking Healthcare

Policy Analysis on Info Sharing

We now have the HCCIC to add to the NCCIC on the list of relevant government acronyms in healthcare cybersecurity. Just how they work with one another remains to be seen, but let's look at what we know so far.

First, the Health Cybersecurity and Communications Integration Center (HCCIC) has three stated goals:

- "Strengthen engagement across HHS Operating Divisions;
- Strengthen reporting and increase awareness of the health care cyber threats across the HHS enterprise; and,
- Enhance public-private partnerships through regular engagement and outreach."

It is striking, given the press coverage and general sentiment in the sector, to see HHS position the HCCIC as being primarily responsible for internal security improvements. Given that positioning, it is unsurprising that the HCCIC has been headquartered under the HHS CISO's office and not in an operating unit with a primarily external facing mission. Location within the CISO's office also makes a lot of sense from a technical perspective – HHS was one of the first agencies to connect with the Automated Indicator Sharing (AIS) system at DHS. The CISO's office pursued AIS to bolster its own defenses and can utilize the AIS pipes to feed information into the HCCIC (and from the HCCIC back to DHS).

Much of the focus on government cybersecurity has been around adoption of shared services and migration to a more defensible technology stack. This is rightly placed and the security (and efficiency!) burden of legacy systems is significant. But there is also a burden of legacy governance in government security programs. Staff and budget are disparate and suffer from a lack of consolidation and scale. It is difficult to align IT and security modernization efforts within departments and across government. Coordinating centers such as the HCCIC may offer some benefit in this regard.

HHS (and other agencies) should be encouraged to try innovative approaches to addressing their own security challenges. For the HCCIC (and other such initiatives) to be successful, it will need to be properly resourced. But the challenge of securing government systems is so significant that experimentation and action (above all else) should be encouraged.

Over the next couple of weeks, we will look at how the HCCIC might look to utilize their relative expertise and work with the NCCIC and NH-ISAC to maximize value in support of the health care sector.

International Engagement

President Trump and President Putin did find time to sit down last week. And, as we speculated -- "the" cyber was discussed in great length. Unfortunately for those of us concerned with the safety and security of the American health care system, the discussion reportedly focused on the election hacking and not on recent attacks against critical infrastructure.

While it is a positive development to see world leaders talking about cybersecurity, the nature of this conversation and its reported outcomes seem to be insignificant at best and damaging at worst. Insignificant because a broad and open-ended commitment to form a bi-lateral cybersecurity unit doesn't commit either side to achieving anything (as opposed to our proposed investigatory effort). Dangerous because Russia, and other countries, can use this meeting and commitment to legitimize their own activities, while diverting attention and effort from important ongoing international engagements, such as the Governmental Group of Experts working group that dissolved last week (see below for articles on this).

Multi-lateral engagement on cybersecurity hangs in a precarious balance. Governments seem to be pulling back from international partnership and dialogue, just at the time when we need them to be most involved. Individual jurisdictions are writing their own rules on everything from encryption to data localization. Regulators are developing unique frameworks and requirements. And companies are increasingly comfortable sharing source code with domestic security services.

We will continue to ponder this challenge in the months ahead, but for now let's look at the other health care cybersecurity news of the week.

The Week Ahead –

Administration Announcements

- DHS Awards Info Sharing Grant

International Organizations

- The Global Commission on the Stability of Cyberspace is soliciting research proposals

Congressional Activity

- Confirmation Hearing – David J. Glawe to be DHS Under Secretary for Intelligence and Analysis (7/11 – 10:00am)
- Confirmation Hearing - Christopher A. Wray to be Director of the FBI (7/12 – 9:30am)
- FY 2018 Homeland Security Appropriations Markup (7/12 – 4:30pm)

Conferences

- Medical Device Workshop at UC San Diego (NH-ISAC) **(Sold Out)** (7/13)
- SANS Los Angeles-Long Beach (7/10-7/15)
- BSides Chicago (7/15)
- 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)
- Basic Best Practices in Cybersecurity – Nebraska (NH-ISAC) (7/26)
- Basic Best Practices in Cybersecurity – Washington (NH-ISAC) (8/2)

Hot Links –

- U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks (WaPo)
- Foreign hackers probe European critical infrastructure networks: sources (Reuters)
- Russians Are Suspects in Nuclear Site Hackings, Sources Say (Bloomberg)
- Foreign hackers probe European critical infrastructure networks: sources (Reuters)

