**SECURITIES AND EXCHANGE COMMISSION**

**17 CFR Parts 229 and 249**

**[Release Nos. 33-10459; 34-82746]**

**Commission Statement and Guidance on Public Company Cybersecurity Disclosures**

**AGENCY: Securities and Exchange Commission.**

**ACTION: Interpretation.**

**SUMMARY:** The Securities and Exchange Commission (the "Commission") is publishing interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

EFFECTIVE DATE: [insert date of publication in the Federal Register]

FOR FURTHER INFORMATION CONTACT: Questions about specific filings should be directed to staff members responsible for reviewing the documents the company files with the Commission. For general questions about this release, contact the Office of the Chief Counsel at (202) 551-3500 in the Division of Corporation Finance, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

## I. Introduction

### A. Cybersecurity

Cybersecurity risks pose grave threats to investors, our capital markets, and our country.[1] Whether it is the companies in which investors invest, their accounts with financial services firms, the markets through which they trade, or the infrastructure they count on daily, the

[1] The U.S. Computer Emergency Readiness Team defines cybersecurity as "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#C (Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009).

investing public and the U.S. economy depend on the security and reliability of information and communications technology, systems, and networks. Companies today rely on digital technology to conduct their business operations and engage with their customers, business partners, and other constituencies. In a digitally connected world, cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission.

As companies' exposure to and reliance on networked systems and the Internet have increased, the attendant risks and frequency of cybersecurity incidents also have increased.[2] Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century. Cybersecurity incidents[3] can result from unintentional events or deliberate attacks by insiders or third parties, including cybercriminals, competitors, nation-states, and "hacktivists."[4] Companies face an evolving landscape of cybersecurity threats in which hackers use a complex array of means to perpetrate cyber-attacks, including the use of stolen access credentials, malware, ransomware, phishing,

[2] See World Economic Forum, Global Risks Report 2017, 12th Ed. (Jan. 2017), available at https://www.weforum.org/reports/the-global-risks-report-2017 (concluding that "greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyber-attacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways."). See also PwC, "Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016" (Oct. 2015), available at https://www.pwccn.com/en/retail-and-consumer/rcs-info-security-2016.pdf. (finding that in 2015 there was a reported 38% increase in detected information security incidents from 2014).

[3] A "cybersecurity incident" is "[a]n occurrence that actually or potentially results in adverse consequences to … an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences." U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#I.

[4] One study using a sample of 419 companies in 13 countries and regions noted that 47 percent of data breach incidents in 2016 involved a malicious or criminal attack, 25 percent were due to negligent employees or contractors (human factor) and 28 percent involved system glitches, including both IT and business process failures. See Ponemon Institute and IBM Security, 2017 Cost of Data Breach Study: Global Overview (Jun. 2017), available at https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states.

structured query language injection attacks, and distributed denial-of-service attacks, among other means. The objectives of cyber-attacks vary widely and may include the theft or destruction of financial assets, intellectual property, or other sensitive information belonging to companies, their customers, or their business partners. Cyber-attacks may also be directed at disrupting the operations of public companies or their business partners. This includes targeting companies that operate in industries responsible for critical infrastructure.

Companies that fall victim to successful cyber-attacks or experience other cybersecurity incidents may incur substantial costs[5] and suffer other negative consequences, which may include:

- 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;[6]
- 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

[5] The average organizational cost of a data breach in the United States in 2016 was $7.35 million based on the sample in the study. Id. However, the total costs a company may incur in connection with a particular cyber-attack or incident could be much higher.

[6] A company's costs may also include payments to perpetrators of ransomware attacks in order to attempt to restore operations or protect customer data or other proprietary information. But see Federal Bureau of Investigation, "How To Protect your Network from Ransomware," Ransomware Prevention and Response for CISOs, available at https://www.justice.gov/criminal-ccips/file/872771/download.

governmental authorities and non-U.S. authorities;[7]

- 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 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. Crucial to a public company's ability to make any 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 that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents.[8] In addition, the Commission believes that the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face.

Additionally, directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include

[7] See, e.g., New York State Department of Financial Services, 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies; European Union General Data Protection Regulation, Council Regulation 2016/679, 2016 O.J. (L 119) 1.

