Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Key Aspects Of SEC Guidance On Cybersecurity Disclosures

By **Mark Krotoski and Kurt Oldenburg** (March 2, 2018, 12:28 PM EST)

Mark Krotoski

Kurt Oldenburg

The U.S. Securities and Exchange Commission on Feb. 21 voted unanimously to approve its commission statement and guidance on public company cybersecurity disclosures. The guidance highlights the need for cybersecurity disclosures based on current reporting obligations and the materiality standard, identifies specific cybersecurity risk factors, and emphasizes two new areas of focus concerning the adoption by public companies of appropriate policies and procedures to address cybersecurity matters and to enforce insider trading prohibitions.

In the guidance, the SEC concluded that, based on "the increasing significance of cybersecurity incidents," it was "necessary to provide further Commission guidance" on cybersecurity disclosures and related issues.[1] As an SEC interpretation,[2] the guidance carries the highest level of authority and "reinforce[es] and expand[s] upon" the prior staff guidance that the SEC staff issued in October 2011.

This article discusses some of the key components contained in the new guidance.

Cybersecurity Disclosures Based on Reporting Obligations

The guidance notes that while current "disclosure requirements do not specifically refer to cybersecurity risks and incidents," the "obligation to disclose such risks and incidents" arises out of "a number of" requirements based on "a company's particular circumstances."[3] This includes, for example, disclosures in periodic reports such as the annual Form 10-K, including within the "management's discussion and analysis" section, and other areas. The guidance surveys many of the reporting requirements that may obligate companies to address cybersecurity risks and incidents in meeting these obligations.

Cybersecurity Disclosures Under the Materiality Standard

Under the guidance, the materiality standard may trigger disclosure obligations related to cybersecurity risks and incidents.[4] Rather than implementing one standard specific to cybersecurity, the materiality determination remains a fact-specific inquiry. The guidance notes 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." A careful assessment and analysis requires that the disclosure is "tailored" to the company's "particular cybersecurity risks and incidents."[5]

A variety of factors weigh on this assessment. It includes "the range of harm that such incidents could cause" 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-US authorities."[6]

In disclosing material cybersecurity risks and incidents, the guidance makes clear that companies are not required to "make detailed disclosures that could compromise its cybersecurity efforts — for example, by providing a 'roadmap' for those who seek to penetrate a company's security protections." The disclosure should not provide information that would make company "systems, networks, and devices more susceptible to a cybersecurity incident."[7]

Timing of Disclosure

The timing of cybersecurity incident disclosure is a critical balance between a company's desire to provide swift disclosure and the importance of ensuring that the essential facts are understood and the disclosed information is accurate. Depending on the nature of the cybersecurity incident, some reasonable amount of time may be required to determine its scope.

The guidance "recognize[s] that a company may require time to discern the implications of a cybersecurity incident."[8] Disclosure also may be affected by requests from law enforcement to cooperate with an ongoing investigation. In considering the timing issue, the guidance observes that "an ongoing internal or external investigation" cannot "provide a basis for avoiding disclosures of a material cybersecurity incident."[9]

Notably, the guidance makes clear that companies "have a duty to correct" disclosures that are determined later to have been untrue when originally made and may have "a duty to update" disclosures that were correct when made based on later material information, such as when reasonable investors are still relying on such disclosure.[10] In particular, "[c]ompanies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident."[11]

Cybersecurity Risk Factors

With regard to the disclosure of cybersecurity risks,[12] the guidance identifies several factors to be considered. Some factors, illustratively, include the following:

- Occurrence of prior cybersecurity incidents;
- Probability of future occurrences and their consequences;
- Adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs;
- Aspects of the company's business and operations that give rise to material cybersecurity risks, and the potential costs and consequences of such risks;
- 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;

- Litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.[13]

As noted in the first bullet above, the guidance states that prior or ongoing cybersecurity incidents need to be considered. For example, it may be necessary "to discuss the occurrence of that [prior] cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose particular risks to the company's business and operations."[14] The guidance notes also that other relevant factors when crafting risk factor disclosure may include "[p]ast incidents involving suppliers, customers, competitors, and others."[15]

Management's Discussion and Analysis of Financial Condition and Results of Operations

Cybersecurity disclosures may be required as part of the management's discussion and analysis of financial conditions, changes in financial condition, and results of operations.[16] As the guidance notes, this may include "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."[17]

The Role of the Board

The guidance notes that disclosure about how the board of directors oversees management's actions relating to cybersecurity risks is important to investors' assessment of how the board is fulfilling its responsibilities in the area of risk oversight.

