Business Roundtable

1000 Maine Avenue, SW, STE 500
Washington, DC 20024
[redacted]
brt.org

May 9, 2022

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
Release No. 34-94382; File No. S7-09-22

Dear Ms. Countryman:

This letter is submitted on behalf of Business Roundtable, an organization whose members lead America's largest companies, employing over 20 million workers. Their companies' total value, over $20 trillion, accounts for half of the value of all publicly traded companies in the United States. They spend and invest over $7 trillion a year, helping sustain and grow tens of thousands of communities and millions of medium- and small-sized businesses.

We appreciate the opportunity to comment on the proposed rules issued by the Securities and Exchange Commission (the "Commission" or "SEC") on March 9, 2022, to require expansive new disclosures by registrants with regard to cybersecurity matters (the "Proposals").[1] These comments address certain areas of particular concern with regard to the Proposals, but necessarily cannot address all aspects of the Proposals in light of the limited time for comment.

INTRODUCTION AND SUMMARY

While Business Roundtable appreciates the SEC's desire to enhance disclosures around cybersecurity risk management, strategy, and governance, as well as the transparency around material cybersecurity incidents, we believe certain aspects of the Proposals raise significant concerns that must be addressed in the final rules adopted by the SEC. Chief among these concerns is the formulation of the proposed reporting requirement and, in particular, its incomplete consideration of the harm that can come from premature disclosure of incidents, including potential exacerbation of the impact of the attack on the target registrant, and the conflict that will arise in many cases between the proposed trigger and disclosure timing requirement on the one hand, and registrant security, national security and law enforcement considerations on the other.[2]

---

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release No. 34-94382 (Mar. 9, 2022), https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[2] For example, the SEC should harmonize its requirements with the already-complex regulatory landscape, including the reporting requirements set out in the Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 117th Cong. (2022).

THE SEC'S PROPOSALS

Overview

The Proposals would (i) amend Form 8-K to require current disclosure of material cybersecurity incidents; (ii) add new Item 106 of Regulation S-K requiring a registrant to: (1) provide updated disclosure in periodic reports about previously reported cybersecurity incidents and require disclosure about certain immaterial incidents that later become material in the aggregate, (2) describe policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity risks as part of its business strategy, financial planning, and capital allocation, and (3) require disclosure about the board's oversight of cybersecurity risk, management's role in assessing and managing such risk, management's cybersecurity expertise, and management's role in implementing the registrant's cybersecurity policies, procedures, and strategies; and (iii) amend Item 407 of Regulation S-K to require disclosure of whether any member of the registrant's board has expertise in cybersecurity, and if so, the nature of such expertise.

Discussion and Recommendations

(i) ***Form 8-K Reporting***

Trigger and Timing for Disclosure of Material Cybersecurity Incidents

The SEC has proposed to amend Form 8-K to add new Item 1.05, which would require a registrant to disclose information about a cybersecurity incident within four business days after determining that it has experienced a "material" cybersecurity incident. In proposing such a requirement, the Commission notes that such reporting would "significantly improve the timeliness of cybersecurity incident disclosures, as well as provide investors with more standardized and comparable disclosures."

While Business Roundtable appreciates the importance of timely and comparable disclosures, investors only benefit when there is decision-useful information that can be provided. Following the initial discovery of a cyber incident, there is often a dearth of confirmed information and resources are best deployed to identify and mitigate the harm from a cybersecurity incident versus managing external communications concerning the incident. Much of what is believed to be the case in the initial days, or even weeks, following an incident will not ultimately be complete and/or accurate and thus will not provide investors with decision-useful information. Rather, premature public disclosure will often cause investors more harm than good because investors will be forced to make decisions based on incomplete and potentially inaccurate information and without full context for other aspects of the registrant's operations, including critical response and remediation efforts. The Commission has acknowledged this concern, noting in the Proposals that a registrant's disclosure about an

incident could "lack the precision needed for investors and the market to properly value the securities, potentially leading to information uncertainty, investor under or overreaction to certain disclosures, and thereby mispricing of registrants' securities." Disclosure before determining the nature and magnitude of information accessed (even when enough is known to reasonably expect the incident is material) will also lead to questions the registrant is incapable of answering, leading to additional risks and reputational harm. The confusion and uninformed market speculation resulting from such disclosure will force the registrant to deal with harmful volatility in its stock while trying to manage through the cyber incident.

