March 2nd, 2021

TLP White

This week, *Hacking Healthcare* begins with the contentious issue of mandating cyberattack disclosures in the wake of SolarWinds and considers what role ISACs and ISAOs could play in improving information sharing. Next, we briefly cover the Biden Administration's recent supply chain Executive Order and its relation to cybersecurity in the healthcare sector. Finally, we end by examining new reports that highlight the interconnected nature of cybercriminal groups and their relationship to nation-states. Welcome back to *Hacking Healthcare*.

1. **Could SolarWinds Lead to Legally Mandated Cyberattack Disclosures?**

   As the dust from the SolarWinds attack continues to settle, the case for more significant information sharing and coordination has been made by both the public and private sectors. One idea gaining traction is the possibility of creating some form of mandatory cyberattack disclosure. The outlines of what a process like this would look like are fuzzy, but at a Senate hearing last week, lawmakers and tech industry representatives appeared sympathetic to the approach.

   The Senate Select Committee on Intelligence held an open hearing last Tuesday, where both lawmakers and representatives of the tech industry, including Microsoft President Brad Smith and the bipartisan pair of Senators Warner (D-VA) and Rubio (R-FL), appeared to agree that some type of cyberattack reporting should be required. The consensus appears to be that reporting requirements may be necessary to effectively counter sophisticated nation-state attacks like SolarWinds, where gauging the true scale of the attack and properly responding to it was made more difficult by the inability to adequately share information.[1]

   It remains to be seen if there is enough political backing to really pursue implementing a policy like this, and there will undoubtedly be drawn out discussions on how narrowly or broadly such a requirement should be written. Liability protections, confidentiality requirements, and even establishing an investigative agency similar to the National Transportation Safety Board were all floated as ideas for consideration.[2]

   While it can be easy to get lost in the details, current information sharing processes and procedures, both between the public and private sector entities and within the public

sector itself, came under fire for their perceived inadequacies during this week's hearing.

Action & Analysis
H-ISAC Membership Required

2. Supply Chain Executive Order

On Wednesday, February 24th, President Biden signed an "Executive Order on America's Supply Chains," citing the need for "resilient, diverse, and secure supply chains to ensure our economic prosperity and national security."[3] The Executive Order noted a broad swath of issues that threaten American supply chains, including "[p]andemics and other biological threats, cyber-attacks, climate shocks and extreme weather events, terrorist attacks, geopolitical and economic competition."[4] Tackling all of these complicated issues will be no easy task, and many have a direct relationship to the healthcare sector.

The initial priority of the Executive Order centers on four issue areas to be assessed through an immediate 100-day review, specifically: (1) the offshoring of active pharmaceutical ingredients, (2) dependency on critical minerals needed for defense and the high-tech sector, (3) the underproduction of semiconductors, and (4) the need to address demand for large capacity batteries.[5] These priorities then expand to an in-depth review of six industry sectors, including the "public health and biological preparedness industrial base and the information and communications technology (ICT) industrial base."

The Executive Order notes more traditional supply chain issues, such as identifying critical goods and materials and manufacturing and transportation risks, but it also delves into workforce needs and cyber. The in-depth review will ask United States federal agencies and departments, including the Department of Health and Human Services (HHS) and the Department of Homeland Security (DHS), to make note of the cyber risks "that may disrupt, strain, compromise, or eliminate the supply chain," including "risks posed by supply chains' reliance on digital products."[6] The Executive Order further reinforces that a key goal is to build out a sustained commitment supply chain resiliency, and that none of this will be possible without partnership and consultation with various stakeholders in "industry, academia, non-governmental organizations, communities, labor unions, and State, local, territorial, and Tribal governments."[7]

Action & Analysis
H-ISAC Membership Required

3. **Nation States Look to Cybercriminals to Augment Abilities**

   Attributing cyberattacks is difficult under the best of circumstances – adding to that difficulty is the fact that cybercrime groups are selling their hacking skills to countries, creating yet another layer of obfuscation. With this arrangement, nation-states don't need to use their own hacking groups to carry out less sophisticated attacks. Instead, they can hire a group not affiliated with a country to carry out the attack for them. These cybercrime groups can provide services such as malware, phishing, and breaching networks,[8] while allowing the country that hired them to obtain the information or access it requested without directly doing any of the dirty work.

   The *BlackBerry 2021 Threat Report* commented on this cybercrime-for-hire scheme, stating: "The emergence, sophistication, and anonymity of crimeware-as-a-service means that nation states can mask their efforts behind third-party contractors and an almost impenetrable wall of plausible deniability."[9] Further complicating attribution, these cybercrime-for-hire groups appear ready to work for a variety of countries with varied strategic interests, making it hard to find a common theme to connect otherwise irreconcilable attacks. These groups' victims vary geographically, and their efforts also vary in terms of the type of attack carried out.

   In related news, CrowdStrike released a chart that outlines the many connections known cybercrime groups have between themselves. The report provides evidence of the frequent extent to which these groups cooperate with one another and attests that the cybercrime ecosystem is more interconnected than many are aware of. The hacking skills offered by these groups can be broken down into services, distribution, and monetization, all of which are interconnected and provided by a variety of groups.[10] The CrowdStrike chart helps to illustrate that well known cybercriminal groups are rarely singular, one-stop shops by themselves, and that cybercrime really is an ecosystem.

   Action & Analysis
   H-ISAC Membership Required

Congress –

Tuesday, March 2nd:
- House of Representatives – Committee on Energy and Commerce – Subcommittee on Health: "The Future of Telehealth: How COVID-19 is Changing the Delivery of Virtual Care"

Wednesday, March 3rd:
- No relevant hearings

Thursday, March 4th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

March 2nd, 2021

EU –

Tuesday, March 3rd:
- EU Health Policy Platform Annual Meeting

Thursday, March 4th:
European Parliament – Committee on the Environment, Public Health and Food Safety: Committee meeting

Conferences, Webinars, and Summits –

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

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

---

[1] https://www.zdnet.com/article/ceos-senators-discuss-mandating-cyber-attack-disclosures/
[2] https://www.zdnet.com/article/ceos-senators-discuss-mandating-cyber-attack-disclosures/
[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
[5] https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/24/fact-sheet-securing-americas-critical-supply-chains/
[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
[7] https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/24/fact-sheet-securing-americas-critical-supply-chains/
[8] https://www.zdnet.com/article/cybercrime-groups-are-selling-their-hacking-skills-some-countries-are-buying/
[9] https://www.blackberry.com/us/en/forms/enterprise/report-bb-2021-threat-report
[10] https://www.zdnet.com/article/this-chart-shows-the-connections-between-cybercrime-groups/