New SEC guidance on public company cybersecurity disclosures

By Kelly Babson, Jason P. Gonzalez, Pierce Han, Carolyn Lowry

On February 21, 2018, the United States Securities and Exchange Commission (the “SEC”) released a Commission Statement and Guidance on Public Company Cybersecurity Disclosures (the “2018 Guidance”), providing new interpretive guidance addressing disclosures involving cybersecurity risks and incidents.1 The 2018 Guidance reinforces and expands upon guidance issued by the SEC staff in 2011 (the “2011 Guidance”) (previously covered by Nixon Peabody here2 and here3), and addresses several new topics, including cybersecurity policies and procedures and implications of cyber risks and incidents for policies and procedures relating to prohibitions against insider trading and selective disclosure.

Similar to the 2011 Guidance, the 2018 Guidance sets forth a principles-based framework for addressing cybersecurity-related disclosures and practices under existing legal and regulatory requirements, rather than proposing new rule-based disclosure or other regulatory requirements. Against this backdrop, twelve key takeaways for public companies from the 2018 Guidance are outlined below.

1. General considerations
Consider the materiality of cybersecurity risks and incidents when drafting and reviewing disclosures to be included in registration statements, periodic reports such as annual reports on Form 10-K and quarterly reports on Form 10-Q and current reports such as Form 8-K or Form 6-K filed with the SEC, and tailor the company’s disclosures appropriately based on specific facts and circumstances. In addition to applicable risk factor disclosures, discussion of cyber risks or incidents may also be appropriate in a company’s disclosures regarding business and operations, legal proceedings, management’s discussion and analysis of financial condition and results of operations (“MD&A”), financial statements and accompanying notes, disclosure controls and procedures and corporate governance. Further discussion of these areas is highlighted below.

3 “Trending cybersecurity disclosures,” January 19, 2017 (available here).
2. **Timeliness and specificity of disclosure**

Provide relevant and timely disclosures of cyber risks and incidents that are material to investors, including discussion of related financial, legal or reputational consequences specific to the company. Cyber-related disclosures should be written so that they are specific and communicate meaningful information that is useful to investors, without reliance on generic or “boilerplate” language. The 2018 Guidance makes clear, however, that such disclosures are not expected to be so technically detailed that they provide roadmaps for potential cyber criminals. Companies are specifically encouraged to use Form 8-K or Form 6-K, as applicable, to disclose material information promptly. In that regard, companies should also be mindful of applicable stock exchange requirements. The 2018 Guidance also includes a reminder that it may be necessary to correct a prior disclosure that a company determines was untrue (or that omitted a material fact necessary to make the disclosure not misleading) at the time the disclosure was made. It may also be necessary to update a disclosure that became materially inaccurate after it was made. Disclosures should be reviewed and refreshed as events warrant, including during the process of a cyber-breach investigation. Particular care should be given to the adequacy and timing of relevant disclosures prior to any offer or sale of securities by the company or trading by corporate insiders.

3. **Materiality assessments**

Assess whether cybersecurity risks or incidents rise to the level of “material” information, which depends on their “nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations” as well as the risk of litigation or regulatory investigations and the range of harm that could occur to the registrant’s reputation, financial performance and customer and vendor relationships. Omitted information can be material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by a reasonable investor as having significantly altered the total mix of information available.

4. **Risk factors**

Disclose cybersecurity risks and incidents, including risks arising in connection with acquisitions, if they are among the most significant factors that make an investment in the company’s securities speculative or risky. Companies should evaluate factors such as the following to determine the appropriate nature and content of cybersecurity risk factor disclosure: the severity and frequency of any prior cyber incidents; the probability and potential magnitude of future incidents; the adequacy of any preventive measures undertaken; particular aspects of the company’s business and operations that give rise to cyber risks (including industry-specific and third-party supplier and service-provider risks); costs of protective measures, including insurance; the potential for reputational harm; existing and pending laws and regulations and the associated costs to the company; and litigation, regulatory investigation and remediation costs associated with cyber incidents. As noted above, these risk disclosures should be tailored and informative for investors, and framed within an appropriate context, rather than simply providing generic “boilerplate” language that could be applicable to any registrant.

5. **MD&A**

Include discussion relating to a cyber risk or incident in MD&A if the costs associated with that risk or incident represent an event, trend or uncertainty that is likely to have a material effect on the company’s results of operations, liquidity or financial condition or if it would cause reported financial information not to be necessarily indicative of future operating results or financial condition. The 2018 Guidance provides the following non-exclusive list of elements to consider in
this disclosure analysis: the financial effects of the cyber-related costs, such as immediate costs of an incident; remediation efforts; ongoing cybersecurity efforts and enhancements to existing efforts; loss of intellectual property; implementation of preventative measures; insurance; responses to litigation and regulatory investigations; harm to reputation; and loss of competitive advantage. Such costs and impacts should be considered for each of a registrant’s reportable segments.