[8] See Section II.B.1 below for further discussion of disclosure controls and procedures.

knowledge regarding a significant cybersecurity incident experienced by the company. Public companies should have policies and procedures in place to (1) guard against directors, officers, and other corporate insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material nonpublic information about the incident, and (2) help ensure that the company makes timely disclosure of any related material nonpublic information.[9] In addition, we believe that companies are well served by considering the ramifications of directors, officers, and other corporate insiders trading in advance of disclosures regarding cyber incidents that prove to be material. We recognize that many companies have adopted preventative measures to address the appearance of improper trading and we encourage companies to consider such preventative measures in the context of a cyber event.

B. CF Disclosure Guidance: Topic No. 2

In October 2011, the Division of Corporation Finance (the "Division") issued guidance that provided the Division's views regarding disclosure obligations relating to cybersecurity risks and incidents.[10] The guidance explains that, although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, companies nonetheless may be obligated to disclose such risks and incidents.[11] After the issuance of the guidance, many companies included additional cybersecurity disclosure, typically in the form of risk factors.[12]

[9] See Section II.B.2 below for further discussion of insider trading.

[10] See CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[11] Id.

[12] For example, Willis North America released a 2013 report that found that approximately 88% of the public Fortune 500 companies and about 78% of the Fortune 501-1000 companies included risk factor disclosure regarding cybersecurity in their annual reports filed in 2012. See Willis Fortune 1000 Cyber Disclosure Report (Aug. 2013),

C. Purpose of Release

In light of the increasing significance of cybersecurity incidents, the Commission believes it is necessary to provide further Commission guidance. This interpretive release outlines the Commission's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies.[13] While the Commission continues to consider other means of promoting appropriate disclosure of cyber incidents, we are reinforcing and expanding upon the staff's 2011 guidance. In addition, we address two topics not developed in the staff's 2011 guidance, namely the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context.

First, this release stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. Companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity. Such robust disclosure controls and procedures assist companies in satisfying their disclosure obligations under the federal securities laws.

---

available at http://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf. In 2015, over 88% of Russell 3000 companies disclosed cybersecurity as a risk. See Audit Analytics, "Cybersecurity Disclosure in Risk Factors," (Jan. 14, 2016), available at http://www.auditanalytics.com/blog/cybersecurity-disclosures-in-risk-factors/.

[13] This release 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. For example, in 2014 the Commission adopted Regulation Systems Compliance and Integrity, applicable to certain self-regulatory organizations, to strengthen the technology infrastructure of the U.S. securities markets. Final Rule: Regulation Systems Compliance and Integrity, Release No. 34-73639 (Nov. 19, 2014) [79 FR. 72252 (Dec. 5, 2014)], available at https://www.sec.gov/rules/final/2014/34-73639.pdf. For additional cybersecurity regulations and resources, see the Commission's website page devoted to cybersecurity issues, available at https://www.sec.gov/spotlight/cybersecurity; see also Cybersecurity Guidance; IM Guidance Update (April 2015), available at https://www.sec.gov/investment/im-guidance-2015-02.pdf (staff guidance on cybersecurity measures for registered investment companies and investment advisers).

Second, we also remind companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and also of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.[14]

The Commission, and the staff through its filing review process, continues to monitor cybersecurity disclosures carefully.

## II. Commission Guidance

### A. Overview of Rules Requiring Disclosure of Cybersecurity Issues

#### 1. Disclosure Obligations Generally; Materiality

Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements under the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act"), and periodic and current reports under the Exchange Act.[15] When a company is required to file a disclosure document with the Commission, the requisite form generally refers to the disclosure requirements of Regulation S-K[16] and Regulation S-X.[17] Although these disclosure

[14] See Final Rule: Selective Disclosure and Insider Trading, Release No. 33-7881 (Aug. 15, 2000) [65 FR 51715 (Aug. 24, 2000)], available at https://www.sec.gov/rules/final/33-7881.htm.

[15] Listed companies also should consider any obligations that may be imposed by exchange listing requirements. For example, the NYSE requires listed companies to "release quickly to the public any news or information which might reasonably be expected to materially affect the market for its securities." See NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Developments. In addition, in 2015, the NYSE, in partnership with Palo Alto Networks, published a summary of information about legal and regulatory aspects of cybersecurity governance for directors and officers of public companies. See Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers. Chicago: Caxton Business & Legal, Inc., 2015, available at https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf. Similarly, Nasdaq requires listed companies to "make prompt disclosure to the public of any material information that would reasonably be expected to affect the value of its securities or influence investors' decisions." See Nasdaq Listing Rule 5250(b)(1).

