SHARING SINCE 2010 Health-ISAC™
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare ○ TLP:WHITE Alert ID : b0103bb8 Oct 19, 2023, 01:59 PM

Interest in broadening and deepening the expectations and responsibilities of senior leadership when it comes to cybersecurity is increasingly taking hold in policy circles globally and in particular in the US and Europe.

This week, *Hacking Healthcare*^{TM} explores a Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Draft Report on how CISA could encourage corporate cybersecurity responsibilities among private sector senior leadership. We review the contents of the Draft Report, how it may influence CISA's engagement with Health-ISAC members, and which actions Health-ISAC members may hope to consider as a result.

Welcome back to *Hacking Healthcare*^{TM}.

CISA Cybersecurity Advisory Board Makes Case for Corporate Cyber Responsibility

The past few years have witnessed an increased interest by policy and lawmakers to incentivize senior leadership of organizations to become more educated on cyber risks and to take greater responsibility for the preparedness of their organizations to defend against, and recover from, cyber incidents. A recent publication from the CISA Corporate Cyber Responsibility (CCR) Subcommittee sheds some light on how CISA and its current private sector partners on the CASC view the issue. Let's explore what they have come up with and how it might impact the healthcare sector.

<u>What are the CSAC and the CCR?</u>

In June 2021, CISA established the CSAC pursuant to a Congressional mandate in the FY2021 National Defense Authorization Act (NDAA).[i] As an independent advisory board, the CSAC provides strategic and actionable consensus recommendations to CISA Director, Jen Easterly, on pertinent cybersecurity challenges. Although the CSAC is obligated to meet at least twice per year, it often meets more frequently, having held four quarterly meetings in 2022.

Currently, the CSAC comprises 33 members—each a subject matter expert in their respective critical infrastructure sectors—and is chaired by Ron Green, Chief Security Officer at Mastercard. Of the CSAC's 33 members, two have extensive experience in the healthcare sector: Marene Allison, former Global Chief

Information Security Officer for Johnson & Johnson, and Brian Gragnolati, President & CEO of Atlantic Health System.

The CSAC also contains six subcommittees, which collectively met 94 times in 2022. The CCR Subcommittee is designated to explore strategies to improve CSAC's engagement with corporate boards and to encourage corporate leadership to incorporate cyber safety and responsibility in their decision-making processes. The Subcommittee is currently chaired by Dave DeWalt, CEO of NightDragon, a venture capital firm focused on developing cybersecurity and privacy companies. Notably, the CCR Subcommittee does not include any representation from the healthcare industry. The Subcommittee did interview various industry representatives including Denise Anderson, Health-ISAC President and CEO for input on the topic.

The Draft Report on Corporate Cyber Responsibility

In the Draft Report, the CCR subcommittee divided its recommendations into four main pillars: 1) Board Member Education; 2) Measurement; 3) Responsibility; and 4) Sustained Leadership and Collaboration. For the purposes of *Hacking Healthcare*TM, we will focus most of our analysis on the third pillar of "Responsibility."

In describing the Responsibility pillar, the CCR subcommittee says, "there must be clearer lines of responsibility and accountability drawn between stakeholders responsible for ensuring the cyber resilience of corporations."[ii] This conversation has been accelerated since the Securities and Exchange Commission (SEC) adopted a new final rule on July 26, 2023, requiring its registrants to disclose information related to an organization's risk management processes and how senior leadership is involved.[iii]

In its Draft Report, the CCR Subcommittee makes numerous recommendations for CISA to consider following up on, including:

- Help directors build better understanding of business impact. CISA should create materials that explain the loss and liability to companies for certain types of cybersecurity events.
- Create methods for directly linking certain actions and non-actions, as well as investments and failure to invest, to potential cyber risk and then, in turn, communicate that risk in dollar amounts.
- Conduct and publish research on this question and in doing so, ask the industry to collaborate and provide data.
- Generate more relevant and accurate data. CISA should create such a data set and continually update it, with assistance from the Information Sharing and Analysis Centers (ISACs) and the insurance industry.
- Create Performance Goals for Cyber-Responsible Boards. CISA, in collaboration with relevant stakeholders, should create Performance Goals that contain a set of principles and accompanying best practices for cyber responsible boards to help directors focus their efforts and attention and help their firms improve cybersecurity outcomes.

- Greater clarity on due diligence and liability. In addition to efforts to support the adoption of the CPGs as the common set of controls for publicly traded companies, CISA should create guidance for directors on what constitutes due diligence when it comes to cybersecurity.
- CISA should help define for boards and management the legal frameworks to help them navigate personal and organizational liability issues.
- CISA should simultaneously work with relevant federal agencies and stakeholders to determine what barriers exist to shareholders pursuing class action lawsuits against companies for weak cybersecurity programs that result in harm to them or their customers.

The recommendations are outlined in more depth within the report for those interested.

So, what does this mean for Health-ISAC members at this time?

Action & Analysis
Included with Health-ISAC Membership

Congress
Tuesday, October 17
No relevant meetings

Wednesday, October 18
No relevant meetings

Thursday, October 19
No relevant meetings

International Hearings/Meetings

[i] https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf
[ii] https://www.cisa.gov/sites/default/files/2023-09/CSAC_CCR_September-Recommendations_20230913_508_1.pdf
[iii] https://www.sec.gov/news/press-release/2023-139
[iv] https://www.sec.gov/files/rules/final/2023/33-11216.pdf
[v] https://eur-lex.europa.eu/eli/dir/2022/2555
[vi] https://cyberscoop.com/wp-content/uploads/sites/3/2023/09/CSAC_September-Quarterly-Meeting_Draft-Recommendations_20230913.pdf

Report Source(s)
Health-ISAC

Reference | References

sec
Cyberscoop
Europa Analytics
Health-ISAC
sec
CISA
congress

Tags

Corporate Responsibility, Hacking Healthcare, law

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 Councils 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 Councils 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-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs 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