Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ **TLP:WHITE** **Alert Id: 6c036b80** **2024-03-01 16:26:07**

This week, *Hacking Healthcare*™ examines the recent publication of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) update from v1.1 to v2.0. We briefly examine what's new, and then we dig into what the changes mean, the international impact this revision is likely to have, and some considerations for Health-ISAC members looking to adopt or transition to v2.0.

Welcome back to *Hacking Healthcare*™.

NIST Publishes CSF 2.0

After roughly a decade since v1.0 was released, the NIST CSF has undergone a major revision that was finalized by NIST on Monday.[i], [ii] The new CSF v2.0 includes quality of life improvements, makes clarifications, and adds necessary substantive revisions to keep the framework relevant, while retaining the effective general structure with which users are familiar with.

What Is the NIST CSF

For those unfamiliar with the NIST CSF, it was originally published in 2014 as a framework to help organizations manage and reduce cyber risk. While it was specifically targeted at U.S. critical infrastructure sectors, it was ultimately designed to be agnostic to an entity's size, sector, and organizational structure and was meant to be helpful and accessible to organizations regardless of where they are in their cybersecurity maturity journey. The NIST CSF has been extremely successful across industries and has had a global impact.

What's New?

The largest differences can be found in the following areas:

- **Governance & Supply Chain Risk**: CSF 2.0 introduces a new function, Govern, that is described as covering how an organization's "cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.[iii] The Govern function also sees an elevation of supply chain considerations with the inclusion of Cybersecurity Supply Chain Risk Management category and ten subcategories.

- **References & New Tools**: One change that will be strikingly apparent is the removal of informative references from each subcategory. While the CSF v1.1 conveniently placed these references in the right-most column of the document, NIST has eliminated this in favor of hosting the references online at its new Cybersecurity and Privacy Reference Tool (CPRT).[iv] In general, there are a few new tools that CSF v2.0 will look to take more advantage of, including the CPRT and CSF 2.0 Implementation Examples.

Actions & Analysis

Included with Health-ISAC Membership

Upcoming International Hearings/Meetings

EU

- No relevant meetings at this time

US

- No relevant meetings at this time

Rest of World

- Health-ISAC APAC Summit (3/19 - 3/21)

[i] https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

[ii] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[iii] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[iv] https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home

[v] https://csrc.nist.gov/projects/olir

[vi] https://www.nist.gov/privacy-framework

[vii] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

[viii] https://www.nist.gov/cyberframework/csf-11-archive/translations#csf-11

[ix] https://www.nist.gov/cyberframework/success-stories

[x] https://www.nist.gov/cyberframework/csf-11-international-resources

[xi] https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

[xii] https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

[xiii] https://www.nist.gov/cyberframework/csf-11-archive/translations#csf-20

[xiv] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf

Reference(s): NIST-CSF, NIST-CSF, NIST-CSF, NIST-CSF, NIST-CSF, NIST-CSF, NIST-CSF, NIST-CSF, NIST-CSF, NIST-CSF, NIST-CSF

Report Source(s): Health-ISAC

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

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■:

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@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