PUBLICATION

SEC Expands Cybersecurity Guidance: All Public Companies Must Take Note

Authors: Matthew George White
February 23, 2018

On February 21, the U.S. Securities and Exchange Commission (SEC) issued interpretive guidance (the "Guidance") to public companies updating and expanding on the SEC Staff's prior cybersecurity guidance that was released in 2011. The SEC's Guidance is intended to inform companies on how and when to disclose actual and potential cybersecurity-related risks, breaches, or incidents. Given the significant breaches over the last seven years, and with many more sure to come, public companies should be well aware of the Guidance.

The Guidance outlines the Commission's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies. In particular, the Guidance addresses two topics that were not discussed in the Staff's 2011 guidance, namely: (1) the importance of cybersecurity policies and procedures; and (2) the application of insider trading prohibitions in the cybersecurity context.

The Guidance stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents, and explains that companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity. The Guidance also reminds companies and their directors, officers and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents. While these obligations are not new, the restatement and reissuance should be noted by public companies that may not have been as diligent in their documentation.

Given the SEC's continued and enhanced focus on cybersecurity-related issues, it does not come as a surprise that it has issued additional guidance on these topics. However, many in the industry do not believe that the Guidance goes far enough. One thing is for certain, however: given the upcoming implementation of the European General Data Protection Regulation (GDPR), as well as several of the recent high-profile data breaches in the last year, financial institutions and publicly traded companies should expect a continued focus from the SEC on cybersecurity-related matters.

Summary of Guidance

While noting that no existing disclosure requirements explicitly refer to cybersecurity risks and cyber incidents, the Guidance outlines the Commission's views with respect to cybersecurity disclosure requirements as they apply to publicly operating companies. Here are several key aspects of the Guidance:

1. Companies should consider the various rules that may require the disclosure of cybersecurity issues. Potentially applicable rules include:

- Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosures that are required in registration statements under the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act"). While the applicable disclosure requirements do not specifically refer to cybersecurity risks and incidents, the Guidance explains that

the Commission views a number of the requirements as imposing an obligation to disclose such risks. For example:

- **Periodic Reports**: Reporting of such events can be required when making disclosures through periodic reports such as Forms 10-K and 10-Q, wherein companies must provide timely and ongoing information regarding material cybersecurity risks and incidents that trigger disclosure obligations.

- **Securities and Exchange Act Obligations**: Securities Act and Exchange Act registration statements must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading. Companies should consider the adequacy of their cybersecurity-related disclosures, among other things, in the context of Sections 11, 12 and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act.

- **Current Reports**: The Commission encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters, such as the costs and other consequences of material cybersecurity incidents. The Commission believes this practice also reduces the risk of selective disclosure, as well as the risk that trading in their securities on the basis of material nonpublic information may occur.

The Guidance does not provide any definitive answers as to when a cybersecurity-related event is "material." The Commission notes that in determining a company's disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The Commission explains that the materiality of cybersecurity risks or incidents depends upon their nature, extent and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities. We recommend consulting with Data Protection, Privacy and Cybersecurity counsel in these decisions.

Ultimately, the Commission explains that when a company has become aware of a cybersecurity incident or risk that would be material to its investors, it would expect the company to make appropriate disclosure timely and sufficiently prior to the offer and sale of securities and to take steps to prevent directors and officers (and other corporate insiders) from trading its securities until investors have been appropriately informed about the incident or risk. However, the Commission will not require companies to make detailed disclosures that would compromise its cybersecurity efforts, such as the disclosure of specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks and devices more susceptible to a cybersecurity incident, i.e., the type of information that would give hackers a "roadmap" to penetrate the company's security protections.

- Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among the most significant factors that make investments in the company's securities speculative or risky, including risks that arise in connection with acquisitions. In particular, the Commission explains that companies should consider the following issues, among others, in evaluating any cybersecurity risk factor disclosure:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;
- the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third-party supplier and service provider risks;
- the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;
- the potential for reputational harm;
- existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and
- litigation, regulatory investigation and remediation costs associated with cybersecurity incidents.

With respect to these disclosures, the Commission notes that a company may need to disclose both previous and ongoing cybersecurity incidents, as well as other past events necessary in order to put these risks in appropriate context.

- The Guidance also explains that companies should consider the extent to which cybersecurity incidents, and the risks that result therefrom, may affect a company's financial statements, including any:
  - expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services;
  - loss of revenue, providing customers with incentives or a loss of customer relationship assets value;
  - claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties, and insurance premium increases; and
  - diminished future cash flows, impairment of intellectual, intangible or other assets; recognition of liabilities; or increased financing costs.

The Guidance notes several other circumstances in which a company needs to consider whether or not disclosures related to cybersecurity events need to be made, including:

- Item 303 of Regulation S-K and Item 5 of Form 20-F, which require a company to discuss its financial condition, changes in financial condition and results of operations. The Commission explains that in this context, the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, could inform a company's analysis. In addition, companies may consider the array of costs associated with cybersecurity issues, including, but not limited to, loss of

intellectual property, the immediate costs of the incident, as well as the costs associated with implementing preventative measures, maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation, and the loss of competitive advantage that may result.

- Item 407(h) of Regulation S-K and Item 7 of Schedule 14A, which require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure. The Commission explains that to the extent cybersecurity risks are material to a company's business, they believe this discussion should include the nature of the board's role in overseeing the management of that risk.

- Item 103 of Regulation S-K, which requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party. The Commission reminds companies to note that this requirement includes any such proceedings that relate to cybersecurity issues.

- Item 101 of Regulation S-K and Item 4.B of Form 20-F, which require companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions. The Commission notes that if cybersecurity incidents or risks materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company must provide appropriate disclosures.

2. Companies should ensure adequate cybersecurity risk management policies and procedures are in place. Companies should also adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. This assessment should include whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications. Senior management should also be enabled to facilitate policies and procedures designed to prohibit directors, officers and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents. The Guidance reminds companies that pursuant to Exchange Act Rules 13a-15 and 15d-15, companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness. These controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents.

3. Companies and their directors, officers and other corporate insiders 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. The Commission reminds companies of what should already be obvious, namely, that it is illegal to trade a security "on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information." *See* Rule 10b5-1(a) of the Exchange Act. The Guidance explains that information about a company's cybersecurity risks and incidents may be material nonpublic information, and directors, officers and other corporate insiders would violate the antifraud provisions if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.

4. Finally, the Commission reminds companies that they may also have disclosure obligations under Regulation FD in connection with cybersecurity matters. Namely, companies should not selectively disclose material nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons before disclosing that same information to the public.

The Commission warns that it will continue to monitor cybersecurity disclosures carefully.

One thing is for sure: the SEC's focus on cybersecurity-related matters is not going away. Companies need to ensure that they have sufficient policies and procedures in place to address cyber-related concerns, should consider whether any disclosure requirements necessitate disclosure of cyber-related issues, and must evaluate SEC risks when handling and responding to a cyber incident.

If you have any questions regarding these issues or any other cybersecurity or data privacy-related matters, please contact Matthew G. White or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.