Updates
February 23, 2018
SEC on Cybersecurity: Jay Clayton's "Light Touch"

This week, the U.S. Securities and Exchange Commission (SEC) issued its first formal interpretative release on public company disclosure obligations relating to cybersecurity since the SEC Division of Corporation Finance's guidance in 2011. The new guidance is close in tone to the 2011 guidance but emphasizes, in SEC Chair Jay Clayton's words, the "importance of maintaining comprehensive policies and procedures related to cybersecurity incidents and risks," as they pertain to disclosure controls and procedures, insider trading and selective disclosures.

The new guidance also makes clear the SEC's expectation that boards' risk management oversight duties include engagement on cybersecurity issues, to the extent material to the company's business. The new guidance reflects a theme of Chair Clayton's term, to take a light touch on new disclosure mandates and to reiterate that companies should disclose *material* risks and events.

Background: 2011 Guidance. While cybersecurity risks have been a concern for listed companies for over 20 years, the SEC has issued guidance on cybersecurity disclosure only once before, in 2011. In the 2011 guidance, the Division of Corporation Finance declined to suggest new line-item disclosure for cybersecurity risks and incidents, instead stating that existing regulations already provided for timely and sufficient disclosure of material cybersecurity attacks, risks and events. The Division pointed to five areas in which disclosure in periodic reports on Forms 10-K and 10-Q may call for cybersecurity disclosure, including Risk Factors, Description of Business, Legal Proceedings, Management's Discussion and Analysis (MD&A) and Financial Statements. The 2011 guidance stressed that cybersecurity disclosure should be disclosed "to the extent material." Since 2011, SEC staff has generally reiterated that the guidance from 2011 has continued to be the touchstone for cybersecurity disclosure in the current environment, such as in an October 2017 speech regarding retail investor protection and cybersecurity by Stephanie Avakian, the SEC Enforcement Division's co-director of enforcement.

Continued Emphasis on "Materiality" as the Disclosure Trigger. The new guidance follows the 2011 guidance's emphasis on "materiality" as the guiding principle for cybersecurity disclosure. The release, for example, describes the standard of materiality articulated by the U.S. Supreme Court in *TSC Industries v. Northway*, as well as the balance of probability and magnitude in *Basic v. Levinson*. Chair Clayton has emphasized materiality before, including in his July 2017 speech to The Economic Club of New York, in which he expressed concern that disclosures "beyond the core concept of materiality" were linked to a significant decline in the number of U.S.-listed public companies.

Areas of Focus in the 2018 Guidance

Disclosure Controls and Procedures. Far short of adopting a formal rule, the SEC's new guidance "encourages companies to adopt comprehensive policies and procedures related to cybersecurity," and to regularly ensure that such measures provide appropriate processing and reporting of cybersecurity incidents and risks within the company.

The guidance proposes companies consider the following key features when designing and evaluating the effectiveness of, or certifying on the design and effectiveness of, disclosure controls and procedures.

- Enable the passage of both disclosable and potentially disclosable cybersecurity information ("up the corporate ladder") to decision makers and certification personnel;
- Allow for open communication channels between technical experts and disclosure advisors;

- Allow for timely public disclosure, if required;
- Ensure that all disclosable information is appropriately preserved and processed;
- Account for the adequacy of the controls and procedures for identifying cybersecurity incidents and risks, as well as the impacts of both; and
- Prevent insiders from trading on material nonpublic cybersecurity information, detailed below.

Insider Trading. The new guidance reminds company leadership that trading securities while in possession of material nonpublic information of a company's cybersecurity risks and incidents (including vulnerabilities and breaches) may be considered unlawful insider trading. It also advises them to consider whether their companies' codes of ethics and insider trading policies specifically take into account and prevent trading on the basis of such information. The SEC suggests that in the course of investigating any cybersecurity incidents, the company should consider when knowledge of the incident rises to the level of implementing a trading blackout for applicable insiders, to both prevent and "avoid the appearance of" insider trading.

Regulation FD and Selective Disclosure. The new guidance provides a reminder that, prior to disclosing material nonpublic cybersecurity risk and incident information, companies and their agents may not selectively disclose such information to Regulation FD-enumerated persons, which include broker-dealers, investment advisors, investment companies and security holders for which it is reasonably foreseeable that such holder will trade the company's securities based on such information. The SEC emphasizes that a company's policies and procedures should prevent such selective disclosure, or else make any Regulation FD-required public disclosure in a timely and compliant manner.

