PAUL HASTINGS

Stay Current

May 2023

Follow @Paul_Hastings

The Board Is Set: Preparing for the SEC's Upcoming Cybersecurity Rules

By Brad Bondi, John Michels & Jeremy Berkowitz

It has been a full year since the initial comment period closed on the Securities and Exchange Commission's ("SEC") proposed rule on cybersecurity disclosure, governance, and risk management for public companies (the "Proposed Rule for Public Companies," or "PRPC"). Although the SEC recently re-opened the comment period on some of its other cybersecurity proposals, it has not done so for the PRPC,[1] and according to its published rulemaking agenda, the PRPC was scheduled for final action last month.

In short, all indications are that the PRPC will be finalized soon, and public company boards of directors should be prepared for the additional burdens the PRPC will impose on boards.

Once finalized, the PRPC, officially titled *Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, will apply broadly to public companies,[2] and will expand significantly the existing cybersecurity disclosure requirements while also imposing a number of new requirements. Notably, these requirements impose a number of disclosure obligations on the boards of directors of public companies, including with respect to the cybersecurity expertise of Board members.

Below, we highlight the key requirements of the PRPC, and provide advice on what boards should be doing to prepare.

What Does the PRPC Require?

The SEC has stated that the intention of the PRPC is to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting."[3] As we discussed in a prior post, the PRPC does this by imposing a number of requirements, including the following:

- ***Four-day disclosure timeframe for "material" cybersecurity incidents.*** The PRPC proposes adding a new Item 1.05 to Form 8-K that requires companies to disclose any "material" cybersecurity incident within four days of discovery. Companies are required to disclose specific information including when the incident was discovered, whether the incident is ongoing, the scope and nature of the incident, and whether any data was compromised. The PRPC also makes clear that the SEC intends to apply the typical securities-law definition of "materiality" in this context—*i.e.*, information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."

- ***Aggregation requirement for incidents that are non-material individually.*** The PRPC includes a new requirement under Regulation S-K that requires companies to disclose circumstances in which prior cybersecurity incidents that, while not material individually, become material in aggregate. Such incidents need to be disclosed in the company's next periodic report following the company's determination that the combined incidents have become material. Any look-back approach to materiality will prove to be challenging to navigate.

- ***Disclosures on Board cybersecurity expertise.*** The PRPC requires disclosures regarding Board oversight of company cybersecurity risk management policies, and the implementation of such policies. These disclosures would include, among other things, the name of any directors that have cybersecurity expertise and "such detail as necessary to fully describe the nature of" their expertise. In the PRPC, the SEC acknowledges that it intentionally is leaving this requirement open-ended by not defining the term "cybersecurity expertise" because a range of experience, skills, and tasks may qualify as expertise. However, the PRPC provides a helpful list of criteria that companies should consider as expertise including the director's prior work experience, relevant certifications or degrees, or other background or skills pertaining to cybersecurity, such as security policy and governance, risk management, security engineering, or business continuity planning.

- ***Disclosures on risk management, oversight, and cybersecurity policies.*** The PRPC requires companies to periodically disclose a description of the company's risk assessment program, whether the company engages third parties in connection with its risk management processes, and the extent to which the company has policies in place to evaluate cybersecurity risks associated with the use of third party service providers. In addition, as part of this disclosure, companies will need to describe whether specific management positions are responsible for quantifying cybersecurity risk at the company, and describe the expertise of those individuals.

What Should Boards Do To Prepare?

Although the PRPC's requirements must be evaluated in the context of your specific organization, Boards generally should prepare for the PRPC in the following ways:

1. ***Integrate cybersecurity into the company's overall business strategy***. One of the fundamental messages of the PRPC is that the SEC expects Boards of Directors to take a holistic approach to organizational cybersecurity efforts. Boards should review, and where necessary, augment the ways in which cybersecurity is integrated into company business strategies and decision-making processes (e.g., risk management evaluations, product development, marketing and sales strategies, supply-chain management, information technology practices, and human resources.) In addition, given the focus of some of the PRPC's disclosure requirements, Boards should consider whether and to what extent their organizations are leveraging third-party vendors to validate cybersecurity safeguards, such as through penetration and vulnerability testing.

2. ***Develop appropriate cybersecurity expertise at all levels***. A number of the PRPC's disclosure requirements relate to the cybersecurity expertise of directors and officers. Boards can ensure that cybersecurity expertise is adequately reflected across all organizational levels by (a) designating a qualified individual in senior management to be responsible for

implementing and overseeing the company's cybersecurity program; (b) ensuring adequate staffing and training of cybersecurity personnel; (c) providing appropriate training for the company's workforce; and (d) as the PRPC makes clear, ensuring that the Board itself includes individuals that have demonstrable cybersecurity expertise, based on education, work experience or other relevant background, or certifications or degrees.

3. ***Build and reinforce clearly defined escalation processes***. Boards should ensure that there are processes and procedures in place that allow appropriate cybersecurity matters to be escalated to senior management and Boards both (a) periodically, and (b) in the case of a critical development such as a material cybersecurity incident, on an *ad hoc* basis. Even where such processes and procedures exist in documentation, Boards also should confirm that the escalation thresholds are both known and followed by appropriate personnel. These guidelines will aid in complying with the PRPC's four-day reporting requirements in the case of material cybersecurity events, and are also a useful feature of company cybersecurity risk assessment and management processes more generally.

4. ***Develop and update incident response and notification guidelines***. Boards should ensure that their companies have considered the PRPC's requirements pertaining to the disclosure of data security incidents. In particular, the PRPC's four-day disclosure requirement for "material" cybersecurity incidents should be described in the company's incident response plan to avoid inadvertent noncompliance in the event of such an incident. Additionally, Boards should work with management to articulate pre-determined materiality guidelines that can be referenced against cybersecurity events, and should work with legal counsel to develop a process to assess whether multiple, non-material cybersecurity events eventually cross the materiality threshold in the aggregate. That assessment inevitably will require the involvement of a securities lawyer, who can help shield the board from potential liability from both the SEC and private litigation.

5. ***Consult with experienced legal counsel throughout the process***. Boards should bear in mind that fully understanding and implementing PRPC requirements likely will be challenging in practice, and that they may intersect, interact with, or augment other regulatory regimes in some cases. Given the complexities of the PRPC and the four-day reporting requirement, Boards should consult with experienced legal counsel on how to meet PRPC obligations and assess materiality when an incident occurs.

The PRPC is one of a number of recent SEC proposed rules in the cybersecurity space, all of which underscore the agency's increasing focus on cybersecurity issues. We expect the SEC's focus on cybersecurity will continue following the implementation of the PRPC and that the SEC's Division of Enforcement will be vigilant in investigating violation of these rules.

Paul Hastings' Data Privacy and Cybersecurity practice regularly advises companies on compliance with cybersecurity requirements at the federal, state, and international levels. If you have any questions concerning how to better prepare for the PRPC or other cybersecurity requirements, please do not hesitate to contact a member of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

John J. Michels
1.312.499.6017
johnmichels@paulhastings.com

Washington, D.C.

Brad Bondi
1.202.551.1701
bradbondi@paulhastings.com

Jeremy Berkowitz
1.202.551.1230
jeremyberkowitz@paulhastings.com

[1] Although the initial comment period closed on May 9, 2022, the SEC temporarily re-opened the comment period between October 7, 2022 and November 1, 2022 due to a technical issue with the SEC's website.

[2] Specifically, the PRPC will apply to all public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.

[3] 87 FR 16590, 16590.