Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare™ | TLP:WHITE | Alert ID : 1f35f58e | Aug 24, 2023, 03:59 PM

This week, *Hacking Healthcare*™ examines the newest draft of the Cybersecurity Framework from the National Institute of Standards and Technology (NIST). We break down the changes to the current framework, how the framework intersects with the healthcare sector, and how members can influence its development going forward.

Welcome back to *Hacking Healthcare*™

Join us for the Monthly Threat Briefing

But first, as a reminder, next Tuesday is the Health-ISAC's monthly threat briefing. Come join your fellow Health-ISAC members as Health-ISAC staff and partner organizations provide an overview of the threat landscape. Presentations include an assessment of emerging malware, APT trends, legal and regulatory issues, physical security concerns, and more. We encourage all Health-ISAC members to take advantage of this service.

NIST Makes Progress on Cybersecurity Framework 2.0

The NIST Cybersecurity Framework, often simply referred to as the CSF, has gained widespread global adoption across numerous sectors since its initial release, including within healthcare. Earlier this month, NIST released the public draft of the newest revision to this framework. What has changed in version 2.0 and how might it affect the healthcare sector entities that make use of it?

To begin, let's quickly provide some context on where the CSF came from and why version 1.1 was in need of a refresh before diving into what's new.

Background

The NIST CSF was born out of a 2013 US President Obama Executive Order that focused on improving critical infrastructure cybersecurity.[i] A provision of that document called for the development of a baseline framework that would reduce cyber risk to critical infrastructure. That effort evolved into the CSF as we know it today, a flexible framework designed to be agnostic to an organization's size, sector, or organizational setup and with application beyond just critical infrastructure.[ii]

Since version 1.0 released in 2014, the CSF has undergone only one significant update back in April of 2018, and while the current CSF 1.1 continues to effectively help mitigate cybersecurity risks, stakeholders have recognized the need for adjustments to accommodate the evolving threat landscape and forthcoming cybersecurity challenges. That recognition led NIST to launch an effort to revise the CSF.

That effort began in February of 2022 with the release of a request for information (RFI) to solicit feedback from stakeholders on where improvements needed to be made. In framing the discussion, NIST highlighted that the widespread adoption of the framework, especially among small and medium-sized entities (SMEs) and globally, and the increasingly important aspect of supply chain risk management, were areas that needed additional consideration.

Thus far, NIST has received hundreds of comments from relevant stakeholders through the RFI, follow-on concept paper, various workshops and working sessions, and an initial draft, all of which has informed the newly released Draft 2.0.[iii]

What's New

The CSF 2.0 brings a stronger focus on implementing the framework. Practical examples of implementation provide actionable steps for organizations to realize the objectives of the CSF subcategories. Moreover, an upcoming online tool will visually map the relationship between CSF core elements and relevant, updateable references.[iv] Additionally, the significance of continuous cybersecurity measurement and assessment is highlighted through the new 'improvement' category in the Identify function, that offers guidance on devising and updating security action plans.

Arguably the most noteworthy addition to the CSF is the new "Govern" function, that emphasizes cybersecurity supply chain risk management. The Govern function encompasses six categories: organizational context; risk management strategy; C-SCRM (Cybersecurity Supply Chain Risk Management); roles, responsibilities, and authorities; policies, processes, and procedures, along with oversight.[v]
Within the new Govern function, the supply chain risk management category and its subcategories define outcomes for establishing, supervising, monitoring, and enhancing cybersecurity supply chain risk management initiatives. Furthermore, the categories and subcategories within the remaining five functions enable organizations to determine fundamental cybersecurity prerequisites for primary suppliers and lower-tier suppliers, contingent on supplier criticality and risk evaluations.
This CSF update also enables suppliers to formulate targeted profiles to inform decisions regarding procuring products and services based on their cybersecurity levels. These profiles can help track any residual risk linked to the product or service through periodic assessments and testing, therefore strengthening cybersecurity outcomes across the supply chain.

Action & Analysis
****Included with Health-ISAC Membership****

Congress

Tuesday, August 22
No relevant hearings

Wednesday, August 23
No relevant meetings

Thursday, August 24
No relevant meetings

International Hearings/Meetings
No relevant meetings

EU
No relevant meetings

Contact us: follow @HealthISAC and email at contact@h-isac.org

About the Author

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat Briefing.

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

Tim can be reached at tmcgiff@h-isac.org and tmcgiff@venable.com

[i] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[ii] https://www.nist.gov/cyberframework/framework
[iii] https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd
[iv] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf
[v] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf
[vi] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

[vii] While developed by the Financial Services Sector Coordinating Council (FSSCC), The Financial Sector Specific Cybersecurity Profile is now maintained, updated, and managed by the Cyber Risk Institute "CRI" and can be found at: https://cyberriskinstitute.org/the-profile/

[viii] https://csrc.nist.gov/pubs/ir/8374/final

[ix] https://www.cybersecuritycoalition.org/frameworks/botnet-profile

[x] https://www.cybersecuritycoalition.org/frameworks/ddos-profile

[xi] https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx

[xii] https://healthsectorcouncil.org/hph-sector-cybersecurity-framework-implementation-guide-health-industry-and-hhs-joint-publication/

[xiii] https://405d.hhs.gov/information

[xiv] https://csrc.nist.gov/News/2023/nist-releases-cybersecurity-framework-2-0-draft

Report Source(s)

Health-ISAC

Reference | References

NIST-CSF
Health Industry Cybersecurity Practices
cybersecuritycoalition
HHS
cyberriskinstitute
NIST-CSF
NIST-CSF
Health-ISAC
cyberriskinstitute
archives
NIST-CSF
NIST-CSF
cybersecuritycoalition
HHS

Tags

Hacking Healthcare, NIST, NIST Cybersecurity Framework (CSF), Risk Management

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.

For Questions or Comments:

Please email us at toc@h-isac.org