Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare™ TLP:WHITE Alert ID : b61cc63f Aug 16, 2023, 01:04 PM

This week, *Hacking Healthcare*™ welcomes a guest essay on the what to make of the new Securities and Exchange Commission (SEC) final rule related to cybersecurity risk management, strategy, governance and incident disclosure.

A Paradigm Shift Towards Governing and Managing Cyber Risk - The Securities and Exchange Commission (SEC) Cybersecurity Risk Governance Rules – by Christopher Hetner

On July 26, 2023, the Securities and Exchange Commission (SEC) adopted new rules on cybersecurity risk management, strategy, governance and incident disclosure for publicly traded companies. The final rules differ somewhat from the rules proposed and include changes to account for feedback during the comment period. These rules require publicly traded companies to describe aspects of cyber incidents, including the nature, scope, and timing of the incident, as well as its material impact or reasonably likely impact on the company. Additionally, the rules require registrants (publicly traded entities) to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats and to describe the boardroom's oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cyber threats.

Incident Reporting

The SEC requires registrants to disclose cybersecurity incidents they believe to be material on a form 8-K filed within four business days of determining whether the incident itself is material or will result in material changes for investors. This rule will require the registrant to disclose "the material aspects of the nature, scope, and timing of the incident, as well as the material impact or likely material impact of the incident on the registrant, including its financial condition and results on operations."
The trigger for establishing the four-day timer for disclosure is the determination that the incident is material, not the discovery of the incident itself. Moreover, material impacts caused by third-party service providers must be represented in the incident disclosure requirements.

The SEC also adopted an exception for reporting when the disclosure of the incident would harm national security. The Attorney General is the approval authority for this exception.

Cybersecurity Risk Management

The rule requires registrants to describe only information useful for an investor, containing a description of the "the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes." The SEC expects a level of detail sufficient to allow investors to evaluate the cybersecurity posture and practices within the organization.

The SEC also adopted a provision in the final rules to describe whether the registrant "engages assessors, consultants, auditors, or other third parties in connection with their cybersecurity." The SEC stated this is to understand the "registrant's level of in-house versus outsourced cybersecurity capacity." The rule does not require naming the third parties or detailing the services they provide.

The final 106(c)(2) rule directs registrants to ***consider*** disclosing information about which of the company's management positions are responsible for managing and assessing cybersecurity risk, their qualifications, whether and how those individuals report to the board, and other potentially relevant data.

Board Oversight

The final rule, as adopted, requires registrants to "describe the board's oversight of risks from cybersecurity threats," and, if applicable, "identify any board committee or subcommittee responsible" for such oversight "and describe the processes by which the board or such committee is informed about such risks." While this is still reasonably detailed, compliance will be significantly less cumbersome than with the proposed rule. Best practice suggests that cybersecurity oversight should be nested into a risk committee that contains complementary risk domains such as supply chain, privacy and geopolitical perils.

A Shift from Cyber to Business Risk

The current cybersecurity ecosystem (people, process, technology) is largely focused on addressing technical level threats used to mitigate risk. While the cybersecurity ecosystem continues to evolve, it still lacks the ability to contextualize cyber threats and incidents to business, operational and financial exposures. The "material" determination is influenced by the incident's impact on the company's business, operations and financial condition.

The types of business and financial factors should be contemplated when determining incident materiality. These costs and adverse consequences as a result of a cybersecurity incident may 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.

Summary of the Disclosure Requirements

Item	**Summary Description of the Disclosure Requirements**
Regulation S-K Item 106(b) – *Risk management and strategy*	Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
Regulation S-K Item 106(c) – *Governance*	Registrants must: - Describe the board's oversight of risks from cybersecurity threats. - Describe management's role in assessing and managing material risks from cybersecurity threats.
Form 8-K Item 1.05 – *Material Cybersecurity Incidents*	Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its: - Nature, scope, and timing; and - Impact or reasonably likely impact. An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General ("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public safety. Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.
Form 20-F	FPIs must: - Describe the board's oversight of risks from cybersecurity threats. - Describe management's role in assessing and managing material risks from cybersecurity threats.

Form 6-K	FPIs must furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders.

About the Author: Chris Hetner is a 30-year cybersecurity veteran who has held roles ranging from Chief Information Security Officer at GE Capital to Senior Cybersecurity Advisor to the Chair of the United States Securities and Exchange Commission. He's currently serving as the Cyber Risk Advisor to the National Association of Corporate Directors and Chairs the Nasdaq Insights Council for Cybersecurity.

Congress

Tuesday, August 15
No relevant hearings

Wednesday, August 16
No relevant meetings

Thursday, August 17
No relevant meetings

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

Report Source(s)
Health-ISAC

Tags

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:

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