March 24th, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins by expanding on the topic of Chinese engagement with international standards bodies to examine China’s overall digital efforts and how they may impact the healthcare sector. Next, we provide an update on how the contentious issue of “right to repair” has spread to state legislatures and has been exacerbated by COVID-19, as well as how H-ISAC members may wish to engage with it. Lastly, we round out this week’s edition with a look at Australia’s recently released ransomware report and examine the country’s approach to balancing public-private responsibility for tackling the problem. Welcome back to *Hacking Healthcare*.

1. The Impact of China’s Digital Silk Road

Last week, we briefly outlined how China has increased its engagement within international standards bodies as a method of furthering its strategic goals and promoting its values. This week, we take a step back to better understand how that activity fits within the context of China’s “Digital Silk Road,” how China is leading companies away from Western-led institutions and values, and what that means for the healthcare sector.

China’s Digital Silk Road is an aspect of its broader overall Belt and Road initiative, a global infrastructure development and investment strategy that the government touts as a “bid to enhance regional connectivity and embrace a brighter future together.”[1] However, the initiative’s critics believe that it’s a strategic play to wield China’s economic power as a lever to curry political favor and geopolitical dominance that will undermine democratic values.

The Digital Silk Road itself is a set of foreign and domestic-oriented projects and policies that have been described as “creating China-centric digital infrastructure, exporting industrial overcapacity, facilitating the expansion of Chinese technology corporations, accessing large pools of data, and projecting sharp power as well as manipulating political perceptions.”[2] Even if the term Digital Silk Road isn’t familiar to you, you’re probably aware of it. China’s recent efforts to integrate Huawei and other Chinese telecommunications equipment into new 5G networks as well as the China Standards

2035 plan that we referenced last week can be seen as part of the Digital Silk Road strategy.

While the United States' vigorous campaign against Huawei ultimately led many allies and some economic partners to spurn Chinese telecommunications, China's ability to provide advanced technologies and infrastructure at low cost is making headway among less developed countries. When combined with other Digital Silk Road projects, like joint research and education programs, Chinese influence in the digital space is making notable inroads in global politics.

Action & Analysis *H-ISAC Membership Required*

2. Right to Repair Laws Under Consideration in 25 States

In addition to creating a global health crisis, COVID-19 has exacerbated several other issues that have been contentiously debated over the past few years. One issue that appears to be picking up steam in the United States is "right to repair," and it could have enormous impacts for the medical device community.

As a quick refresh, the right to repair concept essentially states that if and when a device breaks, the owner or end user should have the right to fix it themselves. While this might seem straightforward, companies can create barriers so only their stores or licensed technicians can fix their products. Potentially frustrating under normal circumstances, this issue has taken on greater significance during the pandemic. Right to repair is a serious issue in the medical device community where differing views exist between medical device manufacturers and the frontline organizations that are the owners and end users of the devices.

Medical devices, which must satisfy exacting standards required by the Food and Drug Administration (FDA) to be cleared for use, are usually serviced by their original manufacturers. Doing so helps ensure that repairs meet quality standards, which in turn protects patients and the manufacturer's reputation. Any repairs conducted by the end user or a third-party potentially increases the risk of damage to what are often sophisticated and carefully calibrated devices, thereby possibly putting patients at increased risk. This perspective can occasionally clash with the view of frontline healthcare organizations who may not have replacements or manufacturer-backed technicians readily available if a medical device needs immediate servicing.

At the forefront of this discussion in the COVID-19 pandemic is ventilators. On occasion during COVID-19, ventilators needing varying levels of servicing were rendered unavailable even when some fixes could potentially have been carried out by hospital staff. With ventilators being critical to treat COVID-19 patients, this issue sparked right to repair medical equipment legislation in both California and Hawaii.[3]

In total, legislators in Connecticut, Colorado, Delaware, Illinois, Maryland, Massachusetts, Missouri, Minnesota, Montana, Nevada, New Jersey, New York, Oklahoma, Oregon, and Washington have introduced right to repair legislation that would broadly apply to some technology's citizens use daily. Additionally, some states that have a large agricultural presence are considering the right to repair legislation specifically for agricultural equipment so farmers would be able to make repairs to their equipment without relying on a manufacturer-backed technician.