[16] 17 CFR 229.10 et seq.

requirements do not specifically refer to cybersecurity risks and incidents, a number of the requirements impose an obligation to disclose such risks and incidents depending on a company's particular circumstances. For example:

- Periodic Reports: Companies are required to file periodic reports[18] to disclose specified information on a regular and ongoing basis.[19] These periodic reports include annual reports on Form 10-K,[20] which require companies to make disclosure regarding their business and operations, risk factors, legal proceedings, management's discussion and analysis of financial condition and results of operations ("MD&A"), financial statements, disclosure controls and procedures, and corporate governance.[21] Periodic reports also include quarterly reports on Form 10-Q,[22] which require companies to make disclosure regarding their financial statements, MD&A, and updated risk factors.[23] Likewise, foreign private issuers are required to make many of these same disclosures in their

---

[17] 17 CFR 210.1-01 et seq.

[18] An issuer with a class of securities registered under Section 12 or subject to Section 15(d) of the Exchange Act is subject to the periodic and current reporting requirements of Section 13 and 15(d), respectively, of the Exchange Act.

[19] "Congress recognized that the ongoing dissemination of accurate information by companies about themselves and their securities is essential to effective operation of the trading markets. The Exchange Act rules require public companies to make periodic disclosures at annual and quarterly intervals, with other important information reported on a more current basis. The Exchange Act specifically provides for current disclosure to maintain the currency and adequacy of information disclosed by companies." Proposed Rule: Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date, Release No. 33-8106, 3-4 (Jun. 17, 2002) [67 FR 42914 (Jun. 25, 2002)].

[20] 17 CFR 249.310.

[21] See Part I, Items 1, 1A and 3 of Form 10-K; Part II, Items 7, 8 and 9A of Form 10-K; and Part III, Item 10 of Form 10-K [17 CFR 249.310].

[22] 17 CFR 308a.

[23] See Part I, Items 1 and 2 of Form 10-Q; Part II, Item 1A of Form 10-Q [17 CFR 249.308a].

periodic reports on Form 20-F.[24] Companies must provide timely and ongoing information in these periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations.

- Securities Act and Exchange Act Obligations: Securities Act and Exchange Act registration statements must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading. Companies should consider the adequacy of their cybersecurity-related disclosure, among other things, in the context of Sections 11, 12, and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act.[25]
- Current Reports: 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,[26] companies can provide current reports on Form 8-K[27] or Form 6-K.[28] Companies also frequently provide current reports on Form 8-K or Form 6-K to report the occurrence and consequences of cybersecurity incidents.[29] The Commission encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure

[24] See Part I, Items 3.D, 4, 5 and 8 of Form 20-F; Part II, Items 15 and 16G of Form 20-F; Part III, Items 17 and 18 of Form 20-F [17 CFR 249.220f].

[25] 15 U.S.C. 77k; 15 U.S.C. 77l; 15 U.S.C. 77q; 15 U.S.C 78j(b); 17 CFR 240.10b-5.

[26] See Item 11(a) of Form S-3 [17 CFR 239.13] and Item 5(a) of Form F-3 [17 CFR 239.33].

[27] 17 CFR 308.

[28] 17 CFR 249.306.

[29] "The registrant may, at its option, disclose under this Item 8.01 [of Form 8-K] any events, with respect to which information is not otherwise called for by this form, that the registrant deems of importance to security holders." 17 CFR 308.

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.[30]

In addition to the information expressly required by Commission regulation, a company is required 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."[31] The Commission considers omitted information to 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 the reasonable investor as having significantly altered the total mix of information available.[32]

In determining their disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, 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 materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any

[30] See Sections II.B.2 and II.B.3 below for further discussion of insider trading and Regulation FD.

[31] Rule 408 of the Securities Act [17 CFR 408]; Rule 12b-20 of the Exchange Act [17 CFR 240.12b-20]; and Rule 14a-9 of the Exchange Act [17 CFR 240.14a-9].

[32] This approach is consistent with the standard of materiality articulated by the U.S. Supreme Court in 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).

compromised information or the business and scope of company operations.[33] The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause.[34] 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.

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. We do not expect companies to publicly disclose specific, technical information about their 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, we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences. Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we 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

[33] For example, the compromised information might include personally identifiable information, trade secrets or other confidential business information, the materiality of which may depend on the nature of the company's business, as well as the scope of the compromised information.