Duty to Promptly Disclose, Even With an Ongoing Investigation. A common theme in the new guidance is the emphasis on promptness of disclosure of cybersecurity risks and incidents. Companies are encouraged to use Item 8.01 on Form 8-K to promptly disclose material information, noting that this is not only an obligation imposed by NYSE and Nasdaq (which require listed companies to "release quickly" and to "make prompt disclosure of" material information, respectively), but also that prompt disclosure maintains the accuracy and completeness of other filings and reduces the risks of selective disclosure and insider trading. While acknowledging that an investigation by law enforcement could affect the scope of disclosure of an incident, the guidance makes clear that the existence of an ongoing internal or external investigation, *alone*, would not serve as a basis to avoid disclosure of a material cybersecurity incident. What is not clear is the impact this portion of the guidance will have on requests by law enforcement to delay notification for specific cyber incident-related reasons.

Duty to Update or Correct. The new guidance reminds companies that they have a duty to correct prior disclosure that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made, or a duty to update disclosure that becomes materially inaccurate after it was made, such as if material facts that were not available at the time of initial disclosure are later uncovered during the process of an investigation.

Board Oversight of Cybersecurity Risk. A popular topic during the March 2014 SEC Cybersecurity Roundtable was the increasing involvement by boards in understanding deeply all aspects of a company's cybersecurity, with one participant stating that boards are "thinking about cyber and enterprise risk management really as being one and the same." It is no surprise, then, that the SEC appears to be sending a strong message to boards that their responsibilities include involvement in cybersecurity risk management. Specifically, the new guidance describes the need for proxy statement disclosure regarding the board of directors' role in the company's cyber risk management program when cybersecurity risk is material to the company's business. While materiality will depend on the company, many businesses that have access to sensitive consumer data already include discussions along these lines in their board risk oversight disclosures.

Practical Tips: What to Do Next

Based on the highlights of the new guidance described above, we offer the following practical tips to public companies:

1. **It's "materiality" that matters.** Only material cybersecurity risks and incidents need be disclosed. Where materiality is unclear, consider involving outside legal counsel in determining the best approach to disclosure decisions and potential insider trading policy blackout periods. Disclose *material* cybersecurity risks and incidents as promptly as possible, recognizing that: (1) "promptly" may be a relative term given the facts and circumstances necessary to determine the materiality of cybersecurity risks and incidents; and (2) the full scope of such incidents and the impact on business operations may not be known until well after the incident is discovered. Update prior disclosures upon discovery of new material information relating to the incident.
2. **Regularly refresh your cybersecurity-related policies and procedures.** It is critical for companies to maintain comprehensive, agile and regularly revisited cybersecurity policies and procedures. Examine your company's disclosure controls and procedures to determine whether existing processes appropriately flag cybersecurity risks and incidents for consideration of materiality and other disclosure obligations, and address any vulnerabilities.
3. **Post-cyber incident trading by insiders raises eyebrows.** Review your company's code of ethics and insider trading policies and consider affirmatively adding cybersecurity risks and incidents as examples of potential material nonpublic information. Consider establishing policies and procedures that trigger a trading blackout period when insiders are aware of material or possibly material nonpublic cybersecurity information to avoid even an appearance of impropriety.
4. **Take steps to prevent selective disclosure of cybersecurity information.** Ensure that employees and third parties involved in investigations and assessments of cybersecurity risks and incidents are aware of your company's policies and procedures regarding selective disclosure of material nonpublic information. Make any public disclosures regarding cybersecurity risks and incidents, including those that may be required by consumer protection statutes, in a Regulation FD-compliant manner.
5. **Disclose board oversight over cybersecurity risk management.** Ensure your board is appropriately engaged in the oversight of cybersecurity risks and incidents, and, if material to the company's business, include specific discussion regarding that engagement in proxy statements.
6. **Keep cybersecurity on the disclosure committee's agenda.** While the new guidance does not mandate disclosures beyond the materiality considerations addressed in 2011, internal disclosure committees should review the new guidance and keep cybersecurity in mind as a key issue for the committee. Any cyber incident, even if seemingly immaterial, should be a topic for discussion with disclosure committees and counsel.

Related Resources

To further your understanding of these issues, we offer these additional resources:

- A helpful recent discussion of a board's cybersecurity oversight duties: "Is That a Target on your Back?: Board Cybersecurity Oversight Duty after the Target Settlement".
- A refresh on Chair Clayton's speech to The Economic Club of New York in July 2017 is covered in Lou Mejia's article, "Jay Clayton's Enforcement Philosophy" in *Law360*.

This update was republished in *Bloomberg BNA's White Collar Crime Report* on 03.16.2018, "New SEC Cybersecurity Guidance Reflects Clayton's 'Light Touch'," and *Bloomberg's Big Law Business* on 03.13.2018, "SEC on Cybersecurity: Jay Clayton's "Light Touch."

Authors

Explore more in

Corporate Governance | Public Companies | Securities Litigation | White Collar & Investigations | Privacy & Security | Corporate Law

Related insights

Update

Two Tools for Trump To Dismantle Biden-Era Rules: the Regulatory Freeze and the Congressional Review Act

Update

The FY 2025 National Defense Authorization Act: What's New for Defense Contractors