Client Alert | US Public Company Advisory / Capital Markets / Data, Privacy & Cybersecurity

SEC Issues Interpretive Guidance on Public Company Cybersecurity Disclosures: Greater Engagement Required of Officers and Directors

February 2018

Authors: Colin Diamond, Michelle Rutta, Steven Chabinsky, Dov Gottlieb, Irina Yevmenenko

On February 21, 2018, the Securities and Exchange Commission ("SEC") issued an interpretive release[1] providing long-awaited guidance (the "New Guidance") to assist public companies in preparing disclosures about cybersecurity risks and incidents.[2] Significantly, the New Guidance discusses cybersecurity and its related disclosure requirements not merely in terms of network threats and vulnerabilities, but as a key element of enterprise risk management in which program development and oversight responsibilities move straight "up the corporate ladder" to officers and directors.

Various divisions of the SEC increasingly have been active in the cybersecurity arena, including instituting a cybersecurity examination initiative for broker-dealers and investment advisors[3], bringing cybersecurity-related enforcement actions,[4] issuing cybersecurity alerts,[5] and offering updated guidance to funds and advisors.[6] Prior to the New Guidance, however, publicly traded companies primarily looked to the SEC's Division of Corporation Finance ("Corp Fin") for regulatory cues, and in particular to Corp Fin's cybersecurity disclosure guidance of 2011 (the "2011 Guidance")[7]. Although the 2011 Guidance made no mention of officers, directors, or risk management, it did clearly focus on the need for public companies to disclose cyber risks and their related impact within the existing disclosure framework.

---

1 Available here.

2 The New Guidance does not address the specific implications of cybersecurity to other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations.

3 More information available here.

4 See the SEC's Cybersecurity Enforcement Actions, available here.

5 See, for example, here and here.

6 See IM Guidance Update, Cybersecurity Guidance, available here.

7 The 2011 Guidance is available here.

Now, the SEC as a whole has decided to speak. What has changed over the past seven years? In the view of the SEC, both a lot and a little. While network compromises and data breaches continue to occur with increasing frequency and severity, the SEC believes there should have been, but has not been, a corresponding rise in the level of adequate risk disclosure. The facts seem to bear this out. For example, while cybersecurity disclosures have increased fourfold from 2012 to 2016, as of October 2017, only 38% of US public companies cited cybersecurity as a risk factor in their annual and quarterly SEC filings[8]. In connection with the issuance of the New Guidance, Chairman Clayton stated that he believes that "providing the SEC's views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors."[9]

Recognizing that "an evolving landscape of cybersecurity threats" poses "grave threats to investors, our capital markets, and our country", the New Guidance reflects the SEC's belief that "it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion." In addition to "reinforcing and expanding upon the…2011 [G]uidance" with respect to disclosure, the New Guidance also addresses: (i) the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and threats, and (ii) the application of insider trading prohibitions and obligations to refrain from making selective disclosures of material nonpublic information ("MNPI") in the cybersecurity context.

Disclosure Obligations

Consistent with the 2011 Guidance, the New Guidance emphasizes that the materiality of cybersecurity risks and incidents informs the determination as to the disclosures that must be made in registration statements under the Securities Act of 1933 and the Securities Exchange Act of 1934 ("Exchange Act") and periodic and current reports under the Exchange Act. While existing disclosure requirements do not specifically reference cybersecurity risks and incidents, the New Guidance re-emphasizes that an obligation to disclose such risks and incidents could arise in a number of contexts, depending on a company's particular circumstances.

Specifically, the New Guidance encourages public companies to consider their obligation to disclose cyber risks and incidents as they relate to their risk factors, MD&A, description of business, legal proceedings and financial statement disclosures, along with their disclosures regarding the role of the company's board of directors in the risk oversight of the company. In addition to specific disclosure requirements, companies also must disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading."

Materiality is inherently a facts and circumstances determination; the New Guidance indicates that in the context of cybersecurity risks and incidents, materiality depends upon their nature, extent, and potential magnitude, as well as the range of potential reputational and financial harm. Companies also should consider the impact on business relationships, the possibility of legal or regulatory investigations or actions, and the occurrence of any prior incidents. Although companies are required to disclose cybersecurity risks and incidents that are material to investors, the New Guidance reiterates that companies are not expected to disclose publicly specific, information about their cybersecurity systems or vulnerabilities that could compromise their cybersecurity efforts and serve as a roadmap for hackers.