[34] As part of a materiality analysis, a company should consider the indicated probability that an event will occur and the anticipated magnitude of the event in light of the totality of company activity. Basic v. Levinson, 485 U.S. 224, 238 (1988) (citing SEC v. Texas Gulf Sulphur Co., 401 F. 2d 833, 849 (2d Cir. 1968)). Moreover, no "single fact or occurrence" is determinative as to materiality, which requires an inherently fact-specific inquiry. Basic, 485 U.S. at 236.

were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk.[35]

Understanding that some material facts may be not available at the time of the initial disclosure, we recognize that a company may require time to discern the implications of a cybersecurity incident. We also recognize 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.

We remind 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[36] (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[37] (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.

---

[35] See Sections 7 and 10 of the Securities Act; Sections 10(b), 13(a) and 15(d) of the Exchange Act; and Rule 10b-5 under the Exchange Act [15 U.S.C 78j(b); 15 U.S.C. 78m(a); 15. U.S.C. 78o(d); 17 CFR 240.10b-5].

[36] See Backman v. Polaroid Corp., 910 F.2d 10, 16-17 (1st Cir. 1990) (en banc) (finding that the duty to correct applies "if a disclosure is in fact misleading when made, and the speaker thereafter learns of this.").

[37] See id. at 17 (describing the duty to update as potentially applying "if a prior disclosure 'becomes materially misleading in light of subsequent events'" (quoting Greenfield v. Heublein, Inc., 742 F.2d 751, 758 (3d Cir. 1984))). But see Higginbotham v. Baxter Intern., Inc., 495 F.3d 753, 760 (7th Cir. 2007) (rejecting duty to update before next quarterly report); Gallagher v. Abbott Laboratories, 269 F.3d 806, 808-11 (7th Cir. 2001) (explaining that securities laws do not require continuous disclosure).

We expect companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents. As the Commission has previously stated, we "emphasize a company-by-company approach [to disclosure] that allows relevant and material information to be disseminated to investors without boilerplate language or static requirements while preserving completeness and comparability of information across companies."[38] Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

2. 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.[39] 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.[40]

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;

[38] See Business and Financial Disclosure Required by Regulation S-K, Release No. 33-10064 (Apr. 13, 2016) [81 FR 23915 (Apr. 22, 2016)]. See also Plain English Disclosure, Release No. 33-7497 (Jan. 28, 1998) [63 FR 6370 (Feb. 6, 1998)]; and Updated Staff Legal Bulletin No. 7: Plain English Disclosure (Jun. 7, 1999) available at https://www.sec.gov/interps/legal/cfslb7a.htm.

[39] 17 CFR 229.503(c); 17 CFR 249.220f.

[40] See Final Rule: Business Combination Transactions, Release No. 33-6578 (Apr. 23, 1985) [50 FR 18990 (May 6, 1985)].

- 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.

3. MD&A of Financial Condition and Results of Operations

Item 303 of Regulation S-K and Item 5 of Form 20-F require a company to discuss its financial condition, changes in financial condition, and results of operations. These items require 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.[41] 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,

[41] 17 CFR 229.303; 17 CFR 249.220f.

and the loss of competitive advantage that may result.[42] Finally, the Commission expects companies to consider the impact of such incidents on each of their reportable segments.[43]

4. Description of Business

Item 101 of Regulation S-K and Item 4.B of Form 20-F require companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions.[44] 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.

5. 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.[45] 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.

---

[42] A number of past Commission releases provide general interpretive guidance on these disclosure requirements. See, e.g., 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 (Dec. 29, 2003)]; 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 (Jan. 25, 2002)]; Management's Discussion and Analysis of Financial Condition and Results of Operations; Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427 (May 24, 1989)].

[43] 17 CFR 229.303(a).

[44] 17 CFR 229.101; 17 CFR 249.220f.

[45] 17 CFR 229.103.

6. 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.[46]

7. 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.[47] The Commission has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to

[46] See Section 13(b)(2)(B) of the Exchange Act [15 U.S.C.78m(b)(2)(B)].

[47] 17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A.

investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company."[48] A company must include a description of how the board administers its risk oversight function.[49] To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk.

In addition, we believe 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.

B. Policies and Procedures

1. 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. We encourage 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

[48] Final Rule: Proxy Disclosure Enhancements, Release No. 33-9089 (Dec. 16, 2009) [74 FR 68334 (Dec. 23, 2009)], available at http://www.sec.gov/rules/final/2009/33-9089.pdf.

