SEC Cybersecurity Rule Presents Burden For Health Care Cos.

By **Bess Hinson and Angad Chopra** (August 14, 2023)

Bess Hinson

Angad Chopra

On July 26, the U.S. Securities and Exchange Commission **announced the adoption**[1] of a broad range of new regulations addressing cybersecurity risk management, strategy, governance and incident disclosure applicable to public companies generally.

These newly adopted rules[2] present a set of potentially burdensome obligations on such companies, as well as uncertainty and potentially conflicting regulatory requirements.

Importantly, the SEC's rules adoption announcement noted that the final rules will become effective 30 days following the publication of the adopting release in the Federal Register. New requirements regarding Form 10-K disclosures, described in more detail below, will become due beginning with annual reports for fiscal years ending on or after Dec. 15.

New Form 8-K disclosures will be due 90 days after the date of publication in the Federal Register or Dec. 18. Smaller companies are provided an additional 180 days before they must begin providing the Form 8-K disclosure.

The Adopted Rules and Accompanying Rationale

Included in the newly adopted rules released by the commission are strict disclosure requirements specific to a publicly traded company's cybersecurity posture.

The rules, for example, would require companies to periodically include updated disclosures in Forms 10-K and 10-Q related to risk oversight policies and procedures.[3] The rules would also require reporting pertaining to a registrant's policies and procedures used to identify and manage cybersecurity risks, as well as governance disclosures set out in more detail below.

The commission also included an incredibly expeditious and onerous four-day cybersecurity incident reporting period to be provided in publicly disclosed Form 8-K after a material cybersecurity incident.[4]

Further, if a company discloses an incident on Form 8-K, changes to Regulation S-K will now require such companies to disclose any material changes, additions or updates on the company's quarterly report on Form 10-Q or annual report on Form 10-K.

These disclosures must include information on "any material effects the prior incident had on the company's operations and financial condition, any potential material future impacts on the company's operations and financial condition, whether the company has remediated or is currently remediating the incident, and any changes in the company's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes."[5]

The commission is clearly indicating an increased emphasis on prescriptive policy requirements, directing regulated companies to focus on written policies and procedures that protect customer records and to assess and memorialize the effectiveness of such policies and procedures.

In addition to robust notification and disclosure requirements, the newly adopted rules also introduce a host of nuanced governance requirements.

For example, the adopted rules would require disclosure regarding the role of the board of directors and management in cybersecurity governance.[6]

Specifically, a company would need to disclose "whether it has designated a chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the company's organizational chart, the relevant expertise of any such persons, the processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection and remediation of cybersecurity incidents, and whether and how frequently such persons and committees report to the board or a committee of the board on cybersecurity risk."

The commission noted that these disclosures of how a company assesses and implements policies, procedures and strategies to mitigate cybersecurity risks would be of importance to investors both as they understand how registrants are planning for cybersecurity risks and as they make decisions as to how to best allocate their capital.

These rules indicate an obvious expectation from the commission that cybersecurity experts become mainstays on public corporate boards.

The commission's aggressive approach toward cybersecurity regulation seems to be a reaction to large-scale incidents like the recent cyberattacks at SolarWinds Corp.[7] and Colonial Pipeline Co.[8]

Such attacks not only drastically affected stock prices and company values, but serve as case examples of how cyberattacks can disrupt key economic functions in society and daily activities. These newly adopted rules would greatly increase the commission's involvement in the management of regulated companies' approach to cybersecurity and system integrity.

The commission seems poised to take on the challenge as it recently doubled[9] the size of its Enforcement Division pertaining to cyber and crypto-assets. Enforcement activity also seems to be on the rise as significant fines have already been levied against publicly traded entities for failing to appropriately protect the records and information of customers.

The newly adopted rules may only be the opening salvo of SEC regulatory activity, as since the adopted rules' proposal, the commission has introduced even more proposed regulations, for example, some targeted[10] at specific industry sectors, including brokers, dealers, investment companies and investment advisers.

The Potential Effect of the Commission's Newly Adopted Rules

Although the commission's chief aim seems to be to increase cybersecurity resiliency and promote a robust cybersecurity posture among some of the nation's largest companies, the result may actually stray far from the desired outcome as entities will now face a far more complicated regulatory environment with increased strategic and litigation risks.

For example, the expeditious four-day cybersecurity incident disclosure obligation requires an incident disclosure after the company conducts a materiality analysis.

The newly adopted rules advise that companies need to "objectively evaluate the mix of the information, taking into consideration all relevant circumstances surrounding the incident," noting that materiality "depends on the significance the reasonable investor would place on" the information.[11]

Short of an event resulting in complete business interruption, companies are likely to struggle to apply the materiality test in an expedited fashion, given that specific details concerning the cybersecurity incident, its precise scope, the type of data accessed or stolen, and the effect on company operations is an analysis that evolves over days and sometimes weeks following the initial discovery of the intrusion.

Moreover, companies often require assistance from specialized technology and review teams in order to confirm whether compromised data in fact contains corporate confidential information, intellectual property or personal information. These reviews sometimes result in monthslong mining of affected data.

By requiring this disclosure a mere four days after the determination of a material cybersecurity incident, the Form 8-K filing could precede data breach notifications provided to state attorneys general, and other regulatory agencies such as the U.S. Department of Health and Human Services, for publicly traded entities also regulated by the Health Insurance Portability and Accountability Act.

Currently, state data breach notification laws require notice under varying timelines, most of which allow for reasonable delay provided that the affected company needs time to act upon measures necessary to determine the scope of the breach and restore the integrity of the information systems, while some statutes require notice to affected individuals within a 30- or 45-day time window.[12]

Moreover, issuing a notice on which investors may rely, but which reflects an evolving set of facts, may result in unnecessary volatility in the markets, particularly if the company is able to restore affected systems and operations more quickly than anticipated or suggested in the initial notice to the SEC.

Affected companies' customers may further frustrate the investigatory process upon learning of an event early in time, by issuing inquiries to the company's information technology and information security professionals, thus distracting internal efforts to completely investigate the extent of the security intrusion in a timely manner.

Further disclosures on Forms 10-K and 10-Q regarding past security incidents, now to be reported on Form 8-K, and updates regarding the same also pose litigation risk. These reports will provide plaintiffs attorneys and regulators with further information that can be scrutinized and molded to create legal claims or justify further investigation into how the company handled the investigation and remediation of prior incidents.

Other disclosures required by the commission's newly adopted rules can provide potential threat actors with a treasure trove of information on some of the nation's largest companies, potentially leading to the disastrous outcome of inadvertently providing nefarious actors with an easy-to-access hit list based on cybersecurity-related disclosures made to the commission as a result of newly adopted regulation.

The Impact on Publicly Traded Health Care Organizations

According to the American Hospital Association, there are 6,093 hospitals in the U.S., of which 1,228 are investor-owned — for-profit — acute care hospitals and 2,960 of which are nongovernment not-for-profit acute care hospitals.[13]

These statistics clearly show that a large number of hospitals and health care companies may need to comply with the recently adopted regulations.

Publicly traded health care companies regularly handling protected health information would potentially have to comply with a trio of regulatory standards emanating from state data breach laws, HIPAA and new SEC regulations.

As such, health care companies may be under the microscope given the regulatory complexity with which they now must comply. HIPAA requires notice no more than 60 calendar days after a material cybersecurity incident, while the recently adopted rules require notification within four days.

Providing preliminary and premature information about an incident prior to the completion of a forensic investigation is likely to expose companies to litigation before the company has full insight into the incident's impact, as well as potentially undermining attorney-client work product.

As such, health-related information is incredibly sensitive, and premature disclosures of a cybersecurity incident present inherent risks, plausibly never before contemplated by entities in the industry.

Hospitals and health care companies handling protected health information rely on a host of third-party providers, which can independently be susceptible to intrusions or cyberattacks to operate their business.

An example includes remote patient-monitoring technology partners, which use connected devices with Internet of Things sensors to offer providers a continuous stream of real-time health data such as heart rate, blood pressure and glucose monitoring.

Other examples include artificial intelligence, diagnostic and advanced imaging devices, as well as implantable medical devices, robotic surgery devices, electronic health records companies and cloud providers.

These third-party providers make health care companies a prime target for threat actors given the sensitivity of the information at issue. As such, it will be increasingly important, especially with heightened regulatory scrutiny, for health care companies to augment and create more stringent contracting requirements with those third-party providers in order to meet the reporting deadlines and prepare proper disclosures now required by new regulation.

Potentially helpfully, the U.S. Food and Drug Administration has published cybersecurity guidance[14] for medical devices and providers as well, which companies can look to in order to boost overall cybersecurity resiliency.

New Liability Linked to Cybersecurity Governance

The newly adopted rules present even further challenges with the increased emphasis on

governance changes including entrenching cybersecurity experts on boards of directors.

For the past decade, there has been a severe shortage[15] of qualified cybersecurity professionals that can step into CISO roles or become a part of boards of directors. Moreover, recent regulatory and even criminal scrutiny has been placed on CISOs, making the position an unattractive option for qualified candidates.

The commission has also been involved in providing Wells notices regarding individual CISOs, such as recommending legal action against the SolarWinds CISO in the aftermath of the 2020 cyberattack for failure to disclose material information.[16]

CISOs will increasingly be held accountable for their decisions. Identifying specific individuals or committees as being responsible for cybersecurity postures at some of the largest companies can present risks for boards of directors, which now need to thoroughly scrutinize personnel to ensure the appropriate level of expertise that the commission seems to seek.

The commission did not expressly note a definition of what qualifications would be beneficial for board members to have given what the commission described as the wide-ranging nature of cybersecurity skills but did include a nonexclusive list of criteria to consider, such as prior work experience; any knowledge, skill or background in cybersecurity; and cybersecurity-specific certifications.[17]

The newly adopted rules also include required disclosures regarding board oversight of cybersecurity risk.

Specifically, the required disclosures include: whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks; the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and whether and how the board or board committees consider cybersecurity risks as part of its business strategy, risk management and financial oversight.[18]

The commission believes that such disclosures will help inform investment and voting decisions but would also present the onerous challenge of introducing cybersecurity expertise as mainstays on boards of directors with proper qualifications.

Preparing for Heightened Scrutiny

Given the adoption of these rules and the inevitability of further proposed regulations, companies should take immediate action to address the new obligations.

As a preliminary step, companies should identify the breach notification regulations applicable to their business given the complex regulatory environment.

Next, companies should analyze and confirm an appropriate budget to ensure compliance with multiple regulations and to boost overall cybersecurity hygiene.

Further, companies should review existing information security preparedness plans and recent cybersecurity assessments to identify potential risks and fill any gaps.

Now would be an ideal time to review applicable cyberliability insurance policies to ensure adequate coverage in the event of an incident and third-party claims. In addition,

companies should rehearse and pressure test key policies and procedures related to incident response and reporting requirements.

Moreover, boards should act quickly to install cybersecurity experts at high levels but ensure proper vetting to reduce overall risk exposure. Companies should designate specific stakeholders throughout the company who will, in turn, communicate among teams new reporting deadlines so that notifications can be provided in a timely manner.

As the commission takes an aggressive approach to cybersecurity resiliency and overall preparedness, companies should be aware that a more complex regulatory environment is on the horizon and prepare while the commission gears up for enforcement.

Bess Hinson is a partner and Angad Chopra is an associate at Holland & Knight LLP.

[1] SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (July 26, 2023) [hereinafter, SEC Rules Adoption Announcement].

[2] Adopted Rules (July 26, 2023) [hereinafter, Adopted Rule].

[3] See Adopted Rule at p. 53.

[4] See Adopted Rule at p. 120.

[5] See Adopted Rule at p.46.

[6] See Section D Adopted Rule at p. 81.

[7] SEC Release Following SolarWinds Attack.

[8] SEC Release Following Colonial Pipeline Attack.

[9] SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit (May 3, 2022).

[10] SEC Proposed Regulation pertaining to broker-dealers, investment companies, and investment advisers.

[11] See Adopted Rule at p. 14.

[12] See e.g. Cal. Civ. Code § 1798.82; see also C.R.S.A. § 6-1-716 (Colorado data breach statute noting a 30-day notification requirement); Ariz. Rev. Stat. § 18-552 (Arizona data breach statute noting a 45-day notification requirement).

[13] Fast Facts on U.S. Hospitals 2023.

[14] U.S. FDA Cybersecurity Guidance.

[15] Attracting and Retaining Top Cybersecurity Talent Amid Worker Burnout and Shortages (December 30, 2022).

[16] SEC notice to SolarWinds CISO and CFO roils cybersecurity industry (June 27, 2023).

[17] See Section D Adopted Rule at p. 81.

[18] Adopted Rule at p. 65.