September 1, 2021

TLP White

This week, *Hacking Healthcare* begins by examining a new Chinese Data Security Law (DSL) that is set to go into effect on September 1st and contains provisions that may significantly impact how multinational organizations operate in China. Next, we provide a readout from the recent White House cybersecurity meeting with industry leaders that convened a broad swath of organizations and led to several private sector commitments that may help improve the nation's cybersecurity. Finally, we wrap up by revisiting the cyber insurance marketplace to review what has happened over the last 18 months and provide some guidance and context for what may come next.

Welcome back to *Hacking Healthcare*.

1. **A New Chinese Data Security Law**

   On September 1st, China's new Data Security Law (DSL) is scheduled to come into effect. The DSL is the product of several revisions over the past few years and is just one of several significant cyber-related laws introduced in China recently.

   Several key aspects of the law that are worth noting include:

   - While the law applies to data activities within mainland China, it also states that entities outside mainland China that "engage in data activities that harm the national security, the public interest, or the lawful interests of citizens or organizations of the People's Republic of China, legal liability will be investigated according to the law."[1] Violations may result in a fine, or the "suspension of business services, license revocation, and general civil and criminal liability."[2]

- The term "data activities" is defined broadly to include "data collection, storage, processing, use, provision, transaction, publication," as well as "other such activities."[3]

- Data falls under different "grades" depending on its importance to economic and social development, national security, impact on public interest, and effect on citizens and organizations.[4] The "grades" range from a focus on export control, national security, and a not yet fully defined set of "important data".[5]

- Article 24 states that "any country or region that adopts discriminatory prohibitions, limitations or other such measures toward the People's Republic of China with respect to investment or trade related to data, data development and use, or technology" may risk similar retaliatory actions.[6]

- Article 25 stipulates that "[t]hose conducting data activities shall, according to the provisions of laws and administrative regulations as well as mandatory requirements in national standards, establish and complete a data security management system across the entire workflow, organize and conduct data security education and training, and adopt corresponding technical measures and other necessary measures to ensure data security."[7]

- Articles 27 and 28 include references to security incident notifications, periodic risk assessments, and the submission of risk assessment reports to the "relevant competent department."

- Organizations may not provide data stored within mainland China to foreign law enforcement without approval from the relevant Chinese government department, with the exception of instances "[w]here the People's Republic of China has concluded or joined an international treaty or agreement with provisions on foreign law enforcement bodies consulting domestic data."[8]

- Any organization or individual may file a complaint or report violations of the law.[9]

Action & Analysis

2. White House Cybersecurity Meeting

On Wednesday, the 25th of August, President Biden convened a White House Summit with leaders from the technology, insurance & finance, education, and critical infrastructure sectors to issue what was described in a background press call as a "call to

action" to improve the nation's cybersecurity.[10] The meeting concluded with a number of announced commitments and initiatives.

In attendance at the invite only meeting were representatives of an eclectic group of organizations that included, Google, Amazon, Apple, Microsoft, IBM, ADP, JPMorgan Chase, Bank of America, TIAA, U.S. Bancorp, Coalition, Vantage Group, Resilience, Travelers, Code.org, University of Texas System, Tougaloo College, Girls Who Code, and Whatcom Community College.[11] Attendees met with the President before breaking off into smaller breakout groups led by various members of the cabinet and national security team. These breakout groups included focuses on the cybersecurity workforce, cybersecurity best practices, and critical infrastructure resilience.

Following the meeting, the White House announced the following developments:

- "The National Institute of Standards and Technology (NIST) will collaborate with industry and other partners to develop a new framework to improve the security and integrity of the technology supply chain."[12]

- An "expansion of the Industrial Control Systems Cybersecurity Initiative to a second major sector: natural gas pipelines."[13]

- Various commitments for training programs and investments from several tech and educational organizations to improve federal, state, and local entities' cybersecurity and bolster the cybersecurity workforce.[14]

Action & Analysis

3. Cyber Insurance Update

For those who haven't been keeping up with developments in the cyber insurance market, it has been in a state of upheaval following the explosion of ransomware attacks and ballooning ransom demands that have materialized in the last 18 months. We felt now was a good time to quickly break down what's been going on in the cyber insurance market and help provide some context for what may come next.

A good starting place may be the U.S. Government Accountability Office's (GAO) 26-page report *Cyber Insurance: Insurers and Policy Holders Face Challenges in an Evolving Market*. Released a few months ago back in May, the report paints a dreary picture. Some of the report's key facts include:[15]

- From 2016 to 2020, insurance clients opting for cyber coverage rose from 26% to 47%.

- Cyber insurance premiums have been steadily rising from 2017 to the middle of 2019, before rapidly increasing through the end of 2020.

- One survey of insurance brokers noted that "more than half of respondents' clients saw prices go up 10–30 percent in late 2020."[16]

- "Industry representatives told GAO the growing number of cyberattacks led insurers to reduce coverage limits for some industry sectors, such as healthcare and education."[17]

- Cyber insurers are increasingly making cyber insurance a standalone policy that removes cyber risk from being integrated with coverage for other issues.

- The lack of complete and transparent historical data on cyberattacks and the costs and losses associated with them has made it difficult to properly assess cyber risk and the costs associated with covering it.

- Despite the growing interest in cyber insurance over the past few years, standardized terminology and definitions have not been settled upon, thereby creating confusion over coverage.

Things have not been getting better in the months following the report, as the CEOs of AIG and Chubb have each reiterated that despite increased rates, they still don't accurately reflect the kind of risk that has been illustrated by major recent cyberattacks.[18]

Recent numbers also underscore how the scourge of ransomware is not an exaggerated threat, with credit ratings agency AM Best reporting that ransomware-related claims account for 75% of total claims, a 20-percentage point increase since 2016.[19] While some other organizations put that number a bit lower, it's still enough to scare more than a few insurers from covering ransomware attacks, or in some cases from providing cyber insurance all together.[20]

Action & Analysis

Congress –

Tuesday, August 31st:
- No relevant hearings

Wednesday, September 1st:
- House of Representatives – Committee on Homeland Security - Hearing: Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021

Thursday, September 2nd:
- No relevant hearings

September 1, 2021

International Hearings/Meetings –
- No relevant meetings

EU –

Conferences, Webinars, and Summits –

https://h-isac.org/events/

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

---

[1] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/
[2] https://www.csis.org/blogs/strategic-technologies-blog/how-data-security-law-sets-stage-tech-industry-china-and-beyond
[3] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/
[4] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/
[5] https://www.csis.org/blogs/strategic-technologies-blog/how-data-security-law-sets-stage-tech-industry-china-and-beyond
[6] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/
[7] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/
[8] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/
[9] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/
[10] https://www.whitehouse.gov/briefing-room/press-briefings/2021/08/25/background-press-call-by-senior-administration-officials-on-the-presidents-upcoming-cybersecurity-meeting/
[11] https://www.whitehouse.gov/briefing-room/press-briefings/2021/08/25/background-press-call-by-senior-administration-officials-on-the-presidents-upcoming-cybersecurity-meeting/
[12] https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/
[13] https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/
[14] https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/
[15] https://www.gao.gov/assets/gao-21-477.pdf
[16] https://www.gao.gov/products/gao-21-477
[17] https://www.gao.gov/products/gao-21-477
[18] https://www.cyberscoop.com/cyber-insurance-ransomware-crisis/
[19] https://www.cyberscoop.com/cyber-insurance-ransomware-crisis/
[20] https://securityintelligence.com/articles/how-ransomware-trends-change-cyber-insurance/