SEC Issues New Guidance on Cybersecurity Disclosure Requirements

On February 21, 2018, the U.S. Securities and Exchange Commission issued interpretive guidance (the Guidance) to assist public companies in drafting their cybersecurity disclosures in SEC filings. See 83 FR 8166 (Feb. 26, 2018). In his public statement accompanying the issuance of this guidance, SEC Chairman Jay Clayton said he believed that “providing the Commission’s views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors.”1 In this new guidance, the SEC is likely intending to signal how it may focus future enforcement concerning the cybersecurity disclosure obligations of public companies, and their underlying disclosure controls, procedures and certifications.

The new components to the SEC’s guidance that all public companies should take into account include the following:

- **Cyber Disclosure Controls and Procedures.** Notwithstanding the fact that there is no specific Regulation S-K line item with respect to cybersecurity, the SEC has made clear that a company’s disclosure controls and procedures, per Exchange Act Rule 13a-15, include controls and procedures to ensure that information about cybersecurity risks and incidents is processed and reported to the appropriate personnel to enable senior management to make disclosure decisions and certifications. Companies that support their CEO and CFO certifications regarding the effectiveness of disclosure controls and procedures with subcertifications by direct reports should consider how these subcertifications will need to be revised and expanded.

  - The Guidance specifies that these 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.

---

This focus on open communications between “technical experts” and disclosure advisors is new.

- **Policies to Prevent Insider Trading Based on Nonpublic Cyber Information.** The Guidance stresses the need for companies to consider implementing policies to prevent insider trading on the basis of any material nonpublic cybersecurity-related information. As a result, insider trading policies, codes of ethics and codes of conduct may need to be amended to expressly address information relating to cybersecurity risks and incidents. In addition, controls and procedures with respect to opening and closing trading windows may also need to be revised.

- **Improving Cyber Disclosures.** In general, the Guidance and the accompanying public statements make clear that the SEC and its Staff believe that current company disclosures about cybersecurity risks and incidents can be and must be improved.

The Guidance is the latest in a series of steps taken by the SEC and its Staff to make clear its increasing focus on cybersecurity matters; it both reinforces and expands upon the 2011 guidance issued by the Division of Corporation Finance regarding disclosure obligations relating to cybersecurity risks and incidents. Undeniably, the Guidance is intended to signal that the SEC and its Staff are raising the bar with respect to their expectations about the quality and usefulness of cybersecurity disclosure, and the compliance and governance framework with respect to how cybersecurity risks and incidents are handled. While a grace period can be expected with respect to the transition to the enhanced normative standards outlined in the Guidance—including comment letters on periodic filings by the Division of Corporation Finance—at some point, those expectations will begin to get enforced by the Division of Enforcement.

To be sure, the two Democrat Commissioners, in their separate public statements, qualified their support for the guidance, indicating that it “essentially reiterates years-old staff-level views on this issue” and is simply “rebranded guidance.” In Commissioner Jackson’s view, “much more needs to be done.” Commissioner Stein agreed: “There is so much more we can and should do.”

Regardless of the debate among the Commissioners, it is important for companies to consider the spirit and the letter of the Guidance when evaluating their approach to cybersecurity reporting and cybersecurity risk.

Set forth below in more detail is an overview of the Guidance.

**OVERVIEW OF RULES REQUIRING DISCLOSURE OF CYBERSECURITY ISSUES**

1. **Disclosure Obligations Generally; Materiality**

   Like the 2011 guidance, the Guidance emphasizes that companies “should consider” the materiality of cybersecurity risks and incidents when preparing required disclosures. 83 FR 8166, 8168 (Feb. 26, 2018). The SEC acknowledged that Regulation S-K does not specifically refer to cybersecurity but has interpreted it to include material cyber risks and incidents. In particular, the SEC states that cybersecurity-related disclosures should be considered in companies’ periodic reports, registration statements and current reports.

---


Further, the Guidance reinforces that the assessment of disclosure obligations is dependent upon a company’s particular circumstances, with thought given to the potential materiality of the identified risk, the importance of compromised information (if any), and/or the impact of an incident on a company’s operations, as applicable. *Id.* Materiality, in turn, is dependent upon, among other things, the nature, extent, and potential magnitude of a risk or incident (particularly in relation to compromised information, the business, or the scope of a company’s operations), as well as the range of harm (including, for instance, as related to a company’s reputation, financial performance, customer/vendor relationships, and/or the possibility of litigation or regulatory investigations or actions). *Id.* at 8168–69.

