November 27, 2018

TLP White

Authors Note: Greetings from the H-ISAC Summit in San Antonio! I will be around all week and looking forward to meeting as many of you as I can and attending the great sessions. I welcome any and all feedback on how Hacking Healthcare can be better, so if you are here and see me, please stop and say hello.

This week we start by recapping a Florida federal court's interpretation of an insured's commercial general liability policy in the context of a data breach. We also discuss the Consumer Data Privacy Act of 2018, privacy legislation that has been offered up for discussion by Sen. Ron Wyden (D-OR) in the Senate. We then turn to the US government's effort to keep its allies from using a Chinese brand of telecommunications equipment due the equipment's cybersecurity vulnerabilities. We end by taking a deeper dive into foreign hacks on healthcare systems.

Welcome back to *Hacking Healthcare*.

Hot Links –

1. ***Court Finds Insured's Commercial General Liability Policy Imposed No Duty to Defend on Insurer for Suits Arising Out of a Data Breach.*** In *St. Paul Fire & Marine Ins. Co. v. Rosen*, a Florida federal court declined to find an insurer had a duty to defend its insured for claims arising out of a data breach, reasoning that the insured's commercial general liability policy did not require such coverage.[1] Despite the fact that the policy provided coverage for "personal injury," which was defined as "injury… including making known to any person or organization covered material that violates a person's right of privacy," the court refused to read this definition to include coverage for lawsuits arising out of a data breach. This late September decision suggests that businesses will need separate cyber insurance or clauses in their commercial general liability policies that specifically pertain to cyber insurance in order to best insulate themselves from costs in the event of a data breach.

[1] https://www.executivesummaryblog.com/files/2018/10/St-Paul-v-Rosen.pdf

St. Paul concerned the Florida-based hotel chain Rosen Hotels & Resorts, Inc. ("Rosen") and its subsidiary IT services provider Rosen Millennium, Inc. ("Millennium").[2] A third-party hacker was able to install malware on the Rosen's payment network, which compromised guests' payment card information. Millennium held an insurance policy with St. Paul that provided for coverage in the event of personal injury or property damage. The case hinged on the court's interpretation of the phrase "made known" in the policy's definition of "personal injury" and whether Millennium's actions caused the data breach. Reasoning that the policy's personal injury definition only applied to Millennium's actions—not the actions of third-party hackers—the court found that the insurer did not have a duty to defend the insured in suits against it or its parent Rosen arising out of the data breach. The court discounted the argument that the insured Millennium was responsible for the breach because it failed to secure the payment information that was the subject of the breach.

2. ***Senator Pushes Privacy Bill That Provides for Steep Penalties.*** Senator Ron Wyden (D-OR) has introduced a draft bill for discussion in the Senate that seeks to institute a national standard for online personal data protections.[3] He introduced similar versions of this Consumer Data Protection Act in 2017 and 2015, but neither garnered enough bipartisan support to stand a chance at becoming law. However, the public's increased focus on data security and privacy coupled with the outcome of the recent midterm elections has led some to believe that legislators may turn their efforts towards comprehensive privacy legislation in the upcoming term. Senator Wyden's 2018 bill, therefore, may finally stand a chance to become the law of the land if it can drum up enough momentum in the current political climate.

   The Consumer Data Protection Act of 2018's penalties are substantial and mirror the penalties of the GDPR. Violations of the bill's terms would cost companies up to 4 percent of their annual gross revenue. The bill also requires executives to provide annual data protection reports to the FTC, and lying or making misrepresentations to the agency in such reports could subject CEOs to 20 years in prison.[4] Despite the bill's similarity to the GDPR in its steep penalties, its terms do not mirror the GDPR when it comes to the breadth of rights conferred on individuals. For example, the GDPR's concept of the "right to be forgotten"—the right of consumers to have data processors to delete their data—is nowhere present in Senator Wyden's bill. This is just one example of a number of ways in which the rights the bill confers to consumers fall short of the scope of the GDPR. Whether that is considered to be a good or bad thing is largely subjective, but notable nonetheless as should this become law, multi-national companies will still not have consistent legislation to build and manage to.

---

[2] https://www.law360.com/articles/1090847

[3] https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf

[4] https://motherboard.vice.com/en_us/article/8xjwjz/sen-ron-wyden-introduces-bill-that-would-send-ceos-to-jail-for-violating-consumer-privacy

3. ***Chinese Telecom Equipment Poses Espionage Risks for U.S. and Allies.*** The United States has asked its allies to refrain from using a certain kind of Chinese telecom equipment due to cybersecurity concerns with the equipment itself. U.S. intelligence agencies reportedly believe that Huawei, a Chinese company that produces mobile network equipment, facilitates espionage on the United States and its allies through its ties to the Chinese government.[5] This belief has become strong enough to motivate U.S. government officials to reach out to allied countries and request that Huawei equipment be removed and banned from future use.

   Though the U.S. has already ensured that Huawei equipment is not used by its own government employees or contractors, many of its allies use the equipment extensively to provide mobile networks to their citizens. In particular, the U.S intelligence community is concerned about allied countries who use the equipment while also being home to U.S. military bases, such as Japan, Italy, and Germany. The concern is that those bases' operations and communications could be vulnerable to Chinese spying or cyber-attacks because the host country uses Huawei telecom equipment.

   Chinese officials have responded to the U.S. government's allegations of espionage by diplomatically asking the U.S. to provide a "fair and predictable" investment environment for Chinese companies. Huawei itself has also reacted by offering to allow regulators to conduct full reviews of its source code at the company's new information security lab in Germany.

   However, it appears that Huawei's efforts to get the U.S. government's stamp of approval will continue to fall on deaf ears. As the threat of state-sponsored hacks and cyber-attacks continues to grow, the U.S. intelligence apparatus will continue to look at Chinese based tech companies through a scrutinizing lens in order to ensure the nation's systems and networks are protected. Whether these efforts truly make infrastructure more secure is not clear given that information about the actual risk isn't shared publicly or widely.

4. ***Foreign Hackers Eye Opportunities in the Healthcare Sector.*** A recent College of Healthcare Information Management Executives ("CHIME") report on national IT trends in the healthcare sector has noted that healthcare targets are more vulnerable than businesses in other sectors to foreign and state-sponsored cyberattacks. The report posits that this is because healthcare businesses appear to be more willing to pay ransoms to hackers than targets in other sectors.[6] Healthcare companies' willingness to fork over funds in exchange for returned use of systems and networks has put a target

[5] https://www.reuters.com/article/us-usa-china-huawei/u-s-asks-allies-to-shun-huawei-equipment-wsj-reports-sector-stocks-fall-idUSKCN1NR2E6?feedType=RSS&feedName=topNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtopNews+%28News+%2F+US+%2F+Top+News%29

[6] https://clearwatercompliance.com/wp-content/uploads/2018/10/Healthcare-Most-Wired-National-Trends-2018.pdf

on the healthcare industry and has made healthcare businesses more susceptible to cyber threats.

Healthcare IT businesses and business units are struggling to stop state-sponsored hackers at their source. Overall, these groups are largely reacting to hacks as they occur as opposed to proactively working to prevent them. For example, the CHIME report stated that only 29% of healthcare institutions have wide-ranging cybersecurity programs in place to help them defend against cyber threats. The report also noted that the growing number of internal and external security threats have made it increasingly more difficult for healthcare organizations to protect sensitive information like protected health information.

