February 20, 2018

Hacking Healthcare

TLP White
This week we revisit budgets, finish up with GDPR, look down-under, and worry about adversaries exploiting our data breach laws. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Budgets:*** The HHS Secretary went in front of House Ways and Means last Wednesday for a two-hour budget hearing. Cybersecurity was mentioned only in passing – by Rep. Patrick Meehan (R-PA) who encouraged the Secretary to engage with Congressional leadership on efforts to protect the safety and privacy of patients.

   Since then, HHS has put out their 2019 "Budget in Brief," which adds details to the high-level budget proposal put out by the President last week. The budget proposes $68 million to "ensure the Department is able to detect, manage, and remediate cybersecurity risks." While these are mostly funds designated to help protect HHS from cyber threats, there is also intent to "proactively engage with a range of stakeholders." The budget proposal represents an increase of $18 million over the 2018 enacted budget.

   A Budget in Brief can also be a helpful way to understand future Departmental plans. This document is no different and reveals OCR's intent to develop guidance documents that explain "how to effectively respond to cybersecurity threats, including issuing resources to illustrate the steps HIPAA-covered entities or business associates should take in response to a cyber-related security incident."

2. ***GDPR:*** For the last couple weeks we have looked at the foundations of GDPR and its implications in terms of breach notification requirements and potential penalties for non-compliance. But compliance with GDPR includes some proactive organizational measures related to how data is protected when stored and processed. Today we will look at those.

   Register as an NH-ISAC member to get access to this analysis each and every week!

3. ***Privacy Shield:*** Tune in next week for more detail on privacy shield – a 2016 agreement that regulates the protections required for transporting data between the EU and US.

Here's a primer if you want to jump right in: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

4. ***Australian Data Breach Law:*** Starting February 22 (this Thursday), Australia will introduce a new data breach notification requirement[1] for organizations conducting business in the country. The law[2] places a requirement to notify individuals and the government in the event of the unauthorized access, disclosure, or loss of personal information "likely to cause serious harm." This requirement applies to all health service providers[3] and organizations that hold health data on individuals. It also covers all other organizations operating in Australia with an annual turnover exceeding $3mm AUS.

   When a data breach that may require notification is discovered, the organization has 30 days to conduct an assessment of the breach. If the assessment determines that serious harm[4] may result, notification must occur "as soon as practicable." Notification can occur through direct notification to impacted individuals or broad publication of the incident. Importantly, notification must include recommendations on how an impacted individual can protect oneself.

   NH-ISAC is planning its first Australian Cybersecurity Workshop on April 13 in Sydney. Sign-up here: https://nhisac.org/events/nhisac-events/healthcare-cybersecurity-workshop-australia/

5. ***On Data Breach Notification:*** As different countries introduce new data breach requirements, a few thoughts strike me on how we might move forward:

   a. Embrace Federalism –

   b. Seek global consensus –

   c. Empower consumers –

   d. Be watchful for emergent risks – If Russia has sought to undermine European and American democracy through cyber-attacks on critical infrastructure, news, and elections, what better way to enhance that operation than by leveraging their targets own regulatory scheme?

[1] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

[2] https://www.legislation.gov.au/Details/C2017A00012

[3] https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/health-service-providers/is-my-organisation-a-health-service-provider

[4] " 'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm."

> I anticipate[5] a slew of GDPR-related attacks designed to pit global companies against European regulators when the law comes into effect in May. This could be done through the "disclosure" of big breaches by Wikileaks or other transparency efforts that prompt European authorities to investigate and threaten/levy large fines.

Congress *– No hearings of note scheduled.*

Conferences and Webinars –

--Third Party Risk Webinar (2/21) <https://nhisac.org/events/nhisac-events/member-third-party-risk-webinar/>

--NH-ISAC GDPR 101 Webinar (3/13) <https://nhisac.org/events/nhisac-events/nh-isac-gdpr-101/>

--Basic Best Practices in Cybersecurity – Alabama (2/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-alabama/>

--InfoSec World – Orlando (3/19) <https://nhisac.org/events/nhisac-events/infosec-world/>

--Medical Device Workshop at Philips Healthcare – Andover, MA (3/20) <https://nhisac.org/events/nhisac-events/medical-device-workshop-at-philips-healthcare-andover-ma/>

--Health IT Summit – Cleveland, OH (3/27) <https://vendome.swoogo.com/2018-Cleveland-Health-IT-Summit>

--Health IT Summit – San Francisco, CA (4/5) <https://vendome.swoogo.com/2018-San-Francisco-HIT-Summit>

--Security Workshops at Intermountain Health – Park City, UT (4/24) <https://nhisac.org/events/nhisac-events/security-workshop-at-intermountain-park-city-ut/>

--Medical Device and Pharmaceutical Security Workshop – London <https://nhisac.org/events/nhisac-events/security-workshops-london/>

--2018 NH-ISAC Spring Summit – Sawgrass, FL (5/14-17) <http://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>

--Health IT Summit – Philadelphia, PA (5/21) <https://vendome.swoogo.com/2018-Philly-HITSummit>

--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>

--Biotech / Pharmaceutical Security Workshop - Dublin, Ireland (6/21) <https://nhisac.org/events/nhisac-events/medical-device-and-pharmaceutical-security-workshop-dublin/>

--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>

--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>

[5] This is not based on any classified or open-source intelligence reporting.

--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--Biotech/Pharma Security Workshop at Gilead Sciences, Foster City, CA (8/29) <https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

--Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) <https://csrc.nist.gov/publications/detail/nistir/8200/draft>
--Nominee for FTC chairman signals scrutiny for tech giants <https://www.washingtonpost.com/news/the-switch/wp/2018/02/14/nominee-for-ftc-chairman-signals-scrutiny-for-tech-giants/>
--Business Associate Dismissal Denied in HIPAA Data Breach Case <https://healthitsecurity.com/news/business-associate-dismissal-denied-in-hipaa-data-breach-case>
--North Korean Malicious Cyber Activity <https://www.us-cert.gov/ncas/current-activity/2018/02/13/North-Korean-Malicious-Cyber-Activity>
--FS-ISAC Unveils 2018 Cybersecurity Trends According to Top Financial CISOs <https://www.fsisac.com/article/fs-isac-unveils-2018-cybersecurity-trends-according-top-financial-cisos>
--Trump to nominate Army cyber chief to lead NSA, official says <http://thehill.com/business-a-lobbying/373705-trump-to-nominate-army-cyber-chief-to-lead-nsa-official-says>
--Our critical infrastructure isn't ready for cyber warfare <http://thehill.com/opinion/cybersecurity/373815-our-critical-infrastructure-isnt-ready-for-cyber-warfare>
--Don’t Let Criminals Hide Their Data Overseas <https://www.nytimes.com/2018/02/14/opinion/data-overseas-legislation.html>
--U.N. chief urges global rules for cyber warfare <https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4>
--Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption <https://www.gao.gov/products/GAO-18-211>

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