Disclosure Controls and Procedures Related to Cyber Risks and Incidents

The New Guidance encourages companies to 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. Specifically, the New Guidance advises that "[c]ontrols 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

[8] "The Cyber Risk Disclosure Groundswell: Corporate Governance Response in the Specter of SEC Oversight", a study by Intelligize, available here.

[9] Available here.

open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents."

Therefore, while a specific reference to cybersecurity may not be required, a company's conclusions with respect to the effectiveness of disclosure controls and procedures must be informed by management's consideration of cybersecurity risks and incidents. The New Guidance also notes that the principal executive officers and principal financial officers responsible for certifying effectiveness of disclosure controls and procedures under the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley") should take into account the degree to which cybersecurity risks impact the effectiveness of those controls and procedures.

Insider Trading

The New Guidance reminds companies and their directors, officers, and other corporate insiders that information about cybersecurity risks and incidents, including vulnerabilities and breaches, may constitute MNPI, and that trading in the company's securities while in possession of such MNPI would violate antifraud provisions of the US federal securities laws.

Regulation FD and Selective Disclosure

In addition to encouraging companies to continue to use Forms 8-K and 6-K to disclose the occurrence and consequences of material cybersecurity incidents promptly, which the SEC believes reduces the risk of selective disclosure, as well as the risk that trading in such companies' securities on the basis of MNPI may occur, the New Guidance reminds companies that they may also have disclosure obligations under Regulation FD in connection with cybersecurity matters. Namely, companies should not selectively disclose MNPI regarding cybersecurity risks and incidents to Regulation FD enumerated persons before disclosing that same information to the public, and any unintentional selective disclosures will require prompt public disclosure in compliance with Regulation FD.

Mergers & Acquisitions

The New Guidance indicates that companies involved in business combination transactions should disclose cybersecurity risks "that arise in connection with acquisitions." Meeting the SEC's expectations in this regard will require, among other things, that acquiring companies consider the scope of their cybersecurity due diligence efforts and the level of expertise of those performing it.

Practical Considerations

While much of the New Guidance builds upon the 2011 Guidance, its issuance also may indicate that the SEC's "careful [] monitor[ing of] cybersecurity disclosures" will lead to cyber-related enforcement actions and insider trading investigations. In light of the New Guidance, companies are advised to consider the following:

Disclosure

Companies should review their disclosure to ensure it accurately reflects the company's cybersecurity risk profile and the potential impact and costs of cybersecurity efforts and initiatives and related risks. Disclosure should be tailored and company-specific, and should convey that the company has been thoughtful about these issues and will remain engaged on cybersecurity issues as they evolve. Companies should be mindful of the following with respect to the specified portions of their disclosure:

- *Risk Factors*: Evaluate how to communicate risks properly in light of the probability and magnitude of past and potential future cybersecurity events; consider disclosure regarding adequacy of preventive actions; discuss material industry, customer and/or supplier-specific risks that may increase the potential impact; discuss material risks related to insurance and other costs; consider disclosure regarding material risks of reputational harm; and consider disclosure regarding compliance with any applicable regulatory requirements.

- *MD&A*: Consider the costs of ongoing cybersecurity efforts and the consequences of cybersecurity incidents when analyzing the events, trends and uncertainties that are reasonably likely to materially impact financial condition or liquidity.
- *Business Description*: Include disclosure of cybersecurity incidents or risks that materially affect products, services, competitive conditions or business relationships, with additional consideration given to any unique cybersecurity risks that may stem from acquisitions.
- *Financial Statements*: Information about the range and magnitude of cybersecurity events, such as investigation and remediation costs, claims, loss of revenue, diminished future cash flow, impairment of assets, and increased financing costs, should be included in financial statement disclosure on a timely basis.