2. **Risk Factors**

Regulation S-K’s Item 503(c) and Form 20-F’s Item 3.D require companies to disclose the most significant factors that make securities investments speculative or risky. *Id.* at 8169–70. The Guidance suggests that companies consider the following factors when evaluating cybersecurity risks for disclosure:

- occurrence, frequency, and severity of prior cybersecurity incidents;
- probability and potential magnitude of cybersecurity incidents;
- adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs;
- aspects of the company’s business and operations that give rise to material cybersecurity risks (including industry-specific risks and third-party supplier/service provider risks);
- costs associated with maintaining cybersecurity protections (such as cyber insurance coverage or service provider payments);
- potential for reputational harm;
- existing or pending laws and regulations that may affect the cyber requirements and the associated costs to companies; and
- litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

The SEC suggests that companies may need to discuss past incidents to provide sufficient context and understanding of cyber risk. For example, the SEC suggests, if a company previously experienced a material denial-of-service attack, it likely would not be sufficient for the company to simply disclose a risk of a denial-of-service incident without mentioning the prior incident and its consequences.

3. **Content and Timing of Disclosures**

The SEC provides particular guidance on the content and timing of cyber disclosures. Regarding content, the SEC states that “companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.” *Id.* at 8169. Companies should disclose “cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences.” *Id.* This includes a “duty to correct” a prior disclosure determined to be untrue or misleading at the time it was made, and a “duty to update” a prior disclosure that becomes materially inaccurate after it is made. *Id.* At the same time, consistent with its 2011 guidance, the SEC cautioned that companies need not and should not provide “detailed disclosures that could compromise cybersecurity efforts” — for instance, by providing a “roadmap” to hackers. *Id.*
On timing, although the SEC recognizes the need for internal investigation and cooperation with law enforcement, the SEC makes clear that such “ongoing internal and external investigation — which often can be lengthy — would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.” *Id.* Thus, such disclosures should be timely and companies should provide them with expediency, though the SEC understands that it may take some time to discern the implications of a cybersecurity incident and that some material facts may not be available at the time of the initial disclosure.

4. **MD&A of Financial Condition and Results of Operations**

Regulation S-K’s Item 303 and Form 20-F’s Item 5 require companies to discuss their financial condition, changes in financial condition, and results of operations. *Id.* at 8170. The SEC recommends that companies consider:

- costs of ongoing cybersecurity efforts (including enhancements to existing efforts);
- costs and other consequences of cybersecurity incidents or of cybersecurity issues more generally, including, for instance, immediate costs of an incident, loss of intellectual property or competitive advantage, reputational harm, implementation of preventative measures, maintenance of insurance, litigation and regulatory response, remediation efforts, compliance with legislation, etc.; and
- risks of potential cybersecurity incidents.

5. **Description of Business**

According to the Guidance, in connection with Item 101 of Regulation S-K and Item 4.B of Form 20-F, a company “must provide appropriate disclosure” if cybersecurity incidents or risks materially affect its products, services, competitive conditions, or relationships with suppliers or customers. *Id.*

6. **Financial Statement Disclosures**

The Guidance notes that cybersecurity incidents and risks may affect a company’s financial statements. *Id.* For example, cybersecurity incidents may result in expenses related to investigation and breach remediation, loss of revenue, insurance premium increases, or diminished future cash flow. As a result, the SEC “expects” companies to design their financial reporting and control systems to provide reasonable assurance that information regarding the range and magnitude of such impacts would be incorporated into its financial statements in a timely manner.

7. **Legal Proceedings**

Regulation S-K’s Item 103 requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party. *Id.* The SEC underscores that this requirement includes any such proceedings that raise 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 disclose such litigation.

8. **Board Risk Oversight**

Regulation S-K’s Item 407(h) and Schedule 14A’s Item 7 require a company to disclose the extent of its board of directors’ risk oversight role, such as how the board administers its oversight function and the board’s leadership structure. *Id.* To the extent cybersecurity risks are material, the company should disclose the board’s oversight of cybersecurity risks. The SEC notes that disclosures regarding the company’s cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues permit investors to assess how the board is discharging its risk oversight responsibility.
POLICIES AND PROCEDURES

The Guidance also expands on two concepts: disclosure processes and protections against insider trading.

