CLIENT ALERTS & INSIGHTS

SEC Issues Guidance on Public Company Cybersecurity Disclosures

FEBRUARY 22, 2018

On February 21, 2018, the Securities and Exchange Commission (the "Commission") released guidance on public company disclosure requirements regarding cybersecurity risk and incidents. This is the first time the Commission has issued a release on this topic since 2011.

In 2011, the Commission's Division of Corporation Finance issued guidance (which can be found in full here) providing that, while public company disclosure requirements do not explicitly reference the disclosure of cybersecurity risk and cyber incidents, companies may be obligated to make disclosures on such matters.

In its recent release, the Commission acknowledged the increase in both cybersecurity risks and incidents. In light of the increase in such risks and incidents - and the attendant costs companies face in addressing them - the Commission was prompted to provide further guidance on its views on cybersecurity disclosure requirements.

The Commission's recent guidance acts to expand on the guidance provided in 2011 and addresses two items not developed in its prior guidance:

- Maintaining comprehensive policies and procedures relating to cybersecurity risks and incidents: The Commission highlighted that companies are required to maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including material events related to cybersecurity. Such controls and procedures should, among other things, ensure that a company is timely collecting and evaluating information concerning cybersecurity incidents and risks that may need to be disclosed.
- Reminder of insider trading prohibitions and selective disclosures: The Commission also used its recent guidance to remind companies and their corporate insiders (e.g., directors, officers and others with inside information on the company) that they are prohibited from trading on inside information, or making selective disclosures (in violation of Regulation FD), regarding a material, non-public cybersecurity incident or risk.

In addition, the recent guidance discussed the various ways in which a company may be obligated to disclose applicable cybersecurity risks and/or incidents (for example, identifying cybersecurity risks in the risk factors included in annual reports on Form 10-K, disclosure of cybersecurity occurrences and consequences in current reports on Form 8-K, discussion of the costs of cybersecurity efforts and/or incidents in MD&A sections, and/or disclosure of the board's oversight of the management of cybersecurity risk in proxy statements).

In connection with the release of the guidance, on February 21, 2018, SEC Chairman Jay Clayton issued a statement and noted that he has asked the Division of Corporation Finance to continue to monitor cybersecurity disclosures as part of their selective filing reviews and, further, the Commission will continue to consider developments in this area and whether further Commission guidance or rules are needed.

The full 2018 guidance can be found here. If you have any questions regarding the Commission's guidance on cybersecurity disclosures, please contact Sarah Hesse at shesse@beneschlaw.com or another member of Benesch's Corporate & Securities Practice Group.