Disclosure Timing

Despite the 2011 Guidance, disclosure related to cyberattacks has been limited, as companies are reluctant to publicize specific attacks, particularly before they have undertaken a thorough accounting of any such incident and its potential implications. However, while recognizing that "some material facts may not be available at the time of initial disclosure", the SEC has indicated that it expects companies to report a material cyber incident promptly. Significantly, the SEC expressly recognized that cooperating with law enforcement could be an appropriate basis for narrowing the scope of disclosure. Regardless, the New Guidance stresses that a lengthy ongoing internal or external investigation is not, on its own, an acceptable basis for avoiding disclosure of a material cybersecurity incident. Separately, companies should ensure they have a protocol in place to quickly inform necessary personnel, including internal and outside legal counsel, and to determine the appropriate timing, nature and form of potential disclosures and breach notifications in case of a cybersecurity incident.

Crisis Management Team and Incident Response Plan

In light of the need to respond to a cybersecurity incident quickly, companies should have a crisis management team in place, including representatives from investor relations, IT, legal and management, in order to: (i) respond quickly and effectively to a cyber incident, (ii) gather information in order to craft accurate disclosure, and (iii) address shareholder concerns when information is released to the market. Companies should seek the advice of qualified cyber counsel in order to formalize, organize, update, and test the adequacy of their incident response plan. Key personnel, including those responsible for corporate communications, should be trained and kept updated on their responsibilities in the event of a cybersecurity incident.

Correcting or Updating Disclosure

The New Guidance reiterates that companies may have a duty to correct prior disclosure about a cybersecurity event that the company later determines was not accurate (or omitted a material fact about such an event) at the time it was made, or a duty to update disclosure that becomes materially misleading after it was made and is still being relied on by reasonable investors. Companies should consider the need to revisit or refresh previous disclosures, including during the process of investigating a cybersecurity incident.

Risk Management and Oversight

Ensuring the adequacy of a company's cybersecurity measures is a critical part of a board's risk oversight responsibilities. To this end, directors must understand the nature of cybersecurity risk and prioritize their oversight of cyber preparedness, detection, response, and disclosure. Boards should receive periodic updates from management and any relevant expert advisors on the company's compliance with applicable standards. Further, board oversight of cyber risk management, including how the board engages with management on cybersecurity issues, should be disclosed to the extent cybersecurity risks are material to the business. Trusted third party advisors, including outside counsel operating under available attorney-client privilege, can be a valuable resource in educating and assisting companies in organizing their enterprise risk management and oversight to incorporate cybersecurity issues, and in evaluating the adequacy of disclosures.

Disclosure Controls and Procedures

Companies should assess whether they have adequate disclosure controls and procedures in place to ensure that cybersecurity risks and incidents are timely identified, evaluated, and reported up the corporate ladder. Companies should consider adding a technical expert to their subcertification and/or disclosure committee procedures, or include regular consultation with appropriate technical personnel and trusted advisors.

Insider Trading Policies and MNPI: Pre-Clearance and Event-Specific Blackouts

Companies should consider including appropriate safeguards in their insider trading policies and procedures to protect against directors, officers, and other corporate insiders trading on the basis of MNPI before public disclosure of a cybersecurity incident is made. Companies should ensure there are procedures in place to relay cybersecurity events in a timely manner to the individual who administers the company's preclearance policy. In addition, companies should consider providing for event-specific blackouts to allow the company to impose trading restrictions when companies are aware of cyber incident related MNPI. In this regard, companies should consider adding cyber events as a specific example of MNPI to their insider trading policy, in order to make clear that knowledge of such events may qualify as MNPI in the context of insider trading.

Closing Thoughts

The SEC's New Guidance has, in no uncertain terms, declared that cybersecurity is not an IT issue, but a board issue; cybersecurity is not a technical support function, but a risk management function. As a result, officers and directors should be especially mindful of the SEC's new focus on cybersecurity as an integral component of a company's broader enterprise-wide risk management structure, including the SEC's interest in how the board engages with corporate executives to oversee cybersecurity risk. Cybersecurity programs must be designed (with respect to policies, procedures, and implementation) to ensure that principal executive officers and principal financial officers are properly informed to make related disclosure decisions and required certifications under Sarbanes-Oxley. In addition, a corporation's attention to cybersecurity should extend well beyond regulatory compliance. In today's global business environment, ensuring adequate security of a corporation's networks and sensitive data is an important business driver, and therefore an important component of financial growth and value.

White & Case LLP
1221 Avenue of the Americas
New York, New York 10020-1095
United States

T +1 212 819 8200