New Areas of Focus Not Included in Prior Staff Guidance

The guidance emphasizes two areas that were not addressed in the 2011 SEC staff guidance:

Cybersecurity Policies and Procedures

First, the SEC makes clear that public companies must "maintain[] comprehensive policies and procedures related to cybersecurity risks and incidents" that include "appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity."[18] Senior management should receive sufficient information about cybersecurity risks and incidents to enable them to make disclosure decisions and execute necessary certifications.[19] To that end, the guidance states that "[a] company's disclosure controls and procedures should not be limited to disclosure specifically required, but should also ensure timely collection and evaluation of information potentially subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company's businesses."[20]

In particular, the guidance further notes the following:

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.[21]

Insider Trading Policies and Procedures Related to Cyberrisks and Incidents

The second area highlighted by the SEC is the need for companies to abide by insider trading prohibitions. The SEC expects companies "to take steps to prevent directors and officers (and other corporate insiders who were aware of these [cyber incident or risk] matters) from trading its securities until investors have been appropriately informed about the incident or risk."[22] The SEC emphasizes the role of "well designed policies and procedures to prevent trading on the basis of all types of material nonpublic information, including information relating to cybersecurity risks and incidents."[23] Additionally, the guidance notes that prophylactic measures in insider trading policies and procedures can protect against directors, officers, and other corporate insiders trading before public disclosure of a cybersecurity incident, while also allowing a company to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure.[24]

Diverging Commissioner Views

While the vote in favor of the guidance was unanimous, the commissioners diverged on whether more can and should be done:

- SEC Chairman Jay Clayton stated his belief that 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." He emphasized that public companies should "examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."[25]

- Commissioner Kara M. Stein noted that "meaningful disclosure has remained elusive" after the 2011 staff guidance, and she was "disappointed with the Commission's limited action."[26] She contended that more can be done given that the guidance "provides only modest changes" to the 2011 staff guidance, and she expressed doubts about whether "rebranded guidance will actually help companies provide investors with comprehensive, particularized, and meaningful disclosure about cybersecurity risks and incidents."[27]

- Commissioner Robert J. Jackson Jr. "reluctantly" supported the guidance, which he observed "essentially reiterates years-old staff-level views on this issue" when "much more needs to be done."[28]

These divergent views suggest that the SEC will revisit the guidance and regulation of cybersecurity disclosures — but for now, the guidance is controlling.

Beyond the Guidance: Other Cybersecurity Regulatory Considerations

One area not mentioned in the guidance, but which regularly occurs, involves compliance with cybersecurity requirements of U.S. or international authorities other than the SEC. Many public companies have cybersecurity standards that must be considered in U.S. federal and state and other global jurisdictions. As such, any SEC disclosures should be considered in the context of other regulatory requirements.

For example, different notification standards are applied by different regulators. Consider these examples for individual or public agency notification:

- Under California law, data breach notification is required to affected individuals "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement ... or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[29]

- For some U.S. states, data breach notification to an individual is required no later than a specific period, such as 30 days in Florida, 45 days in Ohio and Washington, and 90 days in Connecticut.[30]

- Under the New York State Department of Financial Services Cybersecurity Regulation enacted in 2017, notification is required to the agency "as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following: (1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity."[31]

- Other public agency notifications may be required. For example, in California, "a security breach notification" to "more than 500 California residents as a result of a single breach of the security system" also requires notification to the California attorney general.[32]

- Companies that are subject to the forthcoming General Data Protection Regulation will have an obligation to notify the European supervisory authorities within 72 hours of a cybersecurity incident that involves personal data (i.e., any information identifying an individual) unless it is unlikely to result in a risk to the privacy rights and other "rights and freedoms" of the affected individuals. For incidents where there is likely to be a high risk of harm to the individuals, they must be notified directly "without undue delay".[33]

As noted above, a single public company that is subject to the foregoing enforcement agencies will have different notification standards to meet. These are only examples, as other variations exist in the cybersecurity regulations and statutes. Careful consideration of these issues should be undertaken when disclosures are made for any of the applicable cybersecurity statutes and regulations.