Action & Analysis
H-ISAC Membership Required

3. Australian Government Releases Ransomware Report

Last week, the Australian Government's Cyber Security Industry Advisory Committee released a new report titled *Locked Out: Tackling Australia's Ransomware Threat*. The report explains the negative effect ransomware attacks can have on businesses and provides general recommendations to all businesses, as well as specific advice tailored to small businesses, to strengthen defenses against cyber-attacks. Specifically, for small businesses that don't have IT or cybersecurity teams, the report provides several defense suggestions, such as multi-factor authentication, keeping software up to date, employee training, and backup to help prevent a ransomware attack.

The report also shared that from April to June 2020, there was a 65% increase in cyber security incidents that cost businesses an estimated $7.6 billion. The report estimates that if attacks were to continue at that rate, Australia's GDP would be impacted by $86 billion in the next decade. This statement highlights the very real effects cyber-attacks can have on the economy.[4] The report also emphasizes the investment the government will make in cybersecurity as part of Australia's Cyber Security Strategy 2020:

> *"The Federal Government will make the nation's largest ever investment in cyber security, with $1.67 billion to build new cybersecurity and law enforcement capabilities, protect the essential services upon which we all depend, assist businesses to protect themselves and raise the community's understanding of how to be secure online."*[5]

The Australian government's investment also includes allocations for the Australian Signals Directorate (ASD). The ASD is part of Australia's national security community and works across intelligence and cybersecurity. With the additional funding, the ASD is tasked with identifying cyber threats, disrupting foreign cybercriminals, and building partnerships between industry and government all with the goal of protecting Australian citizens.

Locked Out: Tackling Australia's Ransomware Threat provides statistics to further confirm that ransomware is a serious problem for both the economy and individuals. Despite the Australian government's additional cyber funding and the report's emphasis on recommendations for small businesses, Tim Watts, the Shadow Assistant Minister for Cyber Security, Labor Party thinks the government should be stepping up to do more to counter ransomware.

In an interview with CSO Australia, Watts stated that "[t]here are plenty of things the government can do to shape the environment in which these attacks occur. I think we can shape their incentives and alter their decision-making and dissuade them from targeting Australian organizations." [6] He also said that organizations are "crying out" for government leadership on ransomware and expressed concern that the majority of the report focused on what victim organizations should be doing to improve their defenses against an attack, since the government itself is also capable of taking measures on its own.[7]

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, March 23rd:
- No relevant hearings

Wednesday, March 24th:
- No relevant hearings

Thursday, March 25th:
- Senate – Committee on Health, Education, Labor, and Pensions: Hearings to examine our COVID-19 response, focusing on improving health equity and outcomes by addressing health disparities.

International Hearings/Meetings –

- No relevant hearings

EU –

Wednesday, March 24th:
- European Commission: Workshop EU4Health Programme 2021

Conferences, Webinars, and Summits –

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

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

[1] http://english.www.gov.cn/news/top_news/2015/03/28/content_281475079055789.htm
[2] https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political
[3] https://www.vice.com/en/article/z3vavw/half-the-country-is-now-considering-right-to-repair-laws
[4] https://www.homeaffairs.gov.au/cyber-security-subsite/files/tackling-ransomware-threat.pdf
[5] https://www.homeaffairs.gov.au/cyber-security-subsite/files/tackling-ransomware-threat.pdf

March 24th, 2021

[6] https://www.homeaffairs.gov.au/cyber-security-subsite/files/tackling-ransomware-threat.pdf

[7] https://www.csoonline.com/article/3611630/australia-government-says-ransomware-is-for-businesses-to-address.html?upd=1616434944206