PAUL
HASTINGS

SEC Proposed Cybersecurity Rules – What They are and What Our Clients Should be Doing Now

What are the New Rules?

Earlier this year, the Securities and Exchange Commission (SEC) published a new set of proposed cybersecurity disclosure rules for public companies. The proposed rules would significantly increase SEC scrutiny of public companies' cybersecurity-related business activities, decision-making processes and the Board's new role in overseeing cybersecurity.

These proposed rules signal the increasing importance the SEC places on cybersecurity, going farther than any federal agency to date in placing obligations on public companies and their Boards of Directors. One of the most significant new obligations requires public company Board oversight and involvement in the review, assessment, and implementation of cybersecurity policies and procedures. The proposed rules also create stronger and more uniform guidelines for companies regarding disclosures, and ongoing supplementation, of "material" cybersecurity incidents.

The comment period for these rules originally ended on May 9, 2022, with hundreds of comments submitted. However, the SEC recently reopened the comment period for an additional 14 days due to a technical error that may have caused issues with public comments submitted through the SEC's website.

While we do not yet have a date for when the rules will be finalized or effective, the Office of Management Budget indicated that final action will be taken in April 2023. Given the significant changes that are likely to be included in the new rules, companies and their boards should take steps to prepare now.

What are Some of the Key Requirements if the Rules are Adopted?

- If the SEC adopts the rules similar to their proposed form, the key obligations include:
- Report "material cybersecurity incidents" to the SEC within 4 days;
- Report non-material incidents that, when combined with other incidents, become material "in the aggregate";
- Provide updates on prior incidents in periodic SEC disclosures;
- Provide a description of the company's cybersecurity risk management system;
- Describe the Board's oversight of cybersecurity risk; and
- Disclose the cybersecurity expertise of the Board members.

What is Changing from the Current Rules?

- ***Companies and their senior leadership will be held to a higher standard.*** Under the new rules, companies will be required to develop and maintain reasonable cybersecurity practices, describe those practices in public filings, explain how their senior leadership oversee those programs effectively, and report cybersecurity incidents in a way that provides appropriate information to shareholders.
- ***The rules will be clearer (hopefully).*** While more granular and potentially burdensome than in the past, the new rules will provide clarity on and solidify earlier guidance and the outcomes of recent SEC enforcements. Current rules, guidance, and enforcements have created an inconsistent and potentially confusing standard for cybersecurity that will be remedied, at least in part, by these new rules.
- ***More, and more detailed, documentation will be required.*** Among the recent findings in various SEC enforcements is the clear message from the Commission that it believes that cybersecurity incident reports often lack detail, are inconsistent, and are not timely. The new rules provide guidelines for the content, timing, and format of incident reports and periodic disclosures. The new rules also require adequate documentation of companies' cybersecurity and risk management programs.

What Should Companies be Doing to Prepare?

- ***Review cybersecurity and risk management documents.*** Cybersecurity and risk management systems can take months to update. Companies should start reviewing and updating these programs now. Companies should pay particular attention to changes in their technology infrastructure, recent acquisitions and mergers, changes in the threat landscape, and lessons learned from any recent security incidents.
- ***Educate your Board.*** With all of the new requirements for oversight being placed on the Board, the Board will need to ensure that it is prepared to oversee the cybersecurity and risk management policies and procedures of the company. However, few Boards have historically been provided with enough detail to take on this task. Determine whether the full Board, or a subset of the Board, will be primarily responsible for oversight, ensure that they have been properly educated and approve of the company's policies and procedures.
- ***Review your incident response plans.*** All companies should have an incident response plan, but we recommend a review of such plan in light of these new proposed rules. Your incident response team should be aware of this timeline and know whether and how to escalate as needed. The incident response plan should also have a clear escalation plan for raising significant or material incidents with senior leadership and the Board. The window for reporting a material incident to the SEC is 4 days – that is a shorter notification period than any other US law. Like the other cybersecurity policies and procedures, the Board should be educated on the incident response plan and then participate in a table top exercise to simulate a real incident.
- ***Identify what materiality means to your company.*** Any decision on the materiality of an incident, which would require notification within 4 days, should be made by the company's legal team and the senior leadership as appropriate. The Company should specifically ensure that both the incident response plan and operating environment have the appropriate procedures for escalation to the legal team and senior management who will make the materiality determinations.

Our Data Privacy and Cybersecurity practice regularly advises companies on how to meet the requirements of new laws. If you have any questions concerning these new laws and regulations starting in early 2023 or any other data privacy or cybersecurity laws, please do not hesitate to contact any member of our team.

Paul Hastings Data Privacy and Cybersecurity Team

Paul Hastings Privacy and Cybersecurity Solutions Group