October 22nd, 2019

TLP White

We've dedicated this edition of Hacking Healthcare to giving you a primer on some of the impacts geopolitical tensions can have on healthcare organizations, particularly in relation to technology and cybersecurity considerations. By outlining how geopolitics can lead to sanctions, impact third-party dependencies, create unanticipated competition, and increase the likelihood of cyberattacks and IP theft, we hope you will be better positioned to prepare and respond going forward. Welcome back to *Hacking Healthcare*.

Geopolitics and Healthcare Operations

Regardless of the industry sector to which you belong, there is no escaping the role of geopolitics in business operations. From organizations that are susceptible to cyberattacks by state actors for promoting oppositional views, to ill-defined government sanctions that make operating in certain countries or regions fraught with legal danger, geopolitics adds cost and complexity whether you are operating a global business or a purely domestic one. The healthcare industry is not immune to these issues, and it is incumbent on security leaders to understand how geopolitical realities can affect their business or mission.

Economic Sanctions

Economic sanctions, defined as "the withdrawal of customary trade and financial relations for foreign- and security-policy purposes," represent one of the more serious disrupters to an organization's global operations.[1] While the imposition of economic sanctions can take many forms, from all-encompassing prohibitions of trade to industry-specific, partially prohibited commercial interactions, this type of activity is a common policy tool used by governments everywhere.

If there is any good news here, it is that healthcare goods and services are generally understood to be necessities with fewer substitutes than many other types of goods and services. And because most citizens are highly attuned to increased healthcare costs and/or loss of service, economic sanctions tend to avoid directly impacting the healthcare industry as much as possible for as long as possible. As an example, in the current trade conflict between the United States (US) and Peoples Republic of China (PRC), "the US Government exempted crude drugs, pharmaceutical preparations, and low-end medical devices from the original tariff list, and the Chinese Government excluded drugs (both those for treatment and prevention) from taxation

and has removed tariffs on most imported drugs."[2] Unfortunately, the indirect effects of sanctions are nearly impossible to mitigate, with raw materials and component parts being far more likely to be impacted relatively early on.

Economic Sanctions and Third Parties

Even when healthcare organizations find themselves exempt from many of the initial, direct impacts of economic sanctions, the third-party goods and services that are integral to the efficient operation of a healthcare organization may not be. For example, The United States' recent imposition of sanctions on Venezuela has forced Adobe to cut off services to their Venezuelan customers.[3] The sudden, unplanned loss of third-party services, especially in concert with having little time to migrate to an alternative, can be devastating to any organization. Third party effects can be particularly impactful for small and mid-sized businesses who may not have the resources to find and implement an alternative. You should already be maintaining an inventory of your third-party suppliers, and you should carefully consider how the possibility of geopolitical sanctions could impact those products and services.[4]

Market Lockout, Autarky[5], and IP Theft

Of all the issues surrounding the recent geopolitical tension between the United States and the People's Republic of China, the Huawei saga is among the most prominent. The impact of the United States' export ban on Huawei was keenly felt, and losing the ability to use Google's applications on their new mobile devices dealt a significant blow to the company. However, Huawei's response has been to develop their own operating system as a long-term replacement.[6] Even if Google's applications are eventually allowed back into the Chinese market, Huawei's decision to invest heavily in creating its own versions of these applications is unlikely to be abandoned. The effect of the sanctions, in this case, is the creation of a direct market competitor.

It is easy to imagine how this scenario could apply to the healthcare industry. In a situation where broad sanctions that include medical devices or medical applications are imposed on a country, there is the potential for a large state to commit to develop or expand its own medical device industry. This type of autarkic behavior is not realistic for most states, but developed states and economic powerhouses like the PRC, the EU, and the US possess a large enough marketplace and a sufficiently advanced industry to make this route a potentially viable option.

If a state chooses to develop its own products, services, or tools in the event of an economic sanction, there is an increased incentive for cyber operations focused on IP theft. This may be especially true of states that have a vested interest in promoting national champions, as the PRC is doing with Huawei.

Cyber Attacks

It is not a coincidence that the majority of major cyber incidents that are attributed to states are against other geopolitical rivals.[7] Within the United States, many of the worst hacks, like Office of Personnel Management (OPM) and Sony America, have been attributed to Iranian, North Korean, Russian, and Chinese sources.

A common thread in all state-sponsored hacks is that geopolitical rivalries incite cyberattacks. Cyberattacks offer states the ability to negatively impact a geopolitical rival, generally below the threshold for a kinetic response, and with some semblance of plausible deniability. As tensions between states become inflamed, the likelihood of cyberattacks increases.

