December 3rd, 2019

TLP White

In this edition of Hacking Healthcare, we give you an update on yet another case of cyber insurance falling short of covering an expected cost. We then explore the possibility of Iran creating a "white list" for foreign websites. Finally, we discuss the potential impact of China stepping up intellectual property protections and cracking down on IP theft. Welcome back to *Hacking Healthcare*.

1. **More Doubts About Cyber Insurance**. In an update to our continuing coverage of cyber insurance, a subsidiary of AIG is arguing that it is not responsible for paying out roughly $20 million to its customer's legal defense fund for efforts related to a data breach from 2014.[1] Landry's, which owns Bubba Gump Shrimp and the Rainforest Café, was taken to court in 2018 by JP Morgan Chase over a failure to reimburse them for data breach-related expenses such as breach assessments.[2] Landry's expected that around $20 million worth of legal defense expenses would be covered by their insurer, the AIG subsidiary Insurance Company of the State of Pennsylvania, but a federal judge ruled that they could not recover those costs from the insurer in May. Currently, Landry's is appealing the decision in the U.S. Court of Appeals for the Fifth Circuit.[3]

   Skepticism over the cyber insurance market continues to build as more major breach-related claims are denied or brought to court. While it is possible to carefully construct cyber insurance policies with reputable insurers that are likely to reimburse you in all but the most extenuating circumstances, the doubt that insurance funds may not be available instantly is a cause for concern. Many organizations can't accept the damage a long and drawn out breach response and recovery process may inflict on their business, and many business continuity plans are built around the assumption that insurers will provide what is expected from them. For the time being, having an insurance policy is still likely a better option than operating without one, but it is imperative for organizations to vet insurers and involve their security teams in drafting up any cyber insurance policies.

2. **Iran to Introduce Internet White List?** Last week, the Iranian Information Technology Organisation (ITO), an Iranian government organization that oversees cyberspace-related activities, confirmed that it sent a letter to state-run organizations and private companies asking for a list of foreign websites that they "rely on."[4] While the motive

and intent for asking such a question has not been made public, there is speculation that this is a step towards the introduction of a "white list" for foreign websites. Such a strategy may ensure that only certain pre-approved websites that have been deemed appropriate or necessary by the state would be reachable by Iranian Internet users. Additionally, websites and services that may become blocked due to not being on the "white list" would create an opportunity for domestic companies to step in and replace them in the marketplace.

While Iran has not yet announced the creation of such a "white list," the country has a history of Internet censorship, and the state would ideally like to have more control over what it views as subversive or inflammatory Internet content.[5] Iran has implemented content filtering mechanisms in the past, although their tactics have constituted a less extreme version of what China has in place in the form of the Great Firewall. But if a "white list" scheme were to move forward in Iran, it would represent a significant step-up in efforts to control the public's consumption of online content.[6] In keeping with similarities to China and Russia, the possibility of creating domestic replacements for the blocked websites or services in the country echoes a recent and somewhat similar development in Russia that would require many electronics to come with Russian-made software or applications pre-installed.[7]

3. **People's Republic of China (China) Strengthens Intellectual Property Rights**. Of all the impacts of the digital age, the rise of intellectual property (IP) theft and the uneven application of intellectual property protection (IPR) have been among the most economically significant. Whether it is criminal and state-sponsored hacking to steal technology, state laws requiring companies to turn over source code, or states allowing their national champions to deconstruct and copy a competitor's product, organizations in every industry are wary that the millions they spend on research and development may not be recouped if their finished product is simply stolen and sold by someone else. China has long been accused of not doing nearly enough to crack down on IP theft and promote strong IPR. That may be changing according to a report by The Hill last week.

   The Hill report states that a joint directive coming from the General Offices of the Communist Party of China Central Committee and the Chinese State Council has prioritized strengthening IPR.[8] The Hill goes on to list curbing IP infringement, raising social satisfaction of IPR, and "strengthening protections around trade secrets and other intellectual property and their source codes" as key goals of the directive.[9] If China follows through on the joint directive, such a step could significantly boost U.S.-Chinese relations during a time of particular tension.

