HUNTON& WILLIAMS

Client Alert

February 2018

SEC Publishes New Guidance on Public Company Cybersecurity Disclosure

The US Securities and Exchange Commission (SEC) published long-awaited cybersecurity interpretive guidance for public companies on February 21, 2018. The new interpretive guidance, while not revolutionary, marks the first time that the five SEC commissioners, as opposed to agency staff, have provided official agency guidance to public companies regarding their cybersecurity disclosure and compliance obligations. The guidance reiterates public companies' obligation to disclose material information to investors, particularly when that information concerns cybersecurity risks or incidents. It also addresses two topics not previously addressed by agency staff: the importance of cybersecurity policies and procedures in the context of disclosure controls, and the application of insider trading prohibitions in the cybersecurity context.

Key Points

As detailed below, the new guidance focuses on several key points that we believe reflect learnings from the SEC's recent experiences regarding both the Division of Enforcement's investigations of public companies involved in cyber events and the Division of Corporation Finance's ongoing disclosure reviews of registration statements and periodic filings. Central to the guidance are the following themes:

- Crucial to a public company's ability to make required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact such matters may have on the company, as well as a protocol to determine the potential materiality of the risks and incidents.

- Development of effective disclosure controls and procedures is best achieved when a company's directors, officers and others responsible for developing and overseeing the controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face.

- The SEC is concerned about potential insider trading around cyber events, and companies should scrutinize their compliance policies to ensure that such activity is sufficiently addressed.

- In light of the guidance's discussion concerning the potential materiality of cybersecurity, companies should consider whether they need to revisit or refresh previous disclosures made to investors.

Background

The SEC introduced the guidance by observing that "cybersecurity risks pose grave threats to investors, our capital markets, and our country." The guidance notes the rapidly evolving technological landscape in which modern public companies operate, then catalogs a series of costs and other negative consequences that companies falling victim to cyberattacks may suffer:

- remediation costs, such as liability for stolen assets or information, repairs of system damage and incentives 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 and consultants;
- 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 state and federal governmental authorities and non-US 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.

Given the frequency, magnitude and cost of cybersecurity incidents, the SEC expresses its 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 doing so, the SEC notes that this requirement applies not just to companies that have suffered a cyber incident, but also to those that are subject to material cybersecurity risks but may not yet have been the target of a cyberattack.

Materiality of Cybersecurity Disclosure

The new guidance provides a number of pointers as to how a public company should undertake a materiality analysis in the context of a cybersecurity risk or incident. In determining their disclosure obligations, the guidance notes that companies should generally weigh, among other factors, 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 SEC emphasizes 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 such incidents could cause. According to the SEC, such harm could include damage 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, federal and foreign governmental authorities.

The guidance further emphasizes that public companies are not expected to publicly disclose specific, technical information about their cybersecurity systems, nor are they required to disclose potential system vulnerabilities in such detail as to empower threat actors to gain unauthorized access. Moreover, the SEC recognizes that a company may require time to gather the material facts related to a cybersecurity incident before making appropriate disclosure. The SEC also notes that while it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding an incident, the existence of an ongoing internal or external investigation does not on its own provide a basis for avoiding disclosures of a material cybersecurity incident. Likewise, the SEC expects that when a company becomes aware of a cybersecurity risk or incident that would be material to investors, the company should make appropriate disclosure prior to the offer and sale of securities. It should also take steps to prevent insiders from trading in its securities until investors have been appropriately informed about the risk or incident. Notably, the SEC did not impose a Form 8-K reporting obligation regarding cyber events.

Additionally, the guidance provides insight into the SEC's views on the duty to correct and the duty to update in the context of cyber disclosure. The guidance reminds companies that they may have a duty to correct prior disclosure that the company later determines was untrue (or if it omitted a material fact) at the time it was made, such as when a company subsequently discovers contradictory information that existed at the time of the initial disclosure. Likewise, companies may have a duty to update disclosure that becomes materially inaccurate after it is made, such as when an erroneous original statement is still being relied on by investors. Companies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident. As always, the SEC eschews boilerplate disclosures and reminds companies to provide information specifically tailored for their own circumstances.

Risk Factors

The guidance urges companies to consider the following cyber risk factors, among others:

- 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.

Elaborating further, the SEC notes that companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context. For example, the SEC posits that if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident "may" occur. Instead, the SEC believes the company may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose specific risks to the company's business and operations.

MD&A

In preparing MD&A disclosure, the SEC reminds companies that 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, may be relevant to the company's analysis. In addition, companies should consider the need to discuss the various costs associated with cybersecurity issues, including:

- loss of intellectual property;
- the immediate costs of an 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.

Description of Business

Regarding Item 101 of Regulation S-K, the SEC reminds companies that if cybersecurity incidents or risks materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company should provide appropriate disclosure around those issues.

Legal Proceedings

In preparing disclosures under Item 103 of Regulation S-K, the SEC observes that material legal proceedings may include those related to cybersecurity issues. By way of example, the SEC indicates that if a company experiences a cybersecurity incident involving the theft of customer information and the incident results in material litigation by customers against the company, the company should describe the litigation, including the name of the court in which the proceedings are pending, the date the proceedings are instituted, the principal parties, a description of the factual basis alleged to underlie the litigation and the relief sought.