Not only would premature disclosure be harmful to investors, it could exacerbate the respective registrant and/or stakeholder harms stemming from the original attack. Forcing public companies to engage in disclosure about incidents while in the midst of incident response and remediation could have significant unintended consequences. For example, in the case of a ransomware attack, such disclosures could adversely impact a registrant's ransomware negotiation position and strategy. In addition, disclosure of the information that would be required under the Proposals could increase the risk of additional or more aggressive attacks and worsen the overall impact of the incident being reported. In the case of the latter, the proposed new Form 8-K trigger (a determination of materiality) will in many cases occur before remediation, which could lead the threat actor to increase their efforts to exploit the existing vulnerability before it can be remediated or invite new threat actors to exploit the vulnerability. Disclosing an incident too early also could jeopardize an investigation by "tipping-off" the threat actor, allowing them time to destroy indicators of the compromise and/or evidence of data accessed or taken. Furthermore, when the incident relates to a widely-used third-party system, requiring individual registrants that use that system to make disclosure acknowledging they are affected will increase the likelihood that a threat actor will seek to exploit the vulnerability. Absent this disclosure, potential threat actors (whether the original hacker or a different hacker) may not know who the third-party's customers are, nor fully understand the extent to which their attack has impacted the systems under attack. Thus, the proposed disclosures could multiply the risks for the involved parties, including by causing actual harm to the affected public company and thereby its shareholders and other stakeholders such as customers and employees. Compounding these problems, the Proposals unnecessarily increase the risk of frivolous litigation from plaintiffs' lawyers regarding the timing of, and manner by which, a public company determines it experienced a "material cybersecurity incident" given the four-day reporting requirement.

For all of these reasons, Business Roundtable urges the SEC to reevaluate the proposed trigger, scope and timing for current reporting of cybersecurity incidents. Balancing these concerns and conflicting purposes is a complicated task and flexibility for the registrants is needed to address these risks. We maintain that disclosure of this sensitive information presents considerable risks and stands in contrast with security best practices. Accordingly, Business Roundtable urges that the SEC adopt a disclosure standard that better takes into account these concerns. For example, an alternative to the approach proposed could be to require Form 8-K reporting of

material cybersecurity incidents only once the registrant, pursuant to an obligation under applicable law, publicly notifies persons outside the registrant or when a registrant voluntarily elects to make disclosure. At a minimum, the SEC should allow for reporting to occur after the registrant has had a reasonable opportunity to respond to and resolve the incident.

Law Enforcement/National Security/Registrant Security/Public Safety Carveout

Further, we believe it is imperative that the reporting requirement include a law enforcement, national security, and other defensive measures exception that applies when the registrant (i) reasonably believes a particular disclosure may prejudice its efforts to defend itself against threat actors or remediate the incident or (ii) has been informed by governmental or regulatory authorities that delay of disclosure at that time would be in the interest of national security and/or that disclosure at that time would hinder law enforcement efforts to identify or capture the threat actor. In this regard, we note that the SEC acknowledges in the proposing release that "a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents," but concludes that "the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay." We do not believe the Proposals reflect the appropriate balancing of these important interests or that a registrant should be placed in the untenable position of harming its ability to defend/protect itself, impeding law enforcement efforts and/or imperiling national security as a result of an inflexible reporting requirement that results in premature (and thus potentially harmful to investor interests) disclosure. Failure to include a law enforcement exception could directly harm the investors that the disclosure requirement is presumably intended to protect. It is not difficult to imagine a situation where premature disclosure of an incident could impact the ability of law enforcement to seize the ill-gotten gains of a criminal actor, which could have been used to compensate victims, including the public company required to make the disclosure. Similarly, a "public safety" carveout should be considered for safety critical industries. A premature disclosure of an automobile, airplane, or medical device vulnerability could cause individuals to make safety-related decisions based on incomplete information – deferring medical procedures or travel, or disconnecting certain types of devices. We believe our suggested alternative approach would better balance the significant law enforcement and national security considerations without harming investor protection and take into account the significant investor harm that can result from premature disclosure of a cybersecurity incident.

Definition of "Information Systems"

The Proposals broadly define "information systems" as information resources, owned or used by the registrant, organized for the collection, processing, maintenance, use, of the registrant's information to maintain or support the registrant's operations.

As used in the Proposals, this broad definition potentially sweeps in a wide range of incidents, likely including those involving cloud infrastructure and service providers where registrants may have limited information because the registrant is not empowered to conduct an investigation. As many third-party information system arrangements are not set up today to allow for the information flow that is needed to comply with the proposed cyber incident Form 8-K reporting, Business Roundtable believes the scope of the disclosure requirements must be narrowed to capture only those information resources within the registrant's direct control (or third-party information resources beyond the registrant's direct control should otherwise be excepted from the new disclosure requirements). In addition, a phase-in period would be necessary to give registrants and vendors time to assess and develop systems to comply with these new disclosure obligations and the SEC should provide more clarity around which party in these situations has the disclosure obligation (once a material cybersecurity incident has been identified and assuming no national security or other exceptions apply, as discussed above).

(ii) ***Disclosure of Cybersecurity Incidents That Have Become Material in the Aggregate***

The Proposals would require a company to disclose "when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate," with registrants required to "analyze related cybersecurity incidents for materiality, both individually and in the aggregate." Business Roundtable views this aspect of the Proposals as unworkable and of questionable overall value. The requirement provides no temporal limits and would necessitate challenging and potentially imprecise judgments regarding whether incidents are "related," which would be a complex undertaking in the context of the myriad of cybersecurity incidents experienced by companies every day. This requirement also could put companies at a unique disadvantage with respect to potential attackers, letting those attackers know what attempts were successful, or providing ideas for future targets. It also would impose significant costs on registrants to track immaterial incidents to determine whether an after-the-fact examination of the incidents might lead to a conclusion that the incidents were somehow related.

