May 10, 2022

TLP White

This week, Hacking Healthcare begins with a call for participants for this year's Hobby Exercise. Next, we examine recent statements from American officials in the intelligence and defense community that caution against underestimating the Russian cyber threat. The officials point to serious infrastructure attacks in Ukraine as evidence that critical infrastructure in the United States should keep up its guard. We then dive into two recent documents published from the Health Sector Coordinating Council (HSCC). Specifically, we evaluate what members can gain by assessing their guidance on vulnerability communications as well as guidance on responding to and recovering from cyber incidents that create extended enterprise outages.

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).

2. **U.S. Officials Caution Against Underestimating Russian Cyber Threat**

   For years prior to the most recent Russian invasion of Ukraine, it wasn't uncommon for some policymakers and analysts to warn that conflicts involving established cyber powers could lead to "cyber war." However, roughly two months into the Russian

invasion, there have been few notable destructive attacks on Western critical infrastructure. While some have begun to shift to the narrative that "cyber war" and destructive cyber capabilities have been exaggerated, prominent U.S. government officials appear to strongly disagree.

Speaking at an event last week, Gen. Paul Nakasone, dual-hatted as both the Director of the National Security Agency (NSA) and head of U.S. Cyber Command, cautioned against narratives that Russian cyber capabilities were overblown or had not had an impact. General Nakasone stated, "This idea that nothing has happened is not right," and that "there have been destructive attacks, a series of infrastructure attacks [where] satellite communications have been targeted."[1]

These comments were further backed up by NSA Director of Cybersecurity Rob Joyce, who previously served as the U.S. Homeland Security Advisor. Joyce is reported to have stated that "there was some really, extra-unethical cyber pressure brought to Ukrainian internet networks by Russia. You know, don't be dismissive that just because that didn't come directly at the U.S. as much as it did Ukraine that we didn't have a major event."[2]

The NSA and U.S. Cyber Command have first-hand knowledge of these attacks as they have been heavily involved in Ukraine. This includes cyber teams sent on "hunt forward" operations in other countries to help defensive cyber efforts "identify malware and tradecraft our adversaries were using."[3]

Action & Analysis
Membership required

3. Healthcare and Public Health Sector Coordinating Council (HSCC) Publishes New Cybersecurity Guidance

The HSCC, of which Health-ISAC is a contributing member, recently published two useful healthcare cybersecurity documents that members are encouraged to read. The two documents, *MedTech Vulnerability Communications Toolkit* and *Operational Continuity –Cyber Incident*, offer guidance on two critical aspects of cybersecurity in the Healthcare and Public Health Sector.[4, 5]

<u>MedTech Vulnerability Communications Toolkit</u>

The *MedTech Vulnerability Communications Toolkit* helpfully expands upon the vulnerability disclosure topic we covered last week. This particular document is designed to "support effective vulnerability communications processes and improve the clarity of messaging to nontechnical audiences, such as patients and healthcare professionals."[6]

At 18 pages, the *MedTech Vulnerability Communications Toolkit* covers an overview of vulnerability communications, vulnerability categorization, and a helpful vulnerability

communications prioritization table. Furthermore, the document provides a valuable section on terminology and recommendations for communicating sometimes obscure technical language.

While this version of the document was written with the intent "to help medical device manufacturers formulate and communicate vulnerability disclosures," the HSCC has stated that "future versions will focus on more technically oriented audiences in biomedical engineering and cybersecurity roles."[7]

Operational Continuity-Cyber Incident (OCCI)

Operational continuity is key in all critical infrastructure sectors, but especially so in the healthcare and public health sector, where patient wellbeing is often directly tied to uninterrupted service. The OCCI toolkit is a "flexible template for operational staff and executive management of healthcare organizations to respond to and recover from an extended enterprise outage due to a serious cyber-attack."[8]

The 10-page document is an easy-to-read checklist that "outlines recommended initial (first 12 hours) actions and considerations during cybersecurity incidents." It provides a breakdown of actions and considerations across various roles, from the "incident commander" to medical-technical specialists and Public Information Officers and more. While collectively designed by numerous HSCC contributors, it's intended to be "modified or refined according to an organization's size, resources, complexity, and capabilities."

Both documents are freely available on the HSCC website.

Action & Analysis
Membership required

Congress

Tuesday, May 10th:
- No relevant hearings

Wednesday, May 11th:
- House of Representatives – Committee on Science, Space, and Technology: Securing the Digital Commons: Open-Source Software Cybersecurity

Thursday, May 12th:
- 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.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/

[2] https://www.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/

[3] https://www.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/

[4] https://healthsectorcouncil.org/wp-content/uploads/2022/04/Operational-Continuity-Cyber-Incident-OCCI.pdf

[5] https://healthsectorcouncil.org/wp-content/uploads/2022/04/Health-Industry-MedTech-Vulnerability-Communications-Toolkit.pdf

[6] https://healthsectorcouncil.org/wp-content/uploads/2022/04/Health-Industry-MedTech-Vulnerability-Communications-Toolkit.pdf

[7] https://healthsectorcouncil.org/wp-content/uploads/2022/04/Health-Industry-MedTech-Vulnerability-Communications-Toolkit.pdf

[8] https://healthsectorcouncil.org/04-29-2022-occi-checklist-published/