Financial Statement Disclosure

The new guidance provides several examples of how cybersecurity risks and incidents may affect a company's financial statements, including:

- 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.

In this regard, the SEC expects that a company's financial reporting and control systems would be designed to provide reasonable assurance that information about the range and magnitude of the

financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available.

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, such as how the board administers its oversight function and the effect this has on the board's leadership structure. To the extent cybersecurity risks are material to a company's business, the SEC believes this discussion should include the nature of the board's role in overseeing the management of that risk. Additionally, the SEC believes disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues will allow investors to assess how a board of directors is discharging its risk oversight responsibility.

Disclosure Controls and Procedures

The guidance encourages public 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. To that end, the SEC urges companies to assess 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 and 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.

When designing and evaluating disclosure controls and procedures, the SEC reminds companies they should consider whether such controls and procedures will appropriately record, process, summarize and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. 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.

When a company's principal executive officer and principal financial officer make required certifications under Exchange Act Rules 13a-14 and 15d-14 regarding the design and effectiveness of disclosure controls and procedures, the SEC notes that management should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.

Insider Trading

Perhaps in response to several recent events involving allegations of insider trading around cyber incidents that received significant media coverage, the new guidance also provides direction on insider trading law as it relates to information about cybersecurity risks and incidents, including vulnerabilities and breaches. Put simply, the SEC is of the view that information about a company's cybersecurity risks and incidents may be material nonpublic information, and the SEC believes that directors, officers and other corporate insiders would violate the antifraud provisions of the federal securities laws if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.

The guidance encourages companies to consider how their codes of ethics and insider trading policies take into account and seek to prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents. In this respect, the SEC believes that it is important to have 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.

In addition, while companies are investigating and assessing significant cybersecurity incidents, and determining the underlying facts, ramifications and materiality of these incidents, the SEC urges them to consider whether and when it may be appropriate to implement restrictions on insider trading in their securities. The SEC favors insider trading policies and procedures that include prophylactic measures designed to prevent directors, officers and other corporate insiders from trading on the basis of material nonpublic information before public disclosure of the cybersecurity incident. The SEC also believes that companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure.

Regulation FD

The guidance concludes with a reminder that public companies are prohibited in many circumstances from making selective disclosure about cybersecurity matters under SEC Regulation FD. Again, the SEC expects companies to have policies and procedures to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively, and that any Regulation FD required public disclosure is made in a manner otherwise compliant with the requirements of that regulation.

Commissioner Stein's Public Statement

The new guidance is perhaps most notable for the issues it does not address. In a statement issued coincident with the release of the new guidance, Commissioner Kara Stein expressed disappointment that the new guidance did not go further and highlighted four areas where she would have preferred the SEC to have sought public comment in connection with commencing rulemaking. These areas concern:

- rules that address improvements to the board's risk management framework related to cyber risks and threats;
- minimum standards to protect the personally identifiable information of investors and whether such standards should be required for key market participants, such as broker-dealers, investment advisers and transfer agents;
- rules that would require a public company to provide notice to investors (e.g., a Current Report on Form 8-K) in an appropriate time frame following a cyberattack and to provide disclosure that is useful to investors, without harming the company competitively; and
- rules that are more programmatic and that would require a public company to develop and implement cybersecurity-related policies and procedures beyond merely disclosure.

Final Takeaways

Because the SEC cannot legally use interpretive guidance to announce new law or policy—the Administrative Procedure Act still requires public notice and comment for any rulemaking—the guidance is evolutionary, rather than revolutionary. Still, it consolidates into a single document the SEC's latest thinking on this important issue, and spares public companies the need to sift through prior staff

interpretive guidance,[1] staff speeches and publicly available staff comment letters to divine the agency's views on these issues. The guidance signals a number of areas where the SEC expects companies to enhance their compliance policies and procedures, such as those regarding disclosure controls and insider trading. Now is a good time for public companies to begin that review. Companies also should consider whether their current cybersecurity disclosures are consistent with the many topics the guidance addresses.

Given the intense public and political interest in cybersecurity disclosure by public companies, we anticipate that this latest guidance will not be the SEC's final word on this critical issue. Indeed, the SEC noted that the commissioners and staff continue to monitor cybersecurity disclosures carefully.

The new guidance makes clear that the SEC "continues to consider other means of promoting appropriate disclosure of cyber incidents." The SEC has not yet brought a significant enforcement action against a public company due to perceived deficiencies in cybersecurity disclosure. With the release of the new guidance and the clarification of the SEC's views on these issues, companies are also now on notice as to what the agency's Division of Enforcement will expect.

Contacts

Lisa J. Sotto
lsotto@hunton.com

Scott H. Kimpel
skimpel@hunton.com

Matthew P. Bosher
mbosher@hunton.com

Aaron P. Simpson
asimpson@hunton.com

W. Lake Taylor Jr.
tlake@hunton.com

Paul M. Tiao
ptiao@hunton.com

Brittany M. Bacon
bbacon@hunton.com

[1] The SEC staff has not as of yet taken steps to withdraw the Division of Corporation Finance's CF Disclosure Guidance: Topic No. 2 — Cybersecurity, issued in 2011, though its content is largely subsumed into this new guidance. Rules and interpretive materials issued by other SEC offices and divisions with respect to other regulated entities (e.g., broker-dealers or investment advisers) is unaffected by the new guidance.