May 31, 2022

Hacking Healthcare

TLP White

This week, Hacking Healthcare begins with a reminder that the Health-ISAC is looking to hear from members interested in participating in this year's Hobby Exercise. We then examine a new report from the U.S. Senate that laments the lack of data on ransomware and the government's response to it. We evaluate the report's findings, attempt to glean what its recommendations might mean for follow on actions from Congress, and provide our take as to why things may be looking up.

Welcome back to *Hacking Healthcare*.

1. **Hobby Exercise 2022**

   The third iteration of the Health-ISAC Hobby Exercise is on the horizon. This tabletop exercise is an annual Healthcare and Public Health (HPH) event designed to engage the sector and strategic partners, including those in government, on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for continuous organizational improvement while increasing healthcare sector resiliency. It is named for Oveta Culp Hobby, the first U.S. Secretary of Health, Education, and Welfare.

   Health-ISAC members interested in learning more or wishing to participate should email yours truly, John Banghart (jbanghart@h-isac.org). Only a few spots remain open, so please let us know as soon as possible!

2. **Congressional Report on Ransomware Laments Lack of Data and Federal Response**

   Last Tuesday, the Chairman of the Senate Homeland Security and Governmental Affairs Committee (HSGAC), Gary Peters (D-MI), released a Majority Staff Report on ransomware.[1] The 52-page *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns* outlined the dramatic impacts ransomware attacks are having on the country, including on the healthcare sector. Its findings and recommendations shed light on the current state of affairs as well as the potential avenues congressional members may wish to pursue.

Contents & Context: The report is written in an accessible manner for a non-technical audience, and it begins with a brief background history of ransomware and the role that cryptocurrencies have played in facilitating its continued use by malicious actors. It also succinctly explains the current state of ransomware, the various U.S. governmental policies and regulations that touch on cryptocurrency use, the ways in which ransomware and cryptocurrencies relate to national security issues, and an overview of data collection on this issue.

The report was the product of roughly 10 months of investigation conducted by Democratic staff of the Senate's HSGAC and their methodology included interviews with federal law enforcement and regulatory agencies as well as private companies that assist ransomware victims with ransom demands.[2]

Key Findings: The key findings are unlikely to surprise many of you:[3]

- The federal government lacks comprehensive data on ransomware attacks and use of cryptocurrency in ransom payments.
- Current reporting is fragmented across multiple federal agencies.
- A lack of reliable and comprehensive data on ransomware attacks and cryptocurrency payments limits available tools to guard against national security threats.
- Currently available data on ransomware attacks and cryptocurrency payments limits both private sector and federal government efforts to assist cybercrime victims.

Recommendations: Similarly to the key findings, the report's recommendations are generally things that have routinely been advocated for by congressional members:[4]

- The Administration should swiftly implement the new ransomware attacks and ransom payments reporting mandate.
- The federal government should standardize existing federal data on ransomware incidents and ransom payments to facilitate comprehensive analysis.
- Congress should establish additional public-private initiatives to investigate the ransomware economy.
- Congress should support information sharing regarding ransomware attacks and payments including crowdsourcing initiatives.

Conclusion: The report's conclusion credits the various efforts the Biden administration has launched or announced but highlights that comprehensive data on ransomware attacks and payments are needed to inform those efforts. To address that concern, the report ends by calling for the swift implementation of the cyber incident reporting measures that became law as part of the *Cyber Incident Reporting for Critical Infrastructure Act* on March 15, and for Congress to take an active role in exploring other ways to augment and improve existing lines of effort.

Action & Analysis
MEMBERSHIP REQUIRED

Congress

Tuesday, May 31st:
- No relevant hearings

Wednesday, June 1st:
- No relevant hearings

Thursday, June 2nd:
- 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.

[1] https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf

[2] https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf

[3] https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf

[4] https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf