BY EMAIL PDF DELIVERY

May 9, 2022

Chair Gary Gensler
Commissioner Hester M. Peirce
Commissioner Allison Herren Lee
Commissioner Caroline A. Crenshaw
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20459--1090 Email: rule--comments@sec.gov

Re: Comment on Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number S7-09-22)

Dear Chair and Commissioners:

We the undersigned, writing in our individual capacities as seasoned practitioners who bring deep private and public sector experience in strengthening both corporate governance incentives and processes, and the proactive mitigation and remediation of businesses' exposure to information risks attendant to cyber intrusions, urge the U.S. Securities and Exchange Commission ("Commission") to adopt a comprehensive rule pertaining to the way in which public companies' executives and boards of directors should (i) ensure there is *robust, integrated* cybersecurity oversight by the management *and* the board; (ii) *systemically* identify and mitigate firms' *short- and long-run* cybersecurity risks; (iii) design and execute a *dynamic* cybersecurity strategy that provides for *contemporaneous* assessments of risk management should breaches occur; and (iv) *rapidly disclose* incidents and articulate the *lessons learned*.

To this end, the Commission is to be commended for its proposed rule—File Number S7-09-22—published on March 9, 2022. It holds great promise for significant reform of public companies' oversight and management of cyber risks—both in C-suites and boardrooms. However, we believe the proposed rules can be strengthened. In our Comment, we focus on several points that we urge the Commission to consider in its finalization of the rule prior to its adoption.

1. Introduction

We offer our observations in light of our professional experience, which is summarized as follows:

Dr. Harry G. Broadman

Current Positions
- Managing Director, Berkeley Research Group LLC
- Faculty Member, Johns Hopkins University
- Board Leadership Fellow, National Association of Corporate Directors
- Member, Council on Foreign Relations
- Member, Bretton Woods Committee

Previous Positions
- Former Senior Managing Director and Chief Economist, PricewaterhouseCoopers (PwC)

- Former World Bank Senior Official working China; Russia and the CIS; East and South Asia; and Africa.
- Former Chief of Staff, President's Council of Economic Advisers.
- Former U.S. Assistant Trade Representative.
- Former Senior Professional Staff Member, U.S. Senate Homeland Security and Governmental Affairs Committee.

Eric Matrejek

Current Positions

- Managing Director, Berkeley Research Group LLC
- Board Member, CARPLS (Coordinated Advice & Referral Program for Legal Services).

Previous Positions

- Former Partner, Global Computer Forensics & eDiscovery Leader PricewaterhouseCoopers (PwC)
- Former Managing Director, FTI Consulting, Inc.
- Former Operations Director, Monarch Group
- Former Manager of Business Development, Saber Consulting
- Former Solution Architect and Sales Executive, Oracle Corporation
- Former Principal Management Analyst, The Port Authority of New York & New Jersey.

Brad Wilson

Current Positions

- Director, Berkeley Research Group LLC
- Member, High Technology Crime Investigation Association
- Member, US Secret Service Chicago Electronic Crimes Task Force

Previous Positions

- Former Director, Cybersecurity, Privacy and Forensics, PricewaterhouseCoopers (PwC)
- Former Manager, Senior Associate, Associate, Forensic Services, PricewaterhouseCoopers (PwC).

2. Backdrop: Induced Changes in Business Disclosure Responses to Cybersecurity Attacks Are Improving the Governance Environment

The rapidly changing threat landscape, ranging from corporates being compelled by ransomware to release intellectual property (IP) to having to shut down infrastructure, has made it increasingly difficult for companies to manage cyber risks. As a result, whereas past victims tended to keep attacks secret, they're now being encouraged, and even required, to disclose more information with the insurers that are protecting them from liability.

Industry-wide, more than 80% of cyber insurers reported a rise in cyber claims in the fourth quarter of 2021, many related to ransomware attacks, forcing premiums up by 34%. That was the 17th straight quarter in which insurance rates rose.

The changes in disclosure behavior are assisting both the companies and their insurers to not only better predict and calculate the cost of cyber-attacks, but it is also inducing insurance providers to sell cyber insurance more as a service than as a transaction. That is a metaphor for the transformation of corporate behavior towards cybersecurity risks in a fundamentally changed environment.

Moreover, rather than simply completing insurance forms detailing their cyber practices and then paying their premia, corporates are working with insurers to regularly monitor activity on their network and collecting and analyzing file logs. Insurance providers are assessing organizations' cybersecurity performance, providing metrics and benchmarking them against peers. This process is demonstrating to businesses the value of transparency.

At the same time, as cyber breach incidents have become so broad and frequent, some insurers have pulled out of the cyber insurance sector completely. This, of course, increases pressure on companies to properly manage their risk exposure and spend more on acquiring talented people and embracing cutting-edge enterprise technologies.

3. Boards of Directors and Executive Teams Have Shared Responsibilities in Cybersecurity Governance, But Greater Delineation is Needed for the Roles and Qualifications of Each

The Commission's proposed rules require the disclosure by companies of the way in which their cybersecurity governance is overseen by management teams and boards. However, the specificity of the criteria to be met in both cases is lacking.

a) Management

The proposed rules would require firms to (1) specify management's roles and responsibilities for overseeing cybersecurity; (2) delineate the process by which management is informed about breaches and how they monitor their prevention, mitigation, detection; and (3) indicate how frequently management is to update the board on cybersecurity risks, threat events and breaches.

These are all laudable stipulations. While it is understandable that there will be variation across firms of different sizes, sectors, etc. in their definition, the Commission would do well to establish the criteria by which firms must go about this process. The Commission should also give consideration to suggesting a "model" template for firms to follow in going through this process. Even more importantly, the final rule should require companies to specify the *qualifications* of executives overseeing cybersecurity within the firm.

b) Boards

Many corporate boards have made significant progress understanding the importance of how cybersecurity affects the competitive health, operational resilience, investment appeal, customer loyalty, and reputation of the companies they oversee. They've certainly gotten the message that enhancing cybersecurity is not just an "IT issue" but lies at the *core* of businesses' state-of-the-art corporate governance practices. It is surely a crucial part of the "G" in ESG.

There are several instances in the last two years relating to the landmark "Caremark" case that established the key role and performance criteria of corporate director responsibilities and liabilities when it comes to the exercise of risk oversight. Establishing a robust boardroom approach to effective cybersecurity risk oversight necessitates specifying board member competencies, board structure and the boards' approach to understanding such risk, including systemic risk.

But most board directors have yet to move far enough along to become as effectively equipped as they should be to intelligently gauge the extent to which their firms' executive teams are at the top of their games in the war on corporate cyber-attacks.[1]

Few directors—even those who serve on board Risk Committees—engage C-suite executives in rigorous dialogue on the specific *strategies* they're undertaking to reduce vulnerabilities to hacks and why particular approaches *rather than others* are being employed.

Indeed, boards who effectively devolve *full* oversight of cybersecurity to their Risk Committees are myopic. While boards' Risk Committees should *take the lead,* becoming adept at understanding cyber risks and how to mitigate them are truly *cross-cutting* since mistakes can threaten the lifeblood of the company, its workers, its reputation, and its long-run growth. *Where boards' assessments of the impact of cyber risks on business operations most assuredly should not take place is the Audit Committee.* After all, audits are backward-looking. Cyber threats are largely contemporaneous and forward-looking dangers to the enterprise.

Boards not only need to be better educated about cyber threats but also able to engage in a robust dialogue with the executive team about such risks, including how to evaluate the performance of the relevant managers who are responsible for their mitigation.

Regrettably, however, many board members are intimidated to ask the executives who are most centrally responsible for cybersecurity—traditionally Chief Information Officers (CIOs), but increasingly Chief Information Security Officers (CISOs)—all but the most general technical questions. Even then, the issues that board directors raise with the executive team are almost always focus on the magnitude of the *problem* and the degree to which the CIOs/CISOs believe they have *existing* threats contained. It is rare that discussions in the boardroom delve deeply into the *solutions* the executives have either already instituted or are contemplating doing so.

Some, perhaps many, board members become well-versed to ask their firms' Chief Financial Officers (CFOs) technical questions about financial reporting and related details. Yet when it comes to cyber, the conversations are thin. Of course, the Sarbanes-Oxley Act mandated public (and some private) companies to disclose to the Commission which of their directors are "qualified financial experts." To this end, the Commission's proposed rule for ensuring boards have directors who are knowledgeable about cybersecurity is a good start. But more should be stipulated by the Commission.

