April 17, 2018

TLP White

We have a lot in store for you this week. First, we start with a brief summary of Mark Zuckerberg's testimony from last week's congressional hearings and consider how the policies discussed would impact healthcare data practices. We then focus on a healthcare exception to a state's breach notification law and address how the SamSam ransomware impacts the healthcare industry. We also dive into Verizon's recently released Data Breach Report and talk about the latest threats to healthcare. We conclude with a discussion about new data security guidance the HHS is considering for researchers. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Zuckerberg.*** Mark Zuckerberg, Facebook's CEO, voluntarily testified in two hearings this week on Capitol Hill as a result of Cambridge Analytica's unauthorized access of about 87 million Facebook users' data.[1] The testimony and questions focused mainly on data security and privacy, Facebook's data practices, third-party data access and use, online advertising, and the role of government in regulating data security and privacy. Although the hearings did not address healthcare cybersecurity, per se, many of the policies discussed, if implemented, would surely impact the healthcare industry's data practices.

   For example, many members of congress pressed Zuckerberg on the regulatory nature of data privacy such as issuing new government regulations versus establishing industry-led efforts like voluntary guidelines. Senator Ed Markey, in particular, discussed his recently introduced, ''Customer Online Notification for Stopping Edge-provider Network Transgressions'' or the ''CONSENT Act." If enacted, the bill would expand the Federal Trade Commission's authority and require it to issue regulations that protect "the privacy of customers of edge providers," which would cover healthcare entities that provide edge services.[2] The law would, among other things, call on edge providers to "obtain opt-in consent from a customer to use, share, or sell the sensitive customer propriety information [which includes health information] of the customer."

[1] https://www.washingtonpost.com/news/the-fix/wp/2018/04/10/7-takeaways-from-mark-zuckerbergs-marathon-congressional-testimony/?utm_term=.2d79329821bc
[2] https://www.markey.senate.gov/imo/media/doc/CONSENT%20Act%20text.pdf

Congressman Raul Ruiz, in adopting another approach, suggested creating a new federal agency called the "Consumer Digital Protection Agency"[3] – which, if established, would presumably play a role in the healthcare industry's data security practices. Senator Thom Tillis recommended; however, that the government refrain from a "heavy-handed" approach and instead, rely more on industry to develop their own standards and codes of conduct.[4]

2. ***HIPPA Covered Entities Get a Pass.*** In Oregon, HIPAA covered entities are now exempt from the state's 45-day breach notification rule as a result of amendments recently signed into law by Governor Kate Brown.[5]

   The exemption will help avoid potential conflict and confusion between Oregon's law and HIPAA's Breach Notification Rule, which subjects covered entities to a 60-day breach notification requirement.[6] For example, if the 45-day requirement applied to HIPAA covered entities, then the law may have required a covered entity to notify affected individuals sooner than the HIPAA's 60-day requirement. Nonetheless, despite Oregon's exemption, members covered by the HIPAA must still adhere to the HIPAA's 60-day requirement and other states' breach notification laws after incurring a breach.

   The 45-day requirement, of course, still applies to members not covered by the HIPAA who collect health information. The law continues to include a consumer's health insurance information and medical history in its "personal information" definition and applies to all entities that "owns, licenses, or otherwise possesses personal information…use[d] in the course of the [entity's] business…"[7]

3. ***Healthcare Still Targeted by SamSam.*** A form of ransomware known as SamSam continues to target the healthcare sector.[8] We covered the SamSam threat when the attack emerged in 2016.[9] According to an alert published by the Healthcare Cybersecurity and Communications Integration Center, in 2018 there have been at least eight separate cyber-attacks on healthcare and government organizations.[10] The attacks have impacted a range of entities within the healthcare sector, including hospitals, a cloud provider, and an Industrial Control System, among others.

   The SamSam malware permits the attacker to gain unauthorized access to an organization's computer network, uses ransomware software to block most or all of the

[3] https://www.bloomberg.com/news/live-blog/2018-04-11/zuckerberg-testifies-to-house-on-facebook-data-scandal
[4] https://www.c-span.org/video/?c4722725/sen-thom-tillis (4 mins, 20 seconds in)
[5] https://healthitsecurity.com/news/hipaa-covered-entities-get-pass-on-or-data-breach-notification-law
[6] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[7] https://olis.leg.state.or.us/liz/2018R1/Downloads/MeasureDocument/SB1551/Enrolled
[8] http://www.healthcareitnews.com/news/samsam-ransomware-hackers-still-targeting-healthcare-hhs-warns
[9] https://nhisac.org/wp-content/uploads/2016/11/ransomware.pdf
[10] https://www.aha.org/system/files/2018-04/corrected-HCCIC-2018-002W-SamSam-Ransomware-Campaign.pdf

organization's access to their own files and data, and restricts access until a ransom is paid (which typically must be done within a limited period of time.) Hallmarks of the current wave of SamSam attacks include encrypting files with the ".weapologize" extension and displaying a "sorry" message.

4. ***Healthcare's Internal Threat Problem.*** Verizon recently released the 2018 Data Breach Investigations Report, which revealed that healthcare is the only industry where insider threats outnumber outside threat actors.[11] Specifically, the report noted that 56% of healthcare breaches were caused by internal threat actors, while 43% were caused by external risks.

