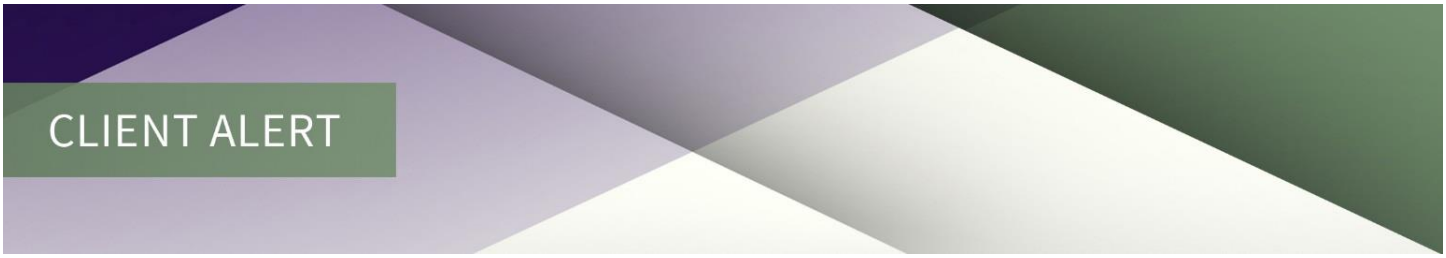

SEC Reinforces Cybersecurity Guidance

February 23, 2018

AUTHOR

Jeffrey S. Hochman

On February 21, 2018, the SEC issued interpretive guidance to assist public companies in their disclosure, oversight and other obligations relating to cybersecurity risks and incidents.[1] This release, in light of the increasing frequency and severity of cybersecurity incidents, and their potential for significant loss, reputational harm and ongoing damage to a company's business, seeks to reinforce and expand upon the SEC staff's previous 2011 cybersecurity guidance.[2] This new interpretive guidance also emphasizes the importance of disclosure controls and procedures and insider trading prohibitions in the cybersecurity context, two topics the SEC did not address in the staff's previous guidance.[3]

General Disclosure Obligations

The SEC notes a litany of substantial costs and other negative consequences to companies that fall victim to successful cyberattacks, including:

- remediation costs, such as liability for stolen assets or information, repairs of system damage and incentives given to customers or business partners in an effort to maintain relationships after an attack;
- increased cybersecurity protection costs, which may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees and engaging third party experts;

[1] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, available here.

[2] SEC Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity, available here.

[3] Due to their importance, cybersecurity issues are being addressed by many regulators in addition to the SEC, such as the CFTC, various state regulators, the U.K.'s Financial Conduct Authority and EU data protection authorities. See, for example, our previous Client Memorandum, *Companies Face a Maze of Cybersecurity Regulations and Heightened Risk Management*, available here.

- lost revenues resulting from the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- litigation and legal risks, including regulatory actions by governmental authorities;
- increased insurance premiums;
- reputational damage that adversely affects customer or investor confidence; and
- damage to the company's competitiveness, stock price and long-term shareholder value.

In light of the potentially severe consequences, the interpretive guidance reminds reporting companies to consider the materiality of these cybersecurity risks when preparing disclosure in registration statements and periodic and current reports.

- Periodic reports such as annual reports on Form 10-K and quarterly reports on Form 10-Q require timely information regarding material risks and incidents, including those involving cybersecurity, and disclosure of all material facts to make the statements therein not misleading. While careful not to impose a specific *current* reporting obligation, the SEC also encourages companies to use Form 8-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters. Companies should also consider whether they need to refresh previous disclosures, as they may have a duty to correct a prior disclosure that either was untrue at the time it was made or, if investors continue to rely on the information, becomes materially inaccurate after it was made.
- As with other disclosure, companies are expected to avoid "boilerplate" and instead provide information tailored to their particular cybersecurity risks and incidents.
- However, the guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts. The SEC does not expect disclosure of specific, technical information in such detail as would make the company more susceptible to a cybersecurity incident.
- The SEC recognizes that a company may require some time to discern the implications of a cybersecurity incident. However, an ongoing investigation would not on its own provide a basis for avoiding disclosure of a material cybersecurity incident.

Rules Requiring Disclosure of Cybersecurity Issues

To the extent material, there are several areas that likely require discussion of cybersecurity-related risks and incidents:

- *Risk Factors.* Item 503(c) of Regulation S-K requires companies to disclose the most significant factors that make investments in the company's securities speculative or risky. Companies should disclose the risks associated with cybersecurity efforts and incidents, tailored to their specific circumstances, and consider disclosure of previous cybersecurity incidents, including their severity and frequency.

- *Management's Discussion and Analysis (MD&A) of Financial Condition and Results of Operations.* Item 303 of Regulation S-K requires companies to discuss their financial condition and results of operations. The costs of ongoing cybersecurity efforts, the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents should be discussed to the extent material to their financial condition and/or results of operations.
- *Description of Business.* Item 101 of Regulation S-K requires companies to discuss their products, services, relationships with customers and suppliers and competitive conditions. If cybersecurity incidents or risks materially affect these factors, appropriate disclosure must be provided.
- *Legal Proceedings.* Item 103 of Regulation S-K requires disclosure of information relating to material pending legal proceedings, including proceedings that relate to cybersecurity issues.
- *Financial Statements.* Cybersecurity incidents and risks may impact a company's financial statements, including expenses related to any investigation, breach or remediation, loss of revenue, warranty or breach of contract claims and/or impairment of intellectual property or other assets.
- *Board Risk Oversight.* Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company. To the extent cybersecurity risks are material to a company's business, this discussion should include the nature of the board's role in overseeing management of that risk.

Policies and Procedures

The SEC emphasizes the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents, including appropriate disclosure controls and procedures that enable reporting companies to make accurate and timely disclosures of material events, including those related to cybersecurity.

- *Disclosure Controls and Procedures.* Cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as they relate to compliance with federal securities laws. Companies should assess whether they have sufficient disclosure controls and procedures in place to ensure timely collection and evaluation of information potentially subject to required disclosure or relevant to assessments of their business. The SEC notes that chief executive officers and chief financial officers, in making their certifications regarding the design and effectiveness of their companies' disclosure controls and procedures, should take into account the adequacy of controls and procedures relating to identifying cybersecurity risks and incidents and assessing their impact.
- *Insider Trading.* In light of the potential materiality of cybersecurity risks and incidents, as evidenced by the significant impact on the stock prices of various companies following disclosure of a major cybersecurity breach, companies should be mindful of complying with the laws related to insider trading in connection with information

about cybersecurity risks and incidents, including vulnerabilities and breaches. Companies' insider trading policies should, as appropriate, address and prohibit trading on the basis of material nonpublic information related to cybersecurity risks and incidents.

- *Regulation FD and Selective Disclosure.* Under Regulation FD, issuers must avoid selective disclosure of material nonpublic information. The SEC notes that, given their importance, cybersecurity matters may implicate Regulation FD concerns, and encourages prompt public disclosure of cybersecurity matters to avoid any potential issues.

Through this new interpretative guidance, issued under the imprimatur of the Commission itself rather than the previous staff guidance, the SEC has reinforced the increasing importance of cybersecurity issues, both in terms of companies' disclosure obligations and their oversight and compliance obligations. The SEC believes that cybersecurity risks pose grave threats to investors, our capital markets and our country, risks that continue to intensify each year. We expect this to be a continued focus of the SEC, both in terms of reviewing companies' disclosures for specific and tailored discussion of these risks and any cybersecurity incidents and the design and implementation of appropriate procedures and policies to address these risks, particularly following any significant breach.[4]

If you have any questions regarding this client alert, please contact the following attorney or the attorney with whom you regularly work.

Jeffrey S. Hochman
212 728 8592
jhochman@willkie.com

[4] Chairman Clayton noted that the SEC will continue to evaluate the need for further guidance or rules in this area. Though supporting the issuance of the guidance, Commissioners Stein and Jackson went further, expressing disappointment in the limited action currently being taken and suggesting additional measures that should be considered, ranging from more specific disclosure obligations and imposing a current reporting requirement on Form 8-K, to improvements in disclosures relating to oversight and policies and procedures, and even to establishing standards for broker-dealers and other market participants to protect the personal information of investors.