December 12, 2017

TLP White
2018 cybersecurity projections are in – this week's NH-ISAC *Hacking Healthcare:*

Hot Links –

1. **New NIST Draft** – NIST published[1] a "second draft of the proposed update" to its Cybersecurity Framework last week. Your comments are due to NIST by January 19, 2018.

   A quick history lesson -- the original Framework was released in February 2014. In winter 2015 and spring of 2016, NIST solicited feedback on the original version. In January of this year, they released a "first draft" of version 1.1.

   This "second draft" incorporates comments submitted over the last year to that first draft.

   The big changes are:

   - The inclusion of a robust new category in the "Identify" function around Supply Chain Risk Management.
   - New subcategories in Prevent-Access Control (PR.AC-6, 7) related to identity proofing and credential management, as well as device authentication.
   - A new subcategory (PR.DS-8) in Prevent-Data Security for verifying hardware integrity.
   - A new subcategory (PR.PT-5) in Prevent-Protective Technology that focuses on increasing system availability.
   - A new subcategory (RS.AN-5) in Respond-Analysis that addresses vulnerability disclosure and management.
   - A number of new reference standards, primarily from CIS and COBIT.
   - A refocusing of section 4 as "Self-Assessing Cybersecurity Risk with the Framework" which "better emphasize[s] how organizations might use the Framework to measure their risk", as Mike Barret of NIST has put it.[2]

[1] https://www.nist.gov/cybersecurity-framework/cybersecurity-framework-draft-version-11
[2] https://www.darkreading.com/cloud/nist-releases-new-cybersecurity-framework-draft/d/d-id/1330579?piddl_msgid=330189#msg_330189

2. **Security Spending –** A new study indicates security will be a priority investment for the largest U.S. health systems in 2018.[3] Nearly all (92 percent) of the roughly 20 respondents said that they would spend more money on security technology. Two-thirds said they would hire more security staff and 42 percent said they would hire more security executives. The focus of the investment is mostly on the "Identify, Protect, and Detect" components of the NIST Framework.

   Great to see the increased spend, but it would be interesting to see the efficacy of technology investment and how efficient that spending is when compared to staff and other risk management and resiliency investments. Does anyone have good data that looks into this? Please send along if you do.

   Also of interest in the study – an increased focus in 2018 on patient generated data, telehealth, and AI to drive clinical decision making. Notably, the study doesn't ask how security is considered when deploying these new technologies.

   Meanwhile, Healthcare IT News has some thoughts on the new technology that could make us more secure in 2018.[4]

3. **Security Threats** – And proving that we are in 2018 prediction season, McAfee Labs has released its 2018 Threats Predictions Report.[5] The good news is that McAfee's top threat for 2018 – ransomware – is well known to the healthcare sector. The bad news is that it is likely to get more disruptive and damaging. Denise Anderson, NH-ISAC President, suggests that "ransomware will continue to be a threat and evolve, not to just encrypting data, but also to blackmailing data owners based on the content of the data."[6] The McAfee report predicts ransomware moving beyond data and holding hostage business critical systems – or the networked personal devices of executives (a soft target[7]).

   Healthcare IT News has a wide ranging look at how we might combat destructive ransomware attacks: http://www.healthcareitnews.com/news/future-proofing-security-protecting-against-new-arsenal-weaponized-malware

[3] https://www.globalcyberalliance.org/90-days-to-dmarc-a-global-cyber-alliance-challenge.html aspx
[4] http://www.healthcareitnews.com/news/2018-primed-blockchain-big-data-and-cloud-computing-advancements-all-better-security-plan
[5] https://securingtomorrow.mcafee.com/mcafee-labs/2018-threats-predictions/
[6] http://www.healthcareitnews.com/news/2018-cybersecurity-prediction-extortion-attempts-ransomware-will-proliferate
[7] https://www.darkreading.com/mobile/android-ransomware-kits-on-the-rise-in-the-dark-web-/d/d-id/1330591

4. **Wired's Guide to Digital Security** – Break this out when the holiday conversation turns to family members asking about how to "cyber": https://www.wired.com/2017/12/digital-security-guide/

5. **DMARC correction** – Last week we highlighted a new DMARC initiative announced by NH-ISAC, the Global Cybersecurity Alliance (GCA), and Agari. While GCA has issued a 90 days to DMARC challenges, the goal for NH-ISAC members is DMARC implementation in 2018. GCA's 90 day sprint provides an implementation roadmap that members can utilize in their own organizations. You can find that resource here: https://dmarc.globalcyberalliance.org/.

