MORRISON
FOERSTER

SEC Publishes New Guidance on Cybersecurity Disclosures and Compliance Practices

Marty Dunn, Miriam H. Wugmeister, Scott Lesmes, John P. Carlin, and David A. Newman

02/22/2018

Global Risk + Crisis Management, Privacy + Data Security, REITs, and Public Companies Counseling + Compliance

Client Alert

In an unusual step that appears to indicate renewed, if not intensified, scrutiny of public companies' cybersecurity practices by the Securities and Exchange Commission (SEC), the SEC's five commissioners unanimously issued guidance (the "Guidance") on February 21, 2018 covering a range of cybersecurity topics including disclosure obligations, board oversight and risk management controls. The SEC staff had issued guidance regarding cybersecurity disclosure in October 2011. While the Commission issued the Guidance unanimously, it is important to note that two of the commissioners have released public statements expressing reserved support for the Guidance, but noting that it in large part recapitulates information already presented in 2011 by the SEC's Division of Corporation Finance.

Public companies should closely review the Guidance for the additional details it provides regarding key disclosure obligations:

- Disclosures regarding cybersecurity threats and practices should be integrated throughout a company's periodic reports, including the Risk Factors, Management's Discussion & Analysis, Description of Business, Legal Proceedings, and Financial Statements Disclosures sections. "Companies should avoid generic cybersecurity-related disclosures and provide specific information that is useful to investors." [1] The Guidance also advised public companies to consider their disclosure regarding Board oversight of the management risks relating to cybersecurity matters.
- While companies are not required to make specific technical disclosures that would compromise their security efforts and while the SEC recognizes that additional details may come to light in the course of ongoing security investigations, companies should make every effort to provide timely disclosures with the information at their disposal so that the public can make informed investment decisions.

The Guidance also touches upon two areas not previously discussed by the SEC:

- Companies are encouraged to adopt, implement and regularly update comprehensive cybersecurity risk management policies. Importantly, these policies should specify disclosure controls and procedures that ensure that relevant information regarding cybersecurity threats and developments are channeled to the right personnel, both for purposes of assessing risk and determining disclosures obligations. There should, in particular, be a free flow of information up the corporate ladder to senior management.
- Information about cybersecurity risks and practices may be material nonpublic information and, therefore, companies should be mindful of applicable insider trading laws when drafting codes of conduct, designing trading black-out periods and otherwise implementing executive trading policies.

In July 2017, SEC Chairman Jay Clayton gave a speech at the Economic Club of New York that many interpreted as signaling a more cooperative enforcement posture by the SEC ("Being a victim of a cyber penetration is not, in itself,

an excuse. But, I think we need to be cautious about punishing responsible companies who nevertheless are victims of sophisticated cyber penetrations" [2]).

Takeaways

The extent to which this newly published Guidance will have a direct impact on enforcement is still not clear, but companies are advised to:

- make cybersecurity training and compliance a priority company-wide;
- review their existing periodic filing disclosures for completeness and timeliness;
- confirm that existing policies and practices include appropriate and timely notification to senior leaders; and
- update their insider trading policies as necessary to expressly contemplate cybersecurity risks as potentially material nonpublic information.

---

[1] https://www.sec.gov/rules/interp/2018/33-10459.pdf

[2] https://www.sec.gov/news/speech/remarks-economic-club-new-york