6. Description of business
Disclose relevant details of a cybersecurity incident or risk within the business description required by Item 101 of Regulation S-K if the incident or risk has a material impact on one of the company’s reportable segments or materially affects the company’s products, services, relationships or competitive conditions.

7. Legal proceedings
Consider whether any legal proceedings involving or related to a cybersecurity incident should be disclosed as material pending legal proceedings as called for by Item 103 of Regulation S-K. If appropriate, such disclosure should include all required information, including the relevant court, dates, parties, factual basis for the claim and relief sought.

8. Financial statement disclosures
Ensure that financial reporting and control systems are designed to provide reasonable assurance that information about the financial impacts of a cybersecurity incident will be included in the company’s financial statements on a timely basis, including, for example, items such as: expenses of investigation, notification, remediation and litigation; loss of revenue or costs of providing customer incentives; costs associated with legal claims or increased insurance costs; diminished future cash flows; asset impairment; recognition of liabilities; and increased financing costs.

9. Board risk oversight
Evaluate the role of the board of directors in cybersecurity risk management. To help investors assess how the company’s board of directors is fulfilling its risk oversight responsibilities, Item 407(h) of Regulation S-K requires a public company to disclose its board of directors’ role in the risk oversight of the company and describe how the board administers this risk oversight function. The 2018 Guidance states that, to the extent cybersecurity risks are material to a company’s business, these governance and risk oversight disclosures should address the nature of the board’s role in the oversight of the company’s cybersecurity risk management and how the board engages with management on cybersecurity issues.

10. Disclosure controls and procedures
Assess the sufficiency of the company’s existing disclosure controls and procedures, and augment or modify these controls and procedures as needed to ensure that relevant information about cyber risks and incidents is processed, summarized and reported on a timely basis and communicated to management to allow management to make informed and timely decisions regarding disclosure of these matters. Additionally, management certifications and evaluations of the company’s disclosure controls and procedures should take into account the adequacy of the established controls and procedures to identify and evaluate the impact of relevant cybersecurity risks and incidents. The 2018 Guidance also points to the role of effective disclosure controls and procedures in facilitating policies and procedures designed to prevent trading by company insiders on the basis of material nonpublic information regarding cybersecurity risks and incidents.
11. Insider trading
Review the company’s insider trading policies and procedures and its code of ethics to determine whether updates are needed to properly address and prevent potential insider trading violations, including those involving cybersecurity-related issues. The 2018 Guidance warns that trading of company securities by directors, officers and other company insiders in breach of their duty of trust or confidence while in possession of material nonpublic information about cybersecurity risks or incidents would violate the antifraud provisions of the federal securities laws and may violate the company’s code of ethics. Additionally, following a significant cybersecurity incident and during the pendency of its investigation and assessment, the affected company should consider whether and when it would be prudent to impose trading restrictions on insiders. The 2018 Guidance notes in this regard the potential benefits of prophylactic measures, including those implemented to avoid the appearance of improper trading occurring between the time of the incident and the time of public disclosure. The 2018 Guidance further indicates, however, that insiders would not be precluded from relying on a properly established Rule 10b5-1 plan.

12. Regulation FD and selective disclosure
Ensure compliance with Regulation FD when communicating information regarding cybersecurity risks and incidents. The company’s disclosure policies and procedures should be reviewed and updated as needed to address and prevent selective disclosure of material nonpublic information regarding cybersecurity risks and incidents and to ensure simultaneous or prompt public disclosure as required by Regulation FD. Directors, officers and other company spokespersons should be reminded of the requirements of Regulation FD and alerted to their applicability in this context.

We expect that cybersecurity will continue to be a top priority for the SEC, as reinforced by the fact that cybersecurity was included again as one of the focus areas of the SEC’s Office of Compliance Inspections and Examinations ("OCIE") in its 2018 National Exam Program Examination Priorities. OCIE states that it will continue to work with firms during exams to focus on identifying and managing cybersecurity risks and threats through an emphasis on governance and risk assessment, access rights and controls, data loss prevention, vendor management, training and incident response.

While the 2018 Guidance is non-binding, it provides helpful insight into the SEC’s views on disclosure requirements for cybersecurity risks and incidents and on the cyber-related policies and procedures the SEC expects public companies to have in place to address cybersecurity-related issues. Chairman Jay Clayton said in his statement on the adoption of the 2018 Guidance that the SEC would continue to evaluate and monitor developments in the cyber disclosure space and consider whether additional guidance or rules may be needed.

For more information on the content of this alert, please contact your regular Nixon Peabody attorney or:

- Kelly Babson at kdbabson@nixonpeabody.com or (617) 345-1036
- Jason P. Gonzalez at jgonzalez@nixonpeabody.com or (213) 629-6019
- Pierce Han at phan@nixonpeabody.com or (202) 585-8139
- Carolyn Lowry at clowry@nixonpeabody.com or (202) 585-8822

---

4 2018 National Exam Program Examination Priorities, available here.
5 Statement on Cybersecurity Interpretive Guidance by SEC Chairman Jay Clayton, Feb. 21, 2018 (available here)