No. 2018-01
22 February 2018

SEC Reporting Update

SEC issues guidance on cybersecurity

In this issue:

What you need to know

- The SEC issued interpretive guidance on cybersecurity that goes beyond the staff's 2011 disclosure guidance by addressing the importance of insider trading prohibitions and the application of disclosure controls and procedures to cybersecurity risks and incidents.
- The new guidance, which carries more weight because it was issued by the Commission itself, largely incorporates the staff's previous guidance.
- The Commission warned registrants and their directors, officers and other corporate insiders about the consequences of insider trading if they have material, nonpublic information about cybersecurity risks and incidents.
- The Commission and the SEC staff continue to monitor cybersecurity disclosures carefully and will consider whether additional actions are needed.
- The guidance will become effective after it's published in the Federal Register.

Overview

The Securities and Exchange Commission (SEC or Commission) unanimously approved the issuance of an interpretive release outlining its views on cybersecurity disclosure requirements under federal securities laws as they apply to public operating companies. The release does not address the implications of cybersecurity for other regulated entities such as registered investment companies, investment advisers, brokers, dealers, exchanges and self-regulatory organizations.

"Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack" the SEC said.

The release builds upon the SEC's Division of Corporation Finance CF Disclosure Guidance: Topic No. 2 – *Cybersecurity*, issued in 2011, in a number of ways, including:

- Clarifying that disclosure controls and procedures should enable registrants to identify cybersecurity risks and incidents, assess and analyze their implications and make timely disclosures
- Highlighting the importance of maintaining insider trading and Regulation FD policies that effectively address the fact that cybersecurity risks and incidents can constitute material, nonpublic information
- Expanding the existing disclosure guidance to address how the board of directors oversees the management of cybersecurity risk, as well as management's discussion and analysis of how cybersecurity incidents affected reportable segments
- Discussing how materiality, as well as the many laws, rules, regulations and SEC form requirements, must be considered when preparing cybersecurity disclosures
- Elevating the guidance from non-authoritative positions taken by the staff to an interpretation of the Commission

'We will continue to evaluate developments in this area and consider feedback about whether any further guidance or rules are needed.'

– SEC Chairman Jay Clayton

How we see it

The interpretive release represents a meaningful progression in the SEC's approach to cybersecurity disclosures and related corporate governance considerations. However, the release did not make significant changes to the existing SEC staff disclosure guidance on cybersecurity. Therefore, if a registrant has already been applying the staff disclosure guidance diligently, the new interpretive release will likely not require significant additional disclosures.

We encourage companies to review their cybersecurity disclosures in light of the SEC interpretive guidance and the evolving landscape of cyber risks and cybersecurity.

As companies are considering this guidance and taking a fresh look at their cybersecurity disclosures, they may find our publication, SEC Reporting Update, *Spotlight on cybersecurity disclosures*, helpful.

The Appendix provides relevant excerpts from the Commission's guidance that we have organized into three broad categories: general disclosure guidance, specific disclosure guidance and corporate governance and compliance.

Appendix: Excerpts from the Commission guidance

General disclosure guidance

Materiality

"Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in [SEC] registration statements … and periodic and current reports. … 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.

Avoiding a roadmap for hackers and boilerplate language

This guidance is not intended to suggest that a company should 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 SEC does] not expect companies to publicly disclose specific, technical information about the 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. Nevertheless, [the SEC expects] companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences.

[The SEC expects] companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents. … Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

Timing of disclosure

Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, [the SEC] would expect it 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 who were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk.

Understanding that some material facts may be not available at the time of the initial disclosure, [the SEC recognizes] that a company may require time to discern the implications of a cybersecurity incident. [The SEC also recognizes] that it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident. However, an ongoing internal or external investigation — which often can be lengthy — would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.

