October 24, 2017

Hacking Healthcare

Welcome back to *Hacking Healthcare!*
TLP White

Hot Links –

1. Don't poke the Bear: DHS has warned critical infrastructure operators that Russian hackers are targeting U.S. critical infrastructure firms and looking for access to systems. Their goal: gain access to ICS/SCADA systems. While healthcare organizations have not been named as targets, it would be surprising to learn that the sector wasn't part of the Russian strategic plan. It is worth being vigilant to the attack TTPs out of caution, especially given other reporting on Russian targeting of cyber experts. The approach has been to access small vendors with poor security via spear-phishing and watering hole attacks and then leveraging trusted access to move across networks to core targets.
2. A different model for private sector support: An interesting report from ITIF that challenges the status quo for counterintelligence. The report places domestic cybersecurity as a subset of counterintelligence and looks at historical efforts by government to support the private sector with information and assistance. This goes back to FBI programs to prevent strategic industries during World War 2. It doesn't offer a panacea for how to fix the issue, but helpful to develop a dialogue in this space. The intelligence community has identified private sector engagement as a weak spot, but leadership has yet to articulate a model for addressing the problem. Public-private exercises, like the *Cyber Outbreak* series NH-ISAC is launching at its fall summit may be one way to develop good ideas for pilots in this space.

Congress –

Tuesday, October 24:

--Hearing: Joint Hearing entitled Public-Private Solutions to Educating a Cyber Workforce.
(House Homeland)

Wednesday, October 25:

October 24, 2017

--Hearing: Bolstering the Governments Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government (House Science)

--Hearing: Continuation of Hearing entitled "Examining the Equifax Data Breach" (House Financial Services)

Thursday, October 26:
--Hearings to examine advanced cyber technologies that could be used to help protect electric grids and other energy infrastructure from cyberattacks (Senate Energy)

Monday, October 30:
--Hearing: Examining Physical Security and Cybersecurity at Our Nations Ports (House Homeland)

Conferences and Webinars –
--Business E-mail Compromise (BEC) Workshop – Akron (NH-ISAC) (10/25)
--Business E-mail Compromise (BEC) Workshop – Phoenix (NH-ISAC) (10/26)
--Business E-mail Compromise (BEC) Workshop – Denver (NH-ISAC) (10/27)
--Business E-mail Compromise (BEC) Workshop – Nashville (NH-ISAC) (10/30)
--Biotec/Pharma Security Workshop at MSD, Prague (NH-ISAC) (11/7)
--Health IT Summit – LA (NH-ISAC) (11/9)
--Cyber Outbreak (NH-ISAC) (11/27)
--NH-ISAC Fall Summit – Cyber Rodeo (11/28-30)
--Health IT Summit – Dallas (NH-ISAC) (12/14)

Sundries –

--House Committee Presses Nuance Executives on NotPetya Attack (healthcare informatics)
--New Report: The Global State of Information Security® Survey 2018 (PWC)
--VA proposes CARE Act to address health IT problems (Healhtcare IT News)
--Report: Healthcare Organizations Struggle with Human Error in Securing PHI (healthcare informatics)

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