The general vulnerability of the healthcare industry has made it prone to foreign attacks. For example, hackers have tailored ransomware viruses to become more focused on infiltrating businesses in the healthcare industry. In 2017, 45% of all ransomware attacks targeted healthcare organizations.[7] In particular, a ransomware program called SamSam has been wreaking havoc on healthcare companies this year. SamSam, a customized virus that targets external facing remote desktop protocol servers, has brought down multiple hospitals and disrupted the business operations of electronic health records vendor Allscripts.[8] Though SamSam has not yet been conclusively attributed to any foreign nation-state actor, experts have noted that its creator is likely a non-native English speaker.[9] Experts also believe that in 2019, hackers' average payment demand for ransomware attacks will increase by 6500%, from an average of $300 to an average of $20,000 per payment.[10]

Foreign hackers have clearly identified an opportunity for large payouts by using ransomware to attack healthcare sector businesses. To defend against these threats, healthcare companies should institute comprehensive cybersecurity programs to become more proactive in the face of cyberattacks from ill-intentioned actors all over the globe.

Congress –

Tuesday, November 27:
--No relevant hearings.

Wednesday, November 28:

[7] https://www.sensorsmag.com/embedded/2019-security-predictions-likely-to-audacious
[8] https://www.healthcareitnews.com/news/what-know-about-samsam-ransomware-hitting-allscripts-hospitals
[9] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf
[10] https://www.sensorsmag.com/embedded/2019-security-predictions-likely-to-audacious

--Hearing to examine reducing healthcare costs, focusing on improving affordability through innovation (Senate Committee on Health, Education, Labor, and Pensions).[11]
--H-ISAC Radio, Live at the Fall Summit. Topic is IAM and Portable Identity. 11:15 am ET (10:15 am CST at Summit). Members look for link in member list server.

Thursday, November 29:
--No relevant hearings.

International Hearings/Meetings –

EU – No relevant hearings.

Conferences, Webinars, and Summits –

--2018 NH-ISAC Fall "Never Stand Alone" Summit – San Antonio, TX (11/26-30)
<https://nhisac.org/summits/2018-fall-summit/>
--Medical Device Security 101 Conference – Orlando, FL (1/21/19-1/22/19)
<https://nhisac.org/events/nhisac-events/medical-device-security-101-conference/>
--FIRST Symposium 2019 – London, UK (3/18/19-3/20/19)
<https://nhisac.org/events/nhisac-events/first-symposium-2019/>
--2019 NH-ISAC Spring Summit – Ponte Vedra Beach, FL (5/13/19-5/17/19)
<https://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>

Sundries –

--**Aurora / Zorro Ransomware Actively Being Distributed**
<https://www.bleepingcomputer.com/news/security/aurora-zorro-ransomware-actively-being-distributed/>
--**US Postal Service Exposes Data of 60 Million Users for Over a Year**
<https://www.bleepingcomputer.com/news/security/us-postal-service-exposes-data-of-60-million-users-for-over-a-year/>
--**How Bipartisanship Could Affect the Advertising Industry Following the Midterms**
<https://www.adweek.com/agencies/how-bipartisanship-could-affect-the-advertising-industry-following-the-midterms/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+adweek%2Fall-news+%28Adweek+All%29>
--**An Ingenious Data Hack is More Dangerous than Anyone Feared**
<https://www.wired.com/story/rowhammer-ecc-memory-data-hack/>
--**FCC's proposed robotext crackdown could block legal messages, critics say**
<https://arstechnica.com/tech-policy/2018/11/fccs-anti-robotext-plan-would-let-carriers-censor-texts-advocates-warn/>
--**What Wells Fargo's cyber boss is doing to protect critical infrastructure**

[11] https://www.senate.gov/committees/hearings_meetings.htm

November 27, 2018

<https://www.cyberscoop.com/rich-baich-wells-fargo-national-infrastructure-advisory-council/>
--**US cybercrime-fighters enter agreements with Indonesia, Singapore**
<https://www.cyberscoop.com/cybercrime-agreements-indonesia-singapore/>

Contact us: follow @HealthISAC, and email at contact@h-isac.org