   And you can watch Jim Routh, CSO at Aetna and Chair of NH-ISAC, talk about the benefits of DMARC and Aetna's implementation here: https://www.youtube.com/watch?v=bmjXsD2Tj5M

Congress –

Tuesday, December 12:
--Hearings to examine digital decision-making, focusing on the building blocks of machine learning and artificial intelligence. (Senate Commerce)

Wednesday, December 13:
--Hearing: Examining the Drug Supply Chain (House Energy and Commerce)
<https://energycommerce.house.gov/hearings/examining-drug-supply-chain/>

--Oversight Hearing with Deputy Attorney General Rod Rosenstein (House Judiciary)
<https://judiciary.house.gov/hearing/oversight-hearing-deputy-attorney-general-rod-rosenstein/>

Conferences and Webinars –

--Business Email Compromise Workshop – New York, NY (12/5)
<https://nhisac.org/events/nhisac-events/business-e-mail-compromise-workshop/>
--Regional Healthcare Cybersecurity Summit – Hebron, KY (12/7)
<https://nhisac.org/events/nhisac-events/regional-healthcare-cybersecurity-summit/>
--Basic Best Practices in Cybersecurity – Savannah, GA (NH-ISAC) (12/13)
<https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-georgia/>
--Health IT Summit – Dallas, TX (12/14) <https://vendome.swoogo.com/Dallas-HITSummit-2017>
--Business Email Compromise Workshop – Dallas, TX (12/14) <https://nhisac.org/events/nhisac-events/business-e-mail-compromise-workshop/>
--2018 Spring Summit – Sawgrass, FL (NH-ISAC) (5/14-17) <https://nhisac.org/summits/2018-spring-summit/>

December 12, 2017

Sundries –

--Andromeda Botnet Dismantled in International Cyber Operation < https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation>
--BD Establishes Product Security Partnership Program to Enhance Cybersecurity of Medical Technology <http://markets.businessinsider.com/news/stocks/BD-Establishes-Product-Security-Partnership-Program-to-Enhance-Cybersecurity-of-Medical-Technology-1010933775>
-- Surveillance inside the Body <https://www.schneier.com/blog/archives/2017/12/surveillance_in_3.html>
--Nope, this isn't the HTTPS-validated Stripe website you think it is < https://arstechnica.com/information-technology/2017/12/nope-this-isnt-the-https-validated-stripe-website-you-think-it-is/>
--Phishers Are Upping Their Game. So Should You. < https://krebsonsecurity.com/2017/12/phishers-are-upping-their-game-so-should-you/>\
--'Mailsploit' Lets Hackers Forge Perfect Email Spoofs < https://www.wired.com/story/mailsploit-lets-hackers-forge-perfect-email-spoofs/>
--Microsoft Issues Emergency Patch for 'Critical' Flaw in Windows Security < https://www.darkreading.com/vulnerabilities---threats/microsoft-issues-emergency-patch-for-critical-flaw-in-windows-security/d/d-id/1330595>
--FBI director again laments strong encryption in remarks to Congress < https://arstechnica.com/tech-policy/2017/12/fbi-director-again-laments-strong-encryption-in-remarks-to-congress/>
--Henry Ford Health System PHI Data Breach Affects 18K <https://healthitsecurity.com/news/henry-ford-health-system-phi-data-breach-affects-18k>
--Ransomware attack on NJ provider locks 16,000 patient records < http://www.healthcareitnews.com/news/ransomware-attack-nj-provider-locks-16000-patient-records>
--Oklahoma health department alerts 47,000 clients about data breach for the 2nd time <http://www.healthcareitnews.com/news/oklahoma-health-department-alerts-47000-clients-about-data-breach-2nd-time>

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