[49] See Item 407(h) of Regulation S-K.

other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.[50]

Pursuant to Exchange Act Rules 13a-15 and 15d-15, companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness.[51] These rules define "disclosure controls and procedures" as those controls and other procedures designed to ensure that information required to be disclosed by the company in the reports that it files or submits under the Exchange Act is (1) "recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms," and (2) "accumulated and communicated to the company's management … as appropriate to allow timely decisions regarding required disclosure."[52]

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.[53] Information also must be

---

[50] See Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm ("We believe that, to assist principal executive and financial officers in the discharge of their responsibilities in making the required certifications, as well as to discharge their responsibilities in providing accurate and complete information to security holders, it is necessary for companies to ensure that their internal communications and other procedures operate so that important information flows to the appropriate collection and disclosure points in a timely manner."); see also Section 10(b) of the Exchange Act and Rule 10b-5 thereunder [15 U.S.C. 78j(b); 17 CFR 240.10b-5].

[51] 17 CFR 240.13a-15; 17 CFR 240.15d-15.

[52] Id.

[53] See Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm ("We believe that the new rules will help to ensure that an issuer's systems grow and evolve with its business and are capable of producing Exchange Act reports that are timely, accurate and reliable.").

evaluated in the context of the disclosure requirement of Exchange Act Rule 12b-20.[54] 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.

Exchange Act Rules 13a-14 and 15d-14[55] require a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and procedures,[56] and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F require companies to disclose conclusions on the effectiveness of disclosure controls and procedures.[57] These certifications and disclosures 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.

---

[54] 17 CFR 240.12b-20.

[55] 17 CFR 240.13a-14; 17 CFR 240.15d-14.

[56] Section 302 of the Sarbanes-Oxley Act of 2002 required the Commission to adopt final rules under which the principal executive officer or officers and the principal financial officer or officers, or persons providing similar functions, of an issuer each must certify the information contained in the issuer's quarterly and annual reports. Pub. L. 107-204, 116 Stat. 745 (2002).

[57] 17 CFR 229.307; 17 CFR 249.220f.

2. 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.[58] 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."[59] 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.[60]

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.[61] We encourage companies to consider how their codes of ethics[62]

---

[58] In addition to promoting full and fair disclosure, the antifraud provisions of the federal securities laws prohibit insider trading, which harms not only individual investors but also the very foundations of our markets by undermining investor confidence in the integrity of those markets. 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

[59] Rule 10b5-1(a) of the Exchange Act [17 CFR 240.10b-5-1(a)].

[60] This would not preclude directors, officers, and other corporate insiders from relying on Exchange Act Rule 10b5-1 if all conditions of that rule are met.

[61] See e.g., NYSE Listed Company Manual Section 303A.10, which states in relevant part that every NYSE "listed company should proactively promote compliance with laws, rules and regulations, including insider trading laws.

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, we believe 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.

3. Regulation FD and Selective Disclosure

Companies also may have disclosure obligations under Regulation FD in connection with cybersecurity matters. Under Regulation FD, "when an issuer, or person acting on its behalf, discloses material nonpublic information to certain enumerated persons it must make public disclosure of that information."[63] The Commission adopted Regulation FD owing to concerns

---

Insider trading is both unethical and illegal, and should be dealt with decisively." See also NASDAQ Listing Rule 5610 and Section 406(c) of the Sarbanes-Oxley Act of 2002.

[62] Item 406 of Regulation S-K [17 CFR 229.406].

[63] 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

about companies making selective disclosure of material nonpublic information to certain persons before making full disclosure of that same information to the general public.[64]

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 to Regulation FD enumerated persons[65] before disclosing that same information to the public.[66] We expect companies to have policies and procedures to ensure that any disclosures of material nonpublic information related to

[64] Id.

[65] Regulation FD applies generally to selective disclosures made to persons outside the issuer who are (1) a broker or dealer or persons associated with a broker or dealer; (2) an investment advisor or persons associated with an investment advisor; (3) an investment company or persons affiliated with an investment company; or (4) a holder of the issuer's securities under circumstances in which it is reasonably foreseeable that the person will trade in the issuer's securities on the basis of the information. 17 CFR 243.100(b)(1).

[66] Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

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 as defined in the rule) or promptly (in the case of a non-intentional disclosure) and is otherwise compliant with the requirements of that regulation.[67]

By the Commission.

Dated: February 21, 2018

Brent J. Fields
Secretary

[67] "Under the regulation, the required public disclosure may be made by filing or furnishing a Form 8-K, or by another method or combination of methods that is reasonably designed to effect broad, non-exclusionary distribution of the information to the public." Id. at 3.