For example, the proposed rules would require disclosure of (1) which board members are responsible for the oversight of cybersecurity risks; (2) the frequency and process by which the board is informed about cybersecurity risks; and (3) whether and how the board considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

However, the Commission should require companies to focus on *specifying the qualifications* of the directors overseeing cybersecurity on the board. In particular, similar to the SEC's approach for mandatory disclosure of "qualified financial experts", boards should be required to designate "qualified cyber experts" to ensure the given set of qualifications are met.[2]

---

[1] See *Forbes*: "Corporate Boards' Oversight Of Cyber Risks Is Too Passive" (November 2018), available at: https://www.forbes.com/sites/harrybroadman/2018/11/28/corporate-boards-oversight-of-cyber-risks-is-too-passive/?sh=7f129e401f81

[2] See *Forbes*: "Boards Can Surmount The Cybersecurity 'Intimidation Factor': 10 Questions Directors Should Discuss With C-Suites" (December 2021), available at: https://www.forbes.com/sites/harrybroadman/2021/12/31/boards-can-surmount-the-cybersecurity-intimidation-factor-10-questions-directors-should-discuss-with-c-suites/?sh=552554d79508

4. Disclosures of Material Cybersecurity Incidents

The Commission's proposed rules would require a company to file a Form 8-K within four (4) business days of a *material* cybersecurity incident. This is a good step forward.

However, the proposed rules do not specify how to determine *materiality* of a cybersecurity incident. Instead, they suggest an evaluation based on the total mix of information, as is the case with other materiality determinations under federal securities laws. Determining the "materiality" of cyber breaches is different than other incidents due to (a) the potential for broader financial and reputational impacts, (b) scope of the breach is difficult to ascertain, and (c) assessment of the impact can change between the short- and long-term phases of the investigation, especially for incidents that were ongoing for months or years.

Companies are responding to internal and external cybersecurity incidents on a daily, and in some industries, hourly basis. There needs to be a discrete set of evaluation criteria to assess incidents' materiality. Without such criteria, the ambiguity and complexity of the evaluation could lead to over- or under-reporting of "material" incidents. The result could well be that the disclosure requirement would be ineffective.

With proper evaluation criteria to determine a material incident, public companies could more effectively, and consistently, assess these diverse set of incidents and engender a reliable disclosure process.

5. Disclosures Regarding Cybersecurity Risk Management and Strategy

The proposed Commission rules would amend Regulation S-K in which companies would have to disclose information regarding their cybersecurity *risk management* strategies. This would include providing a description of the company's policies and procedures for identifying and managing risks from cybersecurity threats.

In addition, the proposed rules would require companies to describe their cybersecurity *risk assessment* program, including whether the company engages third parties to make such assessments and whether the company's financial condition is reasonably likely to be affected by cybersecurity risks and incidents of varying character and magnitude.

The Commission, or an independent group, such as the newly formed CSC 2.0 Non-profit[3], should consider establishing benchmarks as to the quality and coverage of a given firm's level of cybersecurity—perhaps analogous to the Financial Strength Ratings.

6. Holistic Approach to Cyber Risk Management

The proposed Commission rules should require companies to formulate a holistic 360° approach to addressing cyber risks—one that is inclusive of business processes, the technologies utilized, and the people in charge.

Threat actors are no longer just exploiting technical weakness in companies' cyber defenses, they are actively attacking companies' business process and applications as well as the people responsible for managing them. For example, threat actors have compromised companies' sub-contractors in order to gather confidential information and operating details. These data have been used to create a sophisticated business pretext, combined with technical access, to cause companies' staff to by-pass protocols and wire millions of dollars to numerous off-share accounts. Consequently, cybersecurity insurers and bond underwriters are requesting companies to detail their cyber threat resilience strategies so they can be assessed. Companies may then be required to address deficiencies found.

[3] Website available at: https://www.cybersolarium.org/

The Commission should require companies on a regular basis to both disclose their cyber readiness metrics and marshal evidence as to how they are complying with them. To this end, the Commission should consider issuing a template as to best practices for devising such metrics and assessing their compliance.

Conclusion

We appreciate the Commission's invitation to comment on the proposed rule. Thank you for your time and consideration.

Sincerely,

Dr. Harry G. Broadman
[redacted]

Eric Matrejek
[redacted]

Brad Wilson
[redacted]