December 14th, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins by breaking down the issue of cyber incident reporting timelines and makes the case for engagement with regulators and legislators. Next, we examine reports that the National Institute of Science and Technology (NIST) is looking to begin updating its well-regarded cybersecurity framework early next year, and we explore what the new update may focus on. Finally, we cover the announcement of a new healthcare cybersecurity website launched by Health and Human Services (HHS). Welcome back to *Hacking Healthcare*.

***Author's Note:** Hacking Healthcare will be on vacation beginning next week but will return in January. We hope the last few weeks of 2021 treat you well and that you get at least a small break from the daily cybersecurity grind. Thanks for reading us every week, and we look forward to continuing!*

1. The Variance of Cyber Incident Reporting Timelines

A new rule imposed in mid-November on the banking sector in the United States will require the reporting of major cybersecurity incidents to the federal government within 36 hours. This new rule comes at a time when various legislative and regulatory bodies across the globe are considering what kind of timelines and reporting requirements are appropriate for cyber incident reporting. The relatively short window until the rule goes into effect may make it an interesting test case to study as debates continue over how long organizations should reasonably be given before they should be required to provide a cyber incident report.

Formally titled *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, the final rule has an effective date on April 1st and a compliance date of May 1st of this coming year.[1] Given the uncertainty surrounding the quick passage of broader congressional cyber incident reporting, this rule may provide an imperfect case study for how a heavily regulated and generally cybersecurity mature industry handles the relatively short turnaround time.

Legislators and regulators across the globe have yet to coalesce around a specific reporting timeframe, with most efforts somewhere between 12 and 72 hours. Some of the more recent and significant pieces of legislation that include cyber incident reporting timelines are:

- The European Union's (EU) Network and Information Security (NIS)2 Directive is still in process, but the current proposed timing is 24 hours to report availability issues and 72 hours for integrity issues.[2]

- The Australian Critical Infrastructure Bill, which is also still in process, requires critical infrastructure to report a critical cybersecurity incident within 12 hours after becoming aware of an event, and within 72 hours for other cybersecurity incidents.[3]

- Within the United States, the cyber incident reporting provision that failed to make the final version of the 2022 National Defense Authorization Act (NDAA) would have required covered entities to report within 72 hours after reasonably believing a covered cyber incident had occurred or within 24 hours after making a ransomware payment.[4]

- Within the United States, the Department of Homeland Security recently announced two new security directives for the transportation sector. Included is the requirement that owners and operators of covered rail entities must report cybersecurity incidents within 24 hours after identifying one.[5]

Action & Analysis
Included with H-ISAC Membership

2. NIST CSF Update

In 2013, Presidential Executive Order 13636 directed NIST to "work with stakeholders to develop a voluntary framework based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure."[6] The NIST Cybersecurity Framework (CSF) was the result of that particular effort. In a move to strengthen it and ensure it maintains relevancy in an ever-changing cyber landscape, NIST has confirmed that 2022 will be the start of an update process for the framework.

Since its initial version 1.0 release in February 2014, the NIST CSF has been updated just once, with the current version 1.1 being finalized in 2018. NIST is planning to file a Request for Information (RFI) early in 2022 that will kickstart the update process. In a meeting of the NIST Information Security and Privacy Advisory Board, Kevin Stine, chief of the applied cybersecurity division of NIST's Information Technology Laboratory is quoted as saying that the RFI will focus on three areas:[7]

- Whether there are new features to consider for helping organizations better manage their risks

- Opportunities to align the CSF with other resources both internally and externally
- Challenges organizations face from a technology supply chain perspective.

Not much else is known about the timing or process, but we'll be keeping an eye out and let you know what we learn as it unfolds.

Action & Analysis
Included with H-ISAC Membership

3. HHS launches New Healthcare Cybersecurity Website

On December 1st, HHS successfully launched a new website for the purpose of "Aligning Health Care Industry Security Approaches."[8] The new 405(d) program website is presented as a useful place for organization's looking for additional "resources, products, and tools that help raise awareness and provide vetted cybersecurity practices."[9]

The new website is the culmination of an effort that began years ago with the passage of the Cybersecurity Act of 2015. Provisions in that bill led to HHS convening the 405(d) Task Group, named after the provision of the bill, in 2017 in order to "enhance cybersecurity and align industry approaches by developing a common set of voluntary, consensus-based, and industry-led cybersecurity guidelines, practices, methodologies, procedures, and processes that healthcare organizations can use."[10] The group is comprised of over 150 individuals from the public and private sector, including information security officers, medical professionals, and privacy experts.[11, 12]

Visitors to the website will find tabs that provide context for the 405(d) program, comprehensive news and awareness resources, opportunities for involvement, and a long list of all products, publications, and other materials the group has produced alongside additional outside links. There are also placeholders for additional sections on "Enterprise Security Risk Management" and a stated commitment to continue to develop new cybersecurity resources.

Action & Analysis
Included with H-ISAC Membership

Congress

Tuesday, December 14th:
- No relevant hearings

Wednesday, December 15th:
- No relevant hearings

Thursday, December 16th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

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.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank

[2] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[3]https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6657_aspassed/toc_pdf/20182b01.pdf;fileType=application%2Fpdf

[4] https://www.govexec.com/media/mir21f87_-_amendment_as_filed.pdf

[5] https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf

[6] https://www.nist.gov/cyberframework/getting-started

[7] https://www.nextgov.com/cybersecurity/2021/12/nist-outlines-request-information-toward-new-cybersecurity-framework/187427/

[8] https://www.hhs.gov/about/news/2021/12/01/hhs-launches-website-405d-aligning-health-care-industry-security-approaches-program.html

[9] https://405d.hhs.gov/public/navigation/aboutUs

[10] https://www.hhs.gov/about/news/2021/12/01/hhs-launches-website-405d-aligning-health-care-industry-security-approaches-program.html

[11] https://www.nist.gov/system/files/documents/2018/10/18/hhs_fact_sheet_-_csa_405d_cleared.pdf

[12] https://www.hhs.gov/about/news/2021/12/01/hhs-launches-website-405d-aligning-health-care-industry-security-approaches-program.html