   A successful implementation of IPR and a crackdown on IP theft in China could have a significant impact on healthcare organizations. Estimates of Chinese IP theft put the cost to the U.S. at up to $600 billion annually. Additionally, just this year the National Institutes of Health (NIH) and the Federal Bureau of Investigation (FBI) launched 180

investigations of IP theft at research centers and academic institutions.[10, 11] Seventy-one medical schools are included in the broad investigative effort, with theft of biomedical research being highlighted as a primary target of the investigations.[12] It is unlikely that China's joint directive will create substantial change overnight, but it does represent a move in the right direction.

Congress –

Tuesday, December 3rd:
- No relevant hearings

Wednesday, December 4th:
- Hearings to examine legislative proposals to protect consumer data privacy. (Senate Committee on Commerce, Science, and Transportation)

Thursday, December 5th:
- Hearings to examine the evolution of next-generation technologies, focusing on implementing MOBILE NOW. (Senate Committee on Commerce, Science, and Transportation)

International Hearings/Meetings –

EU –

Tuesday, December 3rd:
European Parliament Committee on Environment, Public Health and Food Safety

Conferences, Webinars, and Summits –

--2019 H-ISAC Fall Summit – San Diego, CA (12/2/19-12/6/2019)
https://h-isac.org/summits/fall-summit-2019/
--H-ISAC Security Workshop – London, UK (2/5/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-2/
--Global Cyber Security in Healthcare & Pharma Summit - London, UK (2/6/2020)
http://www.global-engage.com/event/cybsec-health-summit/
--H-ISAC Analysts Security Workshop - Titusville, FL (3/4/2020)
https://h-isac.org/summits/apac-summit-2020/
-- 2020 APAC Summit – Singapore (3/31/2020-4/2/2020)
https://h-isac.org/hisacevents/h-isac-analysts-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Cambridge, MA (4/7/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-cambridge-ma/
--H-ISAC Security Workshop - Atlanta, GA (4/14/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-atlanta/
--H-ISAC Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/

December 3rd, 2019

Sundries –

--Over 38 Million Healthcare Records Exposed in Breaches Over 2019
https://www.bleepingcomputer.com/news/security/over-38-million-healthcare-records-exposed-in-breaches-over-2019/
--APT33 has shifted targeting to industrial control systems software, Microsoft says
https://www.cyberscoop.com/apt33-microsoft-iran-ics/
--NYPD Pulls Fingerprint Database Offline Due to Ransomware Scare
https://www.darkreading.com/threat-intelligence/nypd-pulls-fingerprint-database-offline-due-to-ransomware-scare/d/d-id/1336466
--Windows 7 end-of-life is coming. How much should you worry?
https://www.cyberscoop.com/windows-7-end-of-life-forescout-op-ed/

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

[1] https://www.cyberscoop.com/aig-landrys-lawsuit-cyber-insurance/
[2] https://www.cyberscoop.com/aig-landrys-lawsuit-cyber-insurance/
[3] https://www.cyberscoop.com/aig-landrys-lawsuit-cyber-insurance/
[4] https://www.bbc.com/news/technology-50563917
[5] https://www.bbc.com/news/technology-50563917
[6] https://www.bbc.com/news/technology-50563917
[7] https://www.bbc.com/news/world-europe-50507849
[8] https://thehill.com/policy/cybersecurity/471969-china-issues-directive-to-intensify-protections-around-intellectual
[9] https://thehill.com/policy/cybersecurity/471969-china-issues-directive-to-intensify-protections-around-intellectual
[10] https://thehill.com/policy/cybersecurity/471969-china-issues-directive-to-intensify-protections-around-intellectual
[11] https://www.nytimes.com/2019/11/04/health/china-nih-scientists.html
[12] https://www.nytimes.com/2019/11/04/health/china-nih-scientists.html