Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 73242a18 | May 09, 2023, 04:05 PM

This week, *Hacking Healthcare* begins with a guest essay on advancing business, operational, and financial alignment to cybersecurity threats, which ties into the Securities and Exchange Commission's recently proposed cybersecurity rule requirements. Next, we provide an update on the newest developments surrounding the NIST Cybersecurity Framework revision.

Welcome back to *Hacking Healthcare*.

The Call for Business, Operational, and Financial Aligned Cybersecurity Risk Governance in Healthcare – *Guest Author: Chris Hetner*

The current cybersecurity ecosystem (people, process, technology) is largely focused on addressing technical-level threats used to inform measures to mitigate risk. While the cybersecurity ecosystem continues to evolve, InfoSec teams still lack the ability to contextualize cyber threats and incidents to business, operational, and financial exposures. This lack of capability is problematic for the industry, especially for those publicly traded companies in the United States — including healthcare organizations — given the heightened cyber risk- disclosure requirements driven by the Securities and Exchange Commission (SEC).

Contained in the proposed SEC rule, publicly traded companies are required to report within four days once incidents are deemed to be "material."[i] The "material" determination is influenced by the incident's impact on the company's business, operations and financial condition. Below is an enumeration of the types of business and financial factors that should be contemplated when determining incident materiality:

The types of costs and adverse consequences that companies may incur or experience as a result of a cybersecurity incident include the following:

- Costs due to business interruption, decreases in production, and delays in product launches;
- Payments to meet ransom and other extortion demands;
- Remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;
- Increased cybersecurity protection costs, which may include increased insurance premiums and the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third-party experts and consultants;
- Lost revenues resulting from intellectual property theft and the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;

- Litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;

- Harm to employees and customers, violation of privacy laws, and reputational damage that adversely affects customer or investor confidence; and

- Damage to the company's competitiveness, stock price, and long-term shareholder value.

Per the SEC, "As indicated by the examples enumerated above, the potential costs and damage that can stem from a material cybersecurity incident are extensive. Many smaller companies have been targets of cybersecurity attacks so severe that the companies have gone out of business as a result. These direct and indirect financial costs can negatively impact stock prices, as well as short-term and long-term shareholder value."[ii]

Action & Analysis
Included with Health- ISAC Membership

NIST Releases a Discussion Draft for the Revised Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was released in 2014 following an executive order on improving critical infrastructure cybersecurity under the Obama administration.[iii] The framework categorizes cybersecurity activities to help agencies manage risk by organizing information, enabling risk-management decisions, addressing threats, and learning from previous activities.[iv] Although voluntary by nature, it has been adopted for use by many organizations within the healthcare sector as a means to understand and mitigate cybersecurity risks.

Acknowledging that the threats and technologies are ever-changing, NIST has begun the process of updating the CSF to version 2.0. The most recent development in this process has been the release of a discussion draft with proposed changes that seek to address current and emerging cyber trends, while remaining aligned with the approach and best security practices it's already known for.[v]

For those not familiar, the CSF is made up of three main components: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is described as a "set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure" and is divided into the following functions: Identify, Protect, Detect, Respond, and Recover.[vi] Within these five functions is a number of subcategories that define the practices organizations should take into consideration when designing their own cybersecurity program.

The new preliminary discussion draft identifies the potential functions, categories, and subcategories of the NIST CSF 2.0 Core, and is intended to increase transparency during the revision process by generating discussion and suggestions from industry on ways to improve the framework.[vii]

There are a few notable changes being proposed in the CSF 2.0 draft:

1. **A new Governance function** addresses organization context, risk-management strategies, policies, procedures, roles, and responsibilities.[viii] Its addition is meant to emphasize the importance of developing the appropriate governing polices for a cybersecurity program, and to clearly define expectations for subsequent positions.

2. **New subcategories.** The 2.0 draft also focuses on the resiliency of technology infrastructure through a new Protect function category, and incident response management and incident forensic categories in the Respond and Recover functions.[1]

3. **Expanding cybersecurity supply chain risk management (C-SCRM) outcomes**. As supply chain attacks continue to rise, especially in the healthcare industry,[ix] NIST has proposed several ways to expand focus on this topic by including a supply chain risk-management focus under the Identify function.[x]

4. **Implementation examples**: In order to make the CSF 2.0 scalable for organizations of any size, the new draft includes outcomes applicable to a wide array of organizations and removes language specific to critical infrastructure across the core.[xi] This is meant to help entities achieve the intended outcomes of the subcategories.

The CSF has served as a useful resource for those in the healthcare industry, especially with the rise of digital technologies, cyber-physical systems, and Internet of Things integrating into hospitals and healthcare facilities.[xii] The increased connectivity of medical devices and hospital networks has made protecting against cyberattacks a priority in this industry.

NIST is seeking feedback on whether the CSF 2.0 core draft accurately addresses challenges that organizations are facing and is requesting concrete suggestions on improvements to the draft as well as revisions to functions, categories, and subcategories.[xiii]

Action and Analysis
Included with Health-ISAC Membership

Conclusion

As always, we encourage our members to leverage this call for views to further enable the CSF 2.0 to provide thoughtful guidance relevant to the cybersecurity challenges currently faced in the healthcare industry. While it will remain a sector-agnostic document, if there are areas of concern that you don't feel are properly represented, it is always a good idea to bring those issues to NIST's attention.

Congress
Tuesday, May 9
No relevant hearings

Wednesday, May 10
No relevant meetings

Thursday, May 11
No relevant hearings

International Hearings/Meetings
No relevant meetings

[1]https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
[i] https://www.sec.gov/rules/proposed/2022/33-11038.pdf
[ii] https://www.sec.gov/rules/proposed/2022/33-11038.pdf
[iii] https://healthitsecurity.com/features/breaking-down-the-nist-cybersecurity-framework-how-it-applies-to-healthcare
[iv] https://www.gsa.gov/technology/technology-products-services/it-security/nist-cybersecurity-framework-csf
[v]https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
[vi] https://healthitsecurity.com/features/breaking-down-the-nist-cybersecurity-framework-how-it-applies-to-healthcare

[vii]https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
[viii]https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
[ix] https://www.tripwire.com/state-of-security/healthcare-supply-chain-attacks-raise-cyber-security-alarm#:~:text=The%20healthcare%20sector%20has%20become,first%20half%20of%20the%20year.
[x]https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
[xi]https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
[xii] https://industrialcyber.co/medical/hhs-hscc-publish-guidance-to-assist-healthcare-sectors-align-cybersecurity-programs-with-nist-csf/
[xiii]https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
[xiv] https://www.nist.gov/system/files/documents/2022/05/03/04-25-2022%20-%20HIMSS_Redacted.pdf
[xv] https://www.nist.gov/system/files/documents/2022/05/03/04-25-2022%20-%20HIMSS_Redacted.pdf
[xvi]https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf

---

Reference | References

NIST-CSF
Tripwire
Health-ISAC
gsa
industrialcyber
sec
Health IT Security
NIST-CSF

Report Source(s)

Health-ISAC

Tags

Hacking Healthcare, NIST, SEC, NIST Cybersecurity Framework (CSF), Governance

---

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.