- Health IT Organizations Urge Congress to Increase NIST Funding (Healthcare Informatics)
    - The letter
- Legislators Introduce Bill to Ease Meaningful Use Requirements (Healthcare Informatics)
- HIPAA Regulations Not Applicable in TN Supreme Court Case (HealthITSecurity)
- DHS Updates on Federal Network Cybersecurity, Infrastructure (HealthITSecurity)

Reports –

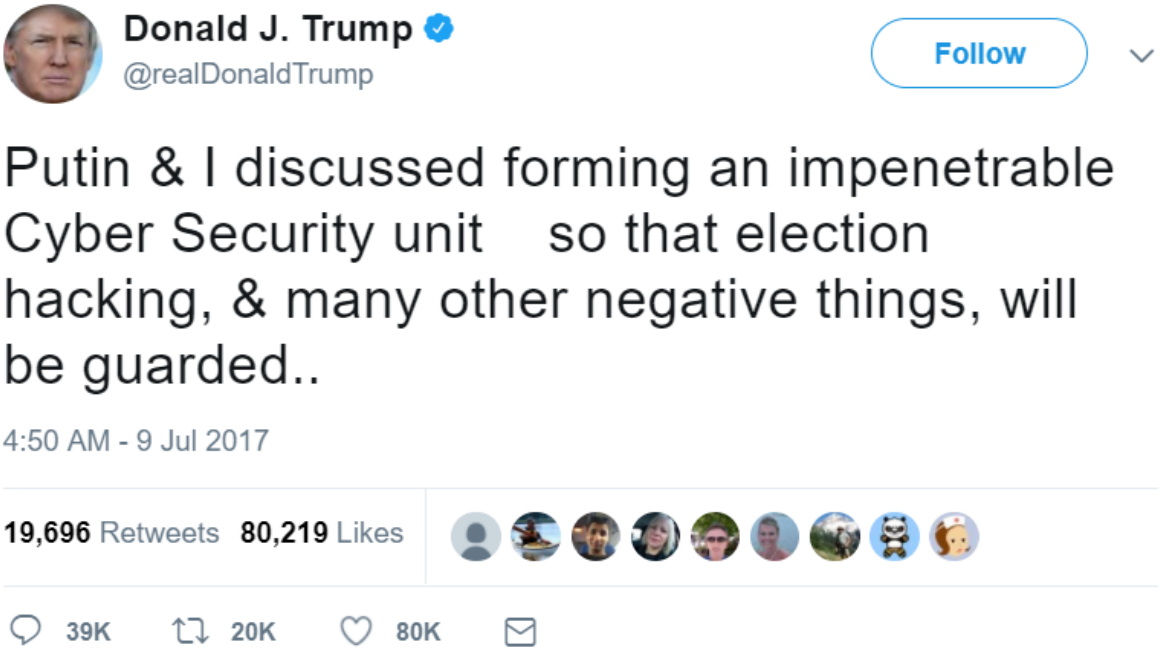
- June 2017 Healthcare and Cross-Sector Cybersecurity Report (Vol. 12) (HIMSS)
- Global Survey: 95 Percent of Healthcare Orgs Don't Use Security Governance or Risk Management Software
    - The report: 2017 IT Risks Report (netwrix)

Sundries –

- International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms (Just Security)
    - Statement by Michele Markoff, US representative to the GGE
- The UN GGE Failed. Is International Law in Cyberspace Doomed As Well? (LawFare)
- Moving Forward on Cyber Norms, Domestically (LawFare)

- Trump's cyber tweets cause dismay, confusion (Politico)
- Trump White House Has Taken Little Action To Stop Next Election Hack (NBC)
- iPhone Bugs Are Too Valuable to Report to Apple (Motherboard)
- Hacker Who Aided Russian Intelligence Is Sentenced to 2 Years (NYT)

(In)Secure Takes –



Daniel Lin
@danwlin

Follow

LEIA: Tarkin & I discussed forming an impenetrable Death Star prevention unit so that planetary destruction & many other negative things...

> **Donald J. Trump** @realDonaldTrump
> Putin & I discussed forming an impenetrable Cyber Security unit so that election hacking, & many other negative things, will be guarded..

8:23 AM - 9 Jul 2017

313 Retweets **764** Likes

14 313 764

Donald J. Trump
@realDonaldTrump

Follow

The fact that President Putin and I discussed a Cyber Security unit doesn't mean I think it can happen. It can't-but a ceasefire can,& did!

5:45 PM - 9 Jul 2017

19,153 Retweets **86,243** Likes

28K 19K 86K

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