Conclusion

We recognize that most of these issues are beyond the direct influence of any one organization or industry, but it is important to recognize and plan for the most plausible events that could affect your organization. Anticipating a potential increase in cyberattacks from a geopolitically-inflamed rival state can help with resource prioritization. Knowing your third-party dependencies can help you plan for suddenly being without them. Early recognition of the potential of a trade or political conflict will give your organization and your industry more time to lobby for its protection. Being aware of these issues may be all you can do, but it can make a significant difference if you ever have to respond to an event that may have been geopolitically motivated.

Congress –

Tuesday, October 22nd:
- Preparing for the Future: An Assessment of Emerging Cyber Threats (House - Committee on Homeland Security - Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation)

Wednesday, October 23rd:
- Markup of H.R. 4237 “Advancing Cybersecurity Diagnostics and Mitigation Act” (House-Committee on Homeland Security)

Thursday, October 24th:
- Hearings to examine data ownership, focusing on exploring implications for data privacy rights and data valuation (Senate – Banking, Housing, and Urban Affairs)

International Hearings/Meetings –

EU –

-No relevant hearings

October 22nd, 2019

Conferences, Webinars, and Summits –

--H-ISAC / MITSF Healthcare Cybersecurity Workshop – Tokyo, Japan (10/24/2019)
http://www.cvent.com/events/h-isac-mitsf-healthcare-cybersecurity-workshop/event-summary-21a9794745bf41c4bb55ba9dd29dc256.aspx
--Key Steps to Building a Threat Intelligence Strategy – Webinar (10/24/2019)
https://h-isac.org/hisacevents/trustar-webinar/
--H-ISAC Security Workshop – Titusville, FL (11/4/2019)
https://h-isac.org/hisacevents/h-isac-security-workshop/
--Maximize your Threat Sharing by Anomali – Webcast (11/6/2019)
https://h-isac.org/hisacevents/maximize-your-threat-sharing/
--CHIME Healthcare CIO Boot Camp – Phoenix, AZ (11/6/2019-11/9/2019)
https://h-isac.org/hisacevents/chime-healthcare-cio-boot-camp/
--Health IT Summit (Southwest) – Houston, TX (11/14/2019-11/15/2019)
https://endeavor.swoogo.com/2019-Dallas-Health-IT-Summit
--Southwest Healthcare Cybersecurity Forum – Dallas, TX(11/15/2019)
https://endeavor.swoogo.com/2019_Southwest_Cybersecurity_Forum
--Health IT Summit (Northwest) – Seattle, WA (11/19/2019-11/20/2019)
https://endeavor.swoogo.com/2019-PacificNorthwest-HITSummit
--Pacific Northwest Healthcare Cybersecurity Forum – Seattle, WA (11/20/2019)
https://endeavor.swoogo.com/2019_Pacific_Northwest_Cybersecurity_Forum
--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/

Sundries –

--Microsoft unveils bug bounty program for election software
https://www.cyberscoop.com/microsoft-bug-bounty-election-guard/
--Industry Wants More Legal Cover for Sharing Supply Chain Threats
https://www.nextgov.com/cybersecurity/2019/10/industry-wants-more-legal-cover-sharing-supply-chain-threats/160680/
--Pentagon official urges contractors to improve cybersecurity
https://www.cyberscoop.com/katie-arrington-pentagon-contracting/
--Unpatched Linux bug may open devices to serious attacks over Wi-Fi
https://arstechnica.com/information-technology/2019/10/unpatched-linux-flaw-may-let-attackers-crash-or-compromise-nearby-devices/
--US claims cyber strike on Iran after attack on Saudi oil facility
https://arstechnica.com/information-technology/2019/10/us-claims-cyber-strike-on-iran-after-attack-on-saudi-oil-facility/

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

[1] https://www.cfr.org/backgrounder/what-are-economic-sanctions#chapter-title-0-1

[2] https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(19)31908-7/fulltext
[3] https://www.theverge.com/2019/10/7/20904030/adobe-venezuela-photoshop-behance-us-sanctions
[4] https://www.theverge.com/2019/10/7/20904030/adobe-venezuela-photoshop-behance-us-sanctions
[5] https://en.wikipedia.org/wiki/Autarky
[6] https://www.ft.com/content/1567d7c2-f1ed-11e9-bfa4-b25f11f42901
[7] https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents