Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 55ad3414 | Jan 25, 2023, 02:22 PM

This week, Hacking Healthcare begins with an update on the National Institute of Standards and Technology's (NIST) ongoing revision of the *Framework for Improving Critical Infrastructure Cybersecurity*, better known as the NIST *Cybersecurity Framework* (CSF). We let you know where things stand and how you can engage in shaping CSF 2.0's development. Next, we call attention to new developments in Europe that should help the global law enforcement crackdown on cyber criminals.

Welcome back to *Hacking Healthcare*.

Health-ISAC Monthly Threat Brief

Before we begin, we would like to remind all Health-ISAC members that next Tuesday, the Health-ISAC will be holding its monthly Threat Brief. This hour-long presentation from Health-ISAC staff and partners briefs members on current and emerging technical, physical, legal, and regulatory threats to the HPH sector. The Threat Brief is for Health-ISAC members only, and we would like to encourage you to attend.

The Latest NIST CSF 2.0 Update

As a quick reminder, a 2013 Obama-era executive order tasked NIST with "work[ing] with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure."[i] The result was the CSF, a flexible cybersecurity framework that could be adapted to a wide range of industries, organizational structures, and sizes. Since its issuance in 2014 and an update to version 1.1 in 2018, it has had global adoption far beyond just critical infrastructure and it has been further augmented by CSF profiles that tackle specific use cases or threats.

Since the 2018 update, the threat landscape and technologies that the CSF addresses have continued to evolve. As such, NIST has begun a process to solicit outside feedback on what the CSF 2.0 update should look like.

There are three developments worth noting:

Concept Paper[ii]

Just recently, NIST published the Cybersecurity Framework Concept paper, which is meant to outline the potential changes that NIST is considering and to solicit feedback on those items. Some of the changes being mulled over by NIST include:

- Renaming and refocusing of the CSF away from a critical infrastructure sector focus toward something that is "helpful to organizations regardless of sector, type, or size";
- Adding a section on governance that will cover topics, such as risk assessment, risk tolerance determination, cybersecurity policy and procedures, and cybersecurity roles and responsibilities;
- Increasing its focus on Cyber-Supply Chain Risk Management;
- Clarification on how the various NIST frameworks connect with one another;
- Increased support for measurement and assessment.

Virtual Workshop[iii]

On February 15th, NIST is hosting their second all-day workshop to discuss many of the potential changes that were outlined in the concept paper as well as previous feedback from the first workshop and RFI comments. The workshop is virtual only, but attendees will be able to interact via Slack.

In-Person Working Sessions

On February 22nd and 23rd, there will be in-person working sessions at the National Cybersecurity Center of Excellence (NCCoE) in Maryland. These working sessions will cover similar content to the virtual workshop but are intended to be for individuals "with hands-on implementation experience with the NIST Cybersecurity Framework."[iv]

Action & Analysis

The NIST CSF has shown itself to be a highly valuable and effective tool, especially for organizations looking for trustworthy guidance for growing their cybersecurity maturity. In general, the CSF 2.0 revision looks likely to become more comprehensive and, as a result, slightly larger and more complex. There is some reasonable concern that an increase in complexity could detract from the approachability of the CSF, which has been one of its hallmarks. Further development of sector-specific Profiles could help to address this and will certainly be a subject for conversation.

While it appears that the current proposals will likely strengthen the CSF to better accommodate the technology and threat landscape that now exist, healthcare sector organizations should still consider providing their unique perspective on the proposed changes. For example, do you feel that the proposed widening of scope detracts from the value for critical infrastructure entities? Should supply chain risk management be its own function or remain as part of the existing structure?

There is also value for those that are leveraging more healthcare-oriented guidance, such as the industry and government collaboration that developed into the *Health Industry Cybersecurity Practices* (HICP). For example, the NIST CSF has undoubtably helped in raising the overall cybersecurity of the digital ecosystem and can be a valuable tool in communicating about risk with industry peers and partners. In this regard, it has helped move many organizations down a path toward cybersecurity maturity beyond what might be required by laws and regulations.

Regardless, the NIST CSF revision is a welcome development that should benefit the healthcare sector. Your organization's need to prioritize engagement will likely depend on whether you use the current iteration of the framework, or whether you have third-party partners or suppliers who do, and you would like to understand what it would mean for them.

International Cooperation on Cybercrime Increases

One of the more daunting challenges in combating cybercrime is navigating the web of jurisdictional challenges and building the necessary trust and familiarity that's required to conduct multinational law enforcement operations. Some progress was made on this front recently with the EU's Parliament noting its support for a new addition to the Council of Europe's *Budapest Convention on Cybercrime* (BCC).

If you've never heard of the BCC or the Council of Europe, let's take a moment to get you up to speed The Council of Europe is an organization focused on a variety of human rights issues, the promotion of democracy, and the rule of law.[v] Despite its name, the Council of Europe is not a European Union organization, although many of its member states are. It has been a significant policy actor since its founding in 1949.

The BCC, signed in 2001, is described by the Council of Europe as "the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with…computer-related fraud,…and violations of network security."[vi] Furthermore, the primary aim of the BCC is to "pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation."[vii] The 22-page document has been ratified by 67 states, including the U.S. and most of Europe.

The new addition, referred to as the *Second Additional Protocol*, seeks to revise provisions of the original BCC text to ensure that it can adequately address today's threat landscape.[viii] Provisions include improving the ability to share electronic data/evidence across borders, increasing the facilitation of joint investigations, and allowing for criminal justice authorities from BCC signatories to directly contact internet service providers in other countries for "pertinent" information.[ix]

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, January 24th:

- No relevant hearings

Wednesday, January 25th:

- No relevant hearings

Thursday, January 26th:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

[i] https://www.nist.gov/cyberframework/getting-started#background

[ii] https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

[iii] https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2

[iv] https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-person-working-sessions

[v] https://www.coe.int/en/web/portal/home

[vi] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[vii] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[viii] https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d

[ix] https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d

[x] https://www.eff.org/deeplinks/2022/12/global-cybercrime-and-government-access-user-data-across-borders-2022-year-review

---

Reference | References

NIST-CSF
EFF
NIST-CSF
NIST-CSF
coe
coe
coe
NIST-CSF

Report Source(s)

Health-ISAC

Tags

Standards, Hacking Healthcare, NIST, NIST Cybersecurity Framework (CSF), Law Enforcement, Europe

---

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.