Recommendations and Next Steps

The SEC has focused its attention and resources on enforcement of cybersecurity issues. On Sept. 25, 2017, the SEC announced the establishment of a "Cyber Unit" designed to "focus the Enforcement Division's substantial cyber-related expertise on targeting cyber-related misconduct."[34]

The guidance represents a significant development on the disclosure of cybersecurity risks and incidents. In light of the guidance, public companies should consider the following steps in addressing cybersecurity risks and disclosures:

- Reports: Future reporting obligations (such as Form 10-K or the management's discussion and analysis section) should be carefully evaluated in the context of the new guidance.

- Materiality Standard: The SEC will continue to apply the fact-specific materiality standard for disclosing a breach. Key issues may include the nature and scope of the attack, the nature of any information compromised, and any resulting harm or costs, including from litigation or regulatory investigations.

- Timing: The timing of any disclosures should be measured against the ability to obtain the necessary facts based on an investigation and obligation to disclose.

- Other Cybersecurity Regulations: The impact of any disclosures should be considered along with the timing under different applicable regulatory or statutory standards at the U.S. federal and state or international levels.

- Prior Disclosures: Past cybersecurity disclosures should be analyzed to determine if they should be corrected or if there may be a duty to update as further material information becomes known.

- Effective Controls and Procedures: Controls and procedures should be reviewed to ensure that cybersecurity risks and potential incidents are identified and addressed.

- Insider Trading Program and Policies: In order to avoid insider trading questions or investigations, insider trading policies should be implemented that encompass cybersecurity incidents. Insider trading policies that include prophylactic measures "can protect against directors, officers, and other corporate insiders trading on the basis of material nonpublic information before public disclosure of the cybersecurity incident."[35]

- Other Practical Measures: Companies also should develop practical tools and response plans before incidents arise.[36]

Mark Krotoski is a partner in the Washington, D.C., office of Morgan Lewis & Bockius LLP. Kurt Oldenburg is an associate in the firm's San Francisco office.

[1] Guidance at 6

[2] See SEC Press Release, "SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures," (Feb. 21, 2018)

[3] Id. at 7-8

[4] See, e.g., TSC Industries v. Northway, 426 U.S. 438, 449 (1976) (A fact is material "if there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available" to the shareholder) (as cited in the Guidance at 10

n.32)

[5] Guidance at 13

[6] Id. at 10-11

[7] Id. at 11

[8] Id. at 12

[9] Id.

[10] Id. but see n.37 in the Guidance.

[11] Id.

[12] As required under 17 CFR 229.503(c); 17 CFR 249.220f (cited in Guidance at 13 and n.39)

[13] Guidance at 13-14

[14] Id. at 14-15

[15] Id. at 15

[16] See Item 303 of Regulation S-K; Form 20-F, Item 5; see also Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056] Commission Statement About Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8056 (Jan. 22, 2002) [67 FR 3746]; Management's Discussion and Analysis of Financial Condition and Results of Operations; and Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427]

[17] Guidance at 15

[18] Id. at 6

[19] Id. at 18-19.

[20] Id. at 19.

[21] Id. at 20

[22] Id. at 6-7

[23] Id. at 22

[24] Id.

[25] SEC Chairman Jay Clayton, Statement on Cybersecurity Interpretive Guidance (Feb. 21, 2018)

[26] SEC Commissioner Kara M. Stein, Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018).

[27] Id.

[28] SEC Commissioner Robert J. Jackson Jr., Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018).

[29] Cal. Civil Code §1798.82(a)

[30] Conn. Gen. Stat. § 36a-701b(b)(1); Fla. Stat. § 501.171(4)(a); Ohio Rev. Code § 1349.19(B)(1); Wash. RCW § 19.255.010(16)

[31] 23 NYCRR § 500.17

[32] Cal. Civil Code §1798.82(f)

[33] Article 34 of the GDPR

[34] See SEC Press Release, "SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors" (Sept. 25, 2017)

[35] Guidance at 22.

[36] See our six-phase outline of procedures that companies should consider incorporating into their cybersecurity incident response
plans. https://www.morganlewis.com/blogs/sourcingatmorganlewis/2015/10/check-it-out-morgan-lewis-data-breach-checklist-available-now