Duty to correct and update

[The Commission reminds] companies that they may have a duty to correct prior disclosure that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made (for example, if the company subsequently discovers contradictory information that existed at the time of the initial disclosure), or a duty to update disclosure that becomes materially inaccurate after it is made (for example, when the original statement is still being relied on by reasonable investors). Companies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

Specific disclosure guidance

Risk factors

Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose the most significant factors that make investments in the company's securities speculative or risky. Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among such factors, including risks that arise in connection with acquisitions.

It would be helpful for companies to consider the following issues, among others, in evaluating 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.

In meeting their disclosure obligations, 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, 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 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 particular risks to the company's business and operations. Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure. In certain circumstances, this type of contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors.

Management's discussion and analysis

[Management's discussion and analysis in SEC filings requires] a discussion of events, trends, or uncertainties that are reasonably likely to have a material effect on its results of operations, liquidity, or financial condition, or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition and such other information that the company believes to be necessary to an understanding of its financial condition, changes in financial condition, and results of operations. 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. Finally, the Commission expects companies to consider the impact of such incidents on each of their reportable segments.

Description of business

[The business description section of SEC filings requires] companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions. 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 disclosure.

Legal proceedings

Item 103 of Regulation S-K requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party. Companies should note that this requirement includes any such proceedings that relate to cybersecurity issues. For example, 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 thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.

Financial statement disclosures

Cybersecurity incidents and the risks that result therefrom may affect a company's financial statements. For example, cybersecurity incidents may result in:

- 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 Commission 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.

Risk oversight by board of directors

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. In addition, [the SEC believes] disclosures regarding a company's

cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.

Current reports on Forms 8-K and 6-K

In order to maintain the accuracy and completeness of effective shelf registration statements with respect to the costs and other consequences of material cybersecurity incidents, companies can provide current reports on Form 8-K or Form 6-K. Companies also frequently provide current reports on Form 8-K or Form 6-K to report the occurrence and consequences of cybersecurity incidents. 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. This practice reduces the risk of selective disclosure, as well as the risk that trading in their securities on the basis of material non-public information may occur.

Exchange Act Rule 12b-20 and Securities Act Rule 408

In addition to the information expressly required by Commission regulation, [Exchange Act Rule 12b-20 and Securities Act Rule 408 require registrants] to 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.' The Commission considers omitted information to be material if there is a substantial likelihood that a reasonable investor would consider the information important to 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.

Corporate governance and compliance

Disclosure controls and procedures

Cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws. [The SEC 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. Companies should 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.

Pursuant to Exchange Act Rules 13a-15 and 15d-15, companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness. … 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. Information also must be evaluated in the context of the disclosure requirement of Exchange Act Rule 12b-20. When designing and evaluating disclosure controls and procedures, companies 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.

[Certifications by a company's principal executive officer and principal financial officer and disclosures on the effectiveness of disclosure controls and procedures] 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

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. [Under Exchange Act Rule 10b5-1(a),] 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.' As noted above, 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.

Beyond the antifraud provisions of the federal securities laws, companies and their directors, officers, and other corporate insiders must comply with all other applicable insider trading related rules. Many exchanges require listed companies to adopt codes of conduct and policies that promote compliance with applicable laws, rules, and regulations, including those prohibiting insider trading. [The SEC encourages] companies to consider how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents. The Commission believes that it is important to have well designed policies and procedures to prevent trading on the basis of all types of material non-public 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, they should consider whether and when it may be appropriate to implement restrictions on insider trading in their securities. Company insider trading policies and procedures 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. As noted above, [the SEC 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 and selective disclosure

Companies also may have disclosure obligations under Regulation FD in connection with cybersecurity matters. … In cases of selective disclosure of material nonpublic information related to cybersecurity, companies should ensure compliance with Regulation FD. Companies and persons acting or their behalf should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents … before disclosing that same information to the public. [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 simultaneously (in the case of an intentional disclosure) or promptly (in the case of a non-intentional disclosure) and is otherwise compliant with the requirements of that regulation."