1. Disclosure Controls and Procedures

Exchange Act Rules 13a-15 and 15d-15 require companies to maintain disclosure controls and procedures and evaluate their effectiveness. Id. at 8171. The Guidance advises companies to assess whether their disclosure controls and procedures are effective to process and report information regarding cybersecurity risks and incidents, including up the corporate ladder, as appropriate “to enable senior management to make disclosure decisions and certifications” and facilitate insider trading prohibitions. Id. In particular, the Guidance indicates that companies should assess whether their controls and procedures enable them to:

- record, process, summarize, and report information related to cybersecurity risks and incidents required to be disclosed in filings;
- identify cybersecurity risks and incidents;
- assess and analyze the impact of cybersecurity risks and incidents 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
- ensure timely disclosures regarding such risks and incidents.

2. Insider Trading

The Guidance reminds companies that their directors, officers, and other corporate insiders should be mindful of complying with the laws related to insider trading in connection with material nonpublic information about cybersecurity risks and incidents, including as related to vulnerabilities and breaches. Id. at 8171–72.

The Guidance 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.” Id. Companies should have policies and procedures in place to prevent trading on the basis of all types of material nonpublic information, including as appropriate information relating to cybersecurity risks and incidents.

3. Regulation FD and Selective Disclosure

Companies should also be sensitive to cybersecurity in the context of evaluating disclosure obligations under Regulation FD and protecting against selective disclosure of material information. Id. at 8172. The Guidance provides that companies should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons before disclosing the same information to the public and outlines an expectation that company policies and procedures would contemplate this risk.
Sidley Privacy and Cybersecurity Practice

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes lawyers experienced in regulatory compliance, litigation, financial institutions, healthcare, EU regulation, IT licensing, marketing counsel, intellectual property and criminal issues. Sidley provides services in the following areas:

• Privacy and Consumer Protection Litigation, Enforcement and Regulatory Compliance
• Data Breach, Incident Response and Cybersecurity Advice, Response and Litigation
• Global Data Protection, International Data Transfer Solutions and Cross-Border Issues
• Corporate Data Protection, Compliance Programs and Information Governance Assessments
• FTC and State Attorney General Investigations of Unfair or Deceptive Acts and Practices
• Cloud Computing, Social Media, Online Advertising, Internet of Things, E-Commerce and Internet Issues
• EU, China, Japan, Singapore, Hong Kong and other International Data Protection and Compliance Counseling
• Gramm-Leach-Bliley and Financial Privacy
• HIPAA and Healthcare Privacy
• Communications Law and Data Protection
• Workplace Privacy and Employee Monitoring
• Website Policies, Online Trademarks and Domain Name Protection
• Records Retention, Electronic Discovery and Defensible Deletion
• Governmental Access and National Security

Sidley Corporate Governance and Executive Compensation Practice

Lawyers in Sidley’s Corporate Governance and Compliance practice regularly advise corporate management, boards of directors and board committees on a wide variety of corporate governance matters, including corporate responsibility, SEC disclosure, legal compliance, fiduciary duties, board oversight responsibilities and issues arising under Sarbanes-Oxley. Our advice relates to the procedural aspects as well as the legal consequences of corporate and securities transactions and other corporate actions, including takeover defenses, proxy contests, SEC filings and disclosure issues, stock option issues and general corporate law matters. Our broad client base allows us to provide advice regarding best practices and trends in such matters as directors’ and officers’ responsibilities, board and committee practices, disclosure controls and procedures, internal controls, executive compensation and other matters.
Sidley Securities & Derivatives Enforcement and Regulatory Practice

Sidley's Securities & Derivatives Enforcement and Regulatory group advises and defends clients in a wide range of securities-and derivatives-related matters. With more than 150 lawyers in 10 offices worldwide, we provide comprehensive regulatory, enforcement, and litigation solutions in matters involving the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), self-regulatory organizations (SROs), state attorneys general and state securities regulators. Our team is distinctive in that it combines the strength of nationally recognized enforcement lawyers with the skills of equally prominent counseling lawyers. We work collaboratively to provide our clients with informed, efficient and effective representation.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.