April 5, 2022

TLP White

This week, *Hacking Healthcare* focuses on the United States and begins by breaking down a new senate bill that looks to improve healthcare cybersecurity. We examine why the bill may not end up being as impactful as its drafters may hope despite its good intentions. Next, we explore what a cybercrime statistics bill would and wouldn't accomplish in helping to improve the nation's ability to tap into comprehensive cybersecurity statistical data.

Welcome back to *Hacking Healthcare*.

1. **Senators' Introduce Healthcare Cybersecurity Bill**

   Last month, a bipartisan bill was introduced into the U.S. Senate with the aim of enhancing the cybersecurity of the Healthcare and Public Health (HPH) sector. While a positive development at first glance, there are reasons to be skeptical that this new bill will lead to meaningful improvement of HPH sector cybersecurity. Let's break down why.

   Introduced on March 23rd, the *Healthcare Cybersecurity Act of 2022* cites an increase in malicious cyberattacks on the HPH sector and the significant number of individuals affected by these attacks as motivation for the legislation.[1] The bill's authors also note that, according to Department of Health and Human Services (HHS) data, "[in] almost every month in 2020, more than 1,000,000 people were affected by data breaches at healthcare organizations," and that attacks increased healthcare delivery costs.[2]

   In terms of what the bill would accomplish, it outlines three lines of effort:

   - CISA collaboration with HHS: The bill would require the Cybersecurity & Infrastructure Security Agency (CISA) to "coordinate with and make resources available to Information Sharing and Analysis Organizations, information sharing and analysis centers."[3] That coordination must include "developing products specific to the needs of [HPH] sector entities and the sharing of information relating to cyber threat indicators and appropriate defensive measures."[4]

- Healthcare Expert Training: CISA would be required to provide "training to [HPH] sector asset owners and operators."[5] This would focus on cybersecurity risks and ways to mitigate those risks and could involve the inclusion of private sector healthcare experts where appropriate.[6]

- Sector Specific Study and Report: Within a year, the Director of CISA and the Secretary of HHS would be required to conduct a study and publish a report that would address the following elements:

  o "An analysis of how identified cybersecurity risks specifically impact [HPH sector] assets, including the impact on rural and small and medium-sized [HPH sector] assets";

  o an evaluation of the challenges [HPH] sector assets face in securing a wide range of devices, equipment, and systems;

  o an evaluation of the challenges HPH sector assets face in implementing cybersecurity protocols;

  o an evaluation of the challenges HPH sector assets face in responding to data breaches or cybersecurity attacks, including the impact on patient access to care, quality of patient care, timeliness of health care delivery, and health outcomes;

  o an evaluation of best practices for the deployment of trained Cyber Security Advisors and Cybersecurity State Coordinators of the Agency into Healthcare and Public Health Sector assets before, during and after data breaches or cybersecurity attacks;

  o an assessment of relevant HPH sector cybersecurity workforce shortages;

  o an identification of cybersecurity challenges related to COVID-19; and

  o an evaluation of the most accessible and timely ways for CISA and HHS to communicate and deploy cybersecurity recommendations and tools to Healthcare and Public Health Sector assets.

The finished report may be referenced by the Secretary of HHS when updating the Healthcare and Public Health Sector Specific Plan.

Action & Analysis
Membership required

April 5, 2022

2. Cybercrime Statistics Gets Boost

At the end of last month, the U.S. House of Representatives passed a Senate bill designed to improve the nation's grasp of cybercrime statistics. The bill, which now heads to President Biden's desk, is a step toward improving the inconsistencies and gaps in cybercrime reporting and statistics that we touched on last week.

The *Better Cybercrime Metrics Act* explicitly calls out that cybercrime may be the most common type of crime and that the "United States lacks comprehensive cybercrime data and monitoring, leaving the country less prepared to combat cybercrime that threatens national and economic security."[7]

If signed into law, it would require the Attorney General and the National Academy of Sciences "to develop a taxonomy for the purpose of categorizing different types of cybercrime and cyber-enabled crime." The taxonomy is to be designed with the intent that it could be used by the Federal Bureau of Investigation (FBI) to "classify cybercrime in the National Incident-Based Reporting System, or any successor system."[8]

Additionally, within two years, the Attorney General would be required to establish cybercrime and cyber-enabled crime as categories within the National Incident-Based Reporting System or its successor. It would also require the inclusion of "questions relating to cybercrime victimization in the National Crime Victimization Survey."[9] Finally, it would require the Comptroller General of the United States to submit a congressional report that assesses:

- the effectiveness of reporting mechanisms for cybercrime and cyber-enabled crime in the United States;
- disparities in reporting data between data relating to cybercrime and cyber-enabled crime; and
- disparities in reporting data between other types of crime data.

Action & Analysis
Membership required

Congress

Tuesday, April 5th:
- Senate – Finance Committee: Hearings to examine the President's proposed budget request for fiscal year 2023 for the Department of Health and Human Services.

April 5, 2022

- Senate – Health, Education, Labor, and Pensions Committee: Hearings to examine FDA user fee agreements, focusing on advancing medical product regulation, and innovation for the benefit of patients.
- House of Representatives – Homeland Security Committee: "Mobilizing our Cyber Defenses: Securing Critical Infrastructure Against Russian Cyber Threats".
Wednesday, April 6th:
- House of Representatives - Education and Labor Committee: Examining the Policies and Priorities of the U.S. Department of Health and Human Services.
- House of Representatives – Homeland Security Committee: "Mobilizing our Cyber Defenses: Maturing Public-Private Partnerships to Secure U.S. Critical Infrastructure".
Thursday, April 7th:
- No relevant hearings

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

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

April 5, 2022

---

[1] https://www.congress.gov/bill/117th-congress/senate-bill/3904/text?q=%7B%22search%22%3A%5B%22rosen%22%2C%22rosen%22%5D%7D&r=1&s=3

[2] https://www.congress.gov/bill/117th-congress/senate-bill/3904/text?q=%7B%22search%22%3A%5B%22rosen%22%2C%22rosen%22%5D%7D&r=1&s=3

[3] https://www.congress.gov/bill/117th-congress/senate-bill/3904/text?q=%7B%22search%22%3A%5B%22rosen%22%2C%22rosen%22%5D%7D&r=1&s=3

[4] https://www.congress.gov/bill/117th-congress/senate-bill/3904/text?q=%7B%22search%22%3A%5B%22rosen%22%2C%22rosen%22%5D%7D&r=1&s=3

[5] https://www.congress.gov/bill/117th-congress/senate-bill/3904/text?q=%7B%22search%22%3A%5B%22rosen%22%2C%22rosen%22%5D%7D&r=1&s=3

[6] https://www.congress.gov/bill/117th-congress/senate-bill/3904/text?q=%7B%22search%22%3A%5B%22rosen%22%2C%22rosen%22%5D%7D&r=1&s=3

[7] https://www.congress.gov/bill/117th-congress/senate-bill/2629/text

[8] https://www.congress.gov/bill/117th-congress/senate-bill/2629/text

[9] https://www.congress.gov/bill/117th-congress/senate-bill/2629/text