(iii) ***Disclosure of Cybersecurity Risk Management and Strategy***

The Proposals would require new disclosures in Form 10-K of a company's policies and procedures for identifying and managing cybersecurity risk, the board's oversight of risk and management's role in assessing and managing risk. Much of the proposed annual disclosure on cybersecurity risk management and strategy has the potential to expose sensitive, confidential

information about a registrant's cybersecurity program, such as the scope and frequency of testing or assessment, the nature of its third-party engagements or systems, its operating environment, specific mitigation and remediation activities, and more. Such disclosures could be exploited by bad actors. Such disclosures also would subject registrants to second-guessing of their procedures and disclosure regarding such procedures by plaintiffs' firms, regulators and others when, as is virtually inevitable at this point, a cybersecurity incident does occur. For these reasons, Business Roundtable urges that the rules make clear that broad summary descriptions of policies and programs should suffice and reiterate that information that would provide a roadmap to bad actors looking for vulnerabilities to exploit need not be disclosed under the new requirements. Further, with regard to board oversight aspects of the Proposals, such disclosure is generally more appropriately provided in proxy materials than in the Form 10-K. Accordingly, we urge that registrants be given the flexibility to provide such disclosure in their proxy materials, similar to the cyber expertise disclosure.

(iv) ***Support for Proposed Safe Harbor and Approach to Form S-3 Eligibility***

As is proposed, and as is the case with other Form 8-K items that require a registrant to assess the materiality of an event or to determine whether a disclosure obligation has been triggered, any required disclosure regarding a cybersecurity incident should have the benefit of the safe harbors from liability and should not impact a company's ability to use short-form registration statements on Form S-3. Accordingly, Business Roundtable supports the Proposal's approach to liability and Form S-3 liability.

(v) ***Disclosures Should Be Furnished Versus Filed***

Finally, given the complex, dynamic and often lengthy nature of cybersecurity incident investigations, the new Item 1.05 of Form 8-K should be considered "furnished" rather than "filed" and should not be automatically subject to liability for material misstatements or omissions in SEC filings under Section 18 of the Exchange Act or automatically incorporated by reference in registration statements under the Securities Act (unless the company specifically elects it to be considered "filed" or incorporates it by reference into an SEC filing as permitted by current Form 8-K rules). Allowing the Form 8-K to be "furnished" would be more appropriate given that the information surrounding a cybersecurity incident is likely to evolve over the course of the related investigation.

(vi) ***Cybersecurity Expertise***

The Proposals would amend Item 407 of Regulation S-K to add a requirement to provide disclosure about the cybersecurity expertise of members of the board of directors of the registrant. While the Proposals do not define "cybersecurity expertise," the SEC has provided a non-exclusive list of criteria that a registrant should consider in reaching a determination on whether a director has expertise in cybersecurity:

- Whether the director has prior work experience in cybersecurity (e.g., prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner).
- Whether the director has obtained a certification or degree in cybersecurity.
- Whether the director has knowledge, skills, or other background in cybersecurity (e.g., in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning).

We agree that disclosure about the skills, background and expertise of board members is important information for our investors, along with disclosure of oversight regarding risk management. In fact, many of our member companies already provide disclosure regarding the cybersecurity expertise of board members and how boards oversee, and company leadership manages, cybersecurity risk. That said, we caution against an ever-expanding set of disclosure requirements regarding specific skills without regard to the materiality of that particular skill to the registrant. Further, we do not believe that the proposed disclosure requirements regarding cybersecurity expertise are necessary at this time. The proposed rules would require a registrant not only to disclose whether any directors have expertise in cybersecurity, but also to "provide such detail as necessary to fully describe the nature of the expertise."

If the Commission determines that this proposed disclosure requirement is necessary and appropriate, we urge the Commission to revise the proposed non-exclusive list of criteria for determining cyber expertise because the list of criteria is unduly narrow. While we understand that the list is non-exclusive, as the Commission knows, such lists often "become the rule" and registrants that are working to comply with a new disclosure requirement will look to that list as indicative of what the SEC expects. Accordingly, Business Roundtable believes the list should be expanded, including to (i) acknowledge the value of previous experience managing cybersecurity functions and leading organizations through data security incidents (similar to the SEC acknowledgement that a CEO is an "Audit Committee Financial Expert" whether or not the person is an accountant because they have had oversight of the accounting function at their company); and to (ii) to recognize adjacent skills, such as in technology. More broadly, the proposed list fails to recognize the oversight function exercised by boards as compared to the management of cybersecurity incidents or programs required at the executive and working levels. Companies do not need directors who are experts at forensic data analysis or similar technical aspects of incident response. Instead, companies benefit from directors who have significant leadership and risk management experience and have demonstrated a capacity to learn new skills and expertise. Otherwise, the SEC risks driving companies to create boards filled with "specialty directors" who have deep but narrow knowledge and struggle to fulfill the broad oversight and related duties required today.

CONCLUSION

Business Roundtable appreciates the opportunity to provide our input during this process. We would be happy to discuss these comments or any other matters you believe would be helpful. Please contact Maria Ghazal, Senior Vice President & Counsel of Business Roundtable, at [redacted] or [redacted].