HACKING HEALTHCARE

Health-ISAC Weekly Blog -- Hacking Healthcare

TLP:WHITE

Feb 16, 2023

This week, Hacking Healthcare explores a new report highlighting the need for cybersecurity regulation harmonization. We highlight the difficulties various stakeholders are encountering with the current lack of alignment as well as the challenges in getting the relevant government entities to cooperate. Next, we assess a new joint government advisory highlighting North Korean cyber threats against the healthcare sector. We breakdown what the advisory says, and then assess the seemingly lackluster response.

Welcome back to *Hacking Healthcare*.

Biden Administration Committee Highlights Need for Cybersecurity Regulation Harmonization

With cyber threats continually growing in scale and sophistication, governments and their regulatory agencies are increasingly looking to impose new and updated cybersecurity regulations on organizations within their jurisdiction. According to one Biden administration committee, this national and international trend is having a detrimental effect on cybersecurity and they have some recommendations.

The President's National Security Telecommunications Advisory Committee (NSTAC) may not be well known to everyone, but it has existed since 1982, and its broad mission includes providing advice to the U.S. government on meeting critical national security and emergency preparedness (NS/EP) challenges. This mission has historically included strong focus on various cybersecurity issues.[i] Its membership is made up of industry representatives, and currently includes numerous executives from a variety of software and telecommunications businesses.

The Problem

The NSTAC's recent draft report was published earlier this month, and one of its key findings highlights the negative aspects of proliferating cybersecurity requirements. The report states that the proliferation of these cybersecurity regulations and requirements are "diverting resources away from improving security to proving compliance with overlapping, redundant and/or inconsistent requirements."[ii]

To help illustrate the point, the report notes that in the past year, 11 countries advanced new or updated critical infrastructure cybersecurity risk requirements and 9 of those also advanced some form of cyber incident reporting.[iii] The NSTAC laments that "these programs often end up diverging across sectors or countries resulting in additional cost without adding security benefit."[iv]

A Possible Solution

The report includes a few recommendations to create policies and processes that will encourage regulatory harmonization within the United States:

- The president should direct agencies wishing to "[issue] a regulatory rulemaking that creates or modifies cybersecurity requirements," and to align those requirements to consensus standards as much as possible. This would include documenting how each requirement aligns to consensus standards or CISA-developed regulatory resources.

- Various government agencies, including the Office of Management and Budget (OMB) and the Office of the National Cyber Director (ONCD) should create processes to assess proposed regulatory rulemakings for cybersecurity standards alignment, assess what opportunities exist to increase harmonization, and coordinate to resolve conflicts.

Action & Analysis

Included with H-ISAC Membership

North Korean Ransomware Continues to Target the Healthcare Sector

A joint advisory released last week has highlighted the persistent threat of the North Korean government (DPRK) to the HPH sector.[vi] The advisory, which reiterates that DPRK threat actors have been actively targeting HPH sector entities with ransomware since at least May of 2021, could understandably draw questions about what the government is doing to respond to continued nation state attacks against critical infrastructure.

The new February 9th joint cybersecurity advisory (CSA) is a product of collaboration between half a dozen U.S. and South Korean government agencies. The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Health and Human Services (HHS), the Republic of Korea (ROK) National Intelligence Service (NIS), and the ROK Defense Security Agency (DSA) all contributed to what is an update to a previous CSA from last July.[vii]

The new CSA provides updated information on the technical details of DPRK operations, mitigation strategies, and an appendix filled with CVE details and indicators of compromise (IOCs). It also reiterates the U.S. government's stance that paying ransoms is highly discouraged, although they add that "the agencies understand that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees, and customers."[viii]

The CSA also attempts to shed some light on goals of the DPRK operations, suggesting that "The authoring agencies assess that an unspecified amount of revenue from these cryptocurrency operations supports DPRK national-level priorities and objectives."[ix] A more complete picture of DPRK cyber threats can be found at CISA's page dedicated to it.[x]

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, February 14th:

- No relevant hearings

Wednesday, January 15th:

- No relevant hearings

Thursday, January 16th:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

[i] https://www.cisa.gov/about-presidents-nstac

[ii] https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2023/feb/cs2023_0015.pdf

[iii] https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2023/feb/cs2023_0015.pdf

[iv] https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2023/feb/cs2023_0015.pdf

[v] https://www.garp.org/risk-intelligence/technology/cyber-risk-landscape-011322

[vi] https://www.cisa.gov/uscert/ncas/alerts/aa23-040a

[vii] https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

[viii] https://www.cisa.gov/uscert/ncas/alerts/aa23-040a

[ix] https://www.cisa.gov/uscert/ncas/alerts/aa23-040a

[x] https://www.cisa.gov/uscert/northkorea

[xi] https://cyberscoop.com/north-korea-ransomware-hospital/

[i] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023

[ii] https://www.cisa.gov/jcdc

[iii] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023

[iv] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023

[v] https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

[vi] https://www.cisa.gov/uscert/ncirp

[vii] https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[viii] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023

[ix] https://healthitsecurity.com/news/white-house-sets-sights-on-new-healthcare-cybersecurity-standards

[x] https://healthitsecurity.com/news/white-house-sets-sights-on-new-healthcare-cybersecurity-standards

[xi] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023

Reference(s)	garp, Cyberscoop, CISA, CISA, CISA, CISA, insidecybersecurity
Report Source(s)	Health-ISAC

Alert ID 55918cff

View Alert

Tags Regulation, Standards, Hacking Healthcare, North Korea

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits

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

Hacking Healthcare

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, 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.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.