   Of the 750 incidents that occurred in the healthcare sector, 79% of the data compromised was medical data, followed by 37% personal data and 4% payment data. Threat actors were largely financially motivated accounting for 75% of incidents, followed by 13% motivated by fun, 5% convenience, and 5% espionage. The report highlighted that miscellaneous errors, crimeware and privilege misuse present 63% of incidents within healthcare. Notably, the report suggests that it is difficult to know if healthcare is in fact more susceptible to ransomware than other industries, or if the high percentages of incidents reported are a product of healthcare's rigorous reporting requirements.

   Beyond insider threat, the healthcare portion of the Verizon report concludes with three recommendations for the healthcare vertical: (1) reduce your risk footprint where you can; (2) ensure that policies and procedures are in place mandating monitoring of internal protected health information accesses, and keep employees aware through training and warning banners; and (3) take preventative measures to minimize the impact of ransomware on your network.

5. ***HHS to Provide Insight Regarding CMS Lack of Oversight.*** A recent Government Accountability Office ("GAO") report concluded that the Centers for Medicare and Medicaid Services ("CMS") failed to develop data security control guidance for researcher organizations that use Medicare beneficiary data to study how health care services are provided to beneficiaries.[12] The report was requested by the chairman of the Senate Finance Committee, House Ways and Means Committee, and the House Energy and Commerce Committee in response to the number of data breaches that continue to impact the healthcare sector.

   In response to the report's findings, the Department of Health and Human Services ("HHS") has vowed to consider developing guidance for researchers that access and handle data on Medicare beneficiaries. In a recent blog post, House Energy and Commerce Committee majority staff noted that "[d]ata breaches have become more

[11] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
[12] https://healthitsecurity.com/news/gao-raps-cms-for-lax-healthcare-data-security-in-medicare

> common in recent months and years, particularly in the health care sector. It is imperative vital Medicare beneficiary data, which can be created and used by a number of different entities, is secure."[13]

Congress –

Tuesday, April 17:
--Hearing titled, "From Core to Edge: Perspective on Internet Prioritization" (House Subcommittee on Communications and Technology)[14]

Wednesday, April 18:
--Hearing to examine accelerating new technologies to meet emerging threats (Senate Subcommittee on Emerging Threats and Capabilities)[15]
--Hearing titled, "From Boston to Austin: Lessons Learned on Homeland Threat Information Sharing" (House Committee on Homeland Security)[16]
--Hearing titled, "Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy" (House Subcommittee on Information Technology)[17]

Thursday, April 19:
--Hearing to examine proposed budget estimates and justification for fiscal year 2019 for the Department of Health and Human Services (Senate Subcommittee on Departments of Labor, Health and Human Services, and Education, and Related Agencies)[18]

Conferences and Webinars –

--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>

---

[13] https://energycommerce.house.gov/news/blog/gao-urges-cms-bolster-medicare-beneficiary-data-security/
[14] https://energycommerce.house.gov/hearings/from-core-to-edge-perspective-on-internet-prioritization/
[15] https://www.armed-services.senate.gov/hearings/18-04-11-accelerating-new-technologies-to-meet-emerging-threats
[16] http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108113
[17] http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108179
[18] https://www.senate.gov/committees/committee_hearings.htm

--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>
--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 –

-- **Thousands of hacked websites are infecting visitors with malware** <https://arstechnica.com/information-technology/2018/04/nasty-malware-campaign-using-thousands-of-hacked-sites-hid-for-months/>
-- **On-Premise Security Tools Struggle to Survive in the Cloud** <https://www.darkreading.com/cloud/on-premise-security-tools-struggle-to-survive-in-the-cloud/d/d-id/1331501?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple>
-- **Virtua To Pay NJ $418,000 for HIPAA Violation** <https://healthitsecurity.com/news/virtua-to-pay-nj-418000-for-hipaa-violation-by-vendor>
-- **West Virginia sues Equifax over data breach** <https://www.reuters.com/article/us-equifax-cyber/west-virginia-sues-equifax-over-data-breach-idUSKBN1HJ37R>
-- **U.S. group sets up framework to keep customers' financial data secure** <https://www.reuters.com/article/us-usa-cyber-financial/u-s-group-sets-up-framework-to-keep-customers-financial-data-secure-idUSKBN1HJ2V2>
-- **Pompeo pressed on plans for cybersecurity at State** <http://thehill.com/policy/cybersecurity/382882-pompeo-pressed-on-plans-for-cyber-at-state>
-- **Uber agrees to revised settlement with FTC following revelation of 2016 data breach** <http://thehill.com/policy/technology/382861-uber-agrees-to-revised-settlement-with-ftc-following-revelation-of-2016>
-- **State Department warns staff of surge in hacking attempts** <https://www.politico.com/story/2018/04/12/state-department-attempted-hacking-warnings-479725>
-- **Ex-NSA chief Alexander: U.S. flying blind to nation-state hackers**

April 17, 2018

<https://www.cyberscoop.com/keith-alexander-nation-state-hackers/>
-- **AMD Releases Spectre v2 Microcode Updates for CPUs Going Back to 2011**
<https://www.bleepingcomputer.com/news/hardware/amd-releases-spectre-v2-microcode-updates-for-cpus-going-back-to-2011/>

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