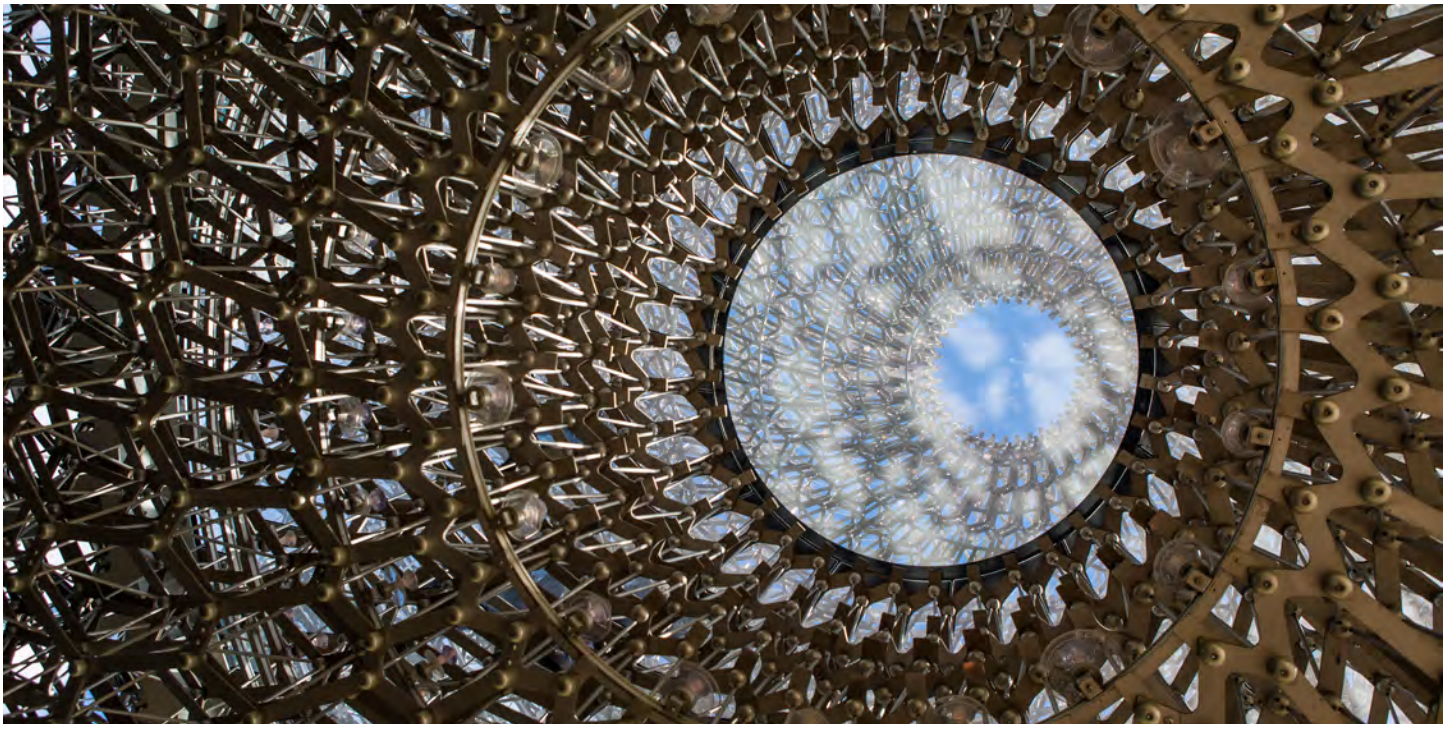
Deloitte.

Heads Up | Volume 25, Issue 2
February 23, 2018



In This Issue

"In today's environment, cybersecurity is critical to the operations of companies and our markets."

— SEC Chairman Jay Clayton

In the Spirit of Full Cybersecurity Disclosure

by Christine Mazor and Sandra Herrygers, Deloitte & Touche LLP

Background

On February 21, 2018, the SEC issued interpretive guidance (the "release")[1] in response to the pervasive increase in digital technology as well as the severity and frequency of cybersecurity threats and incidents. The release largely refreshes existing SEC staff guidance related to cybersecurity and, like that guidance, does not establish any new disclosure obligations but rather presents the SEC's views on how its existing rules should be interpreted in connection with cybersecurity threats and incidents.

The release will become effective on the date of its publication in the *Federal Register*. In a public statement about the release, SEC Chairman Jay Clayton noted that he has asked the Division of Corporation Finance to continue to closely monitor cybersecurity disclosures as part of its filing review process and that the SEC will continue to evaluate whether further guidance is needed. In light of the SEC's focus on cybersecurity matters, companies may want to revisit their disclosures and their disclosure controls and procedures (DCPs), including controls over the sales of securities by executives.

Cyberattacks can vary widely from company to company. They can include the theft of a company's (or its customers' or vendors') financial assets, intellectual property, or sensitive information, the disruption of a company's operations, or the targeting of entities that operate in industries responsible for critical infrastructure, such as the energy and public utility industries. Costs and consequences of a cybersecurity incident may include remediation expenses, lost revenues, litigation, increased insurance premiums, reputational damage, and erosion of shareholder value.

[1] SEC Interpretative Release No. 33-10459, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*.

In 2011, the SEC's Division of Corporation Finance issued principles-based guidance[2] that provided the SEC's views on cybersecurity disclosure obligations, including those related to risk factors, MD&A, and the financial statements. The release expands on the concepts discussed in that guidance and concentrates more heavily on cybersecurity policies and controls, most notably those related to cybersecurity escalation procedures and the application of insider trading prohibitions. It also addresses the importance of avoiding selective disclosure as well as considering the role of the board of directors in risk oversight.

The release applies to public operating companies, including foreign private issuers, but does not address the specific implications of cybersecurity for other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations.

Overview of the SEC's Guidance on Cybersecurity Disclosures and Procedures

The tables below provide an overview of the SEC's views on cybersecurity disclosure requirements and procedures under the federal securities laws as articulated in the release. They also note how the release affects the SEC staff guidance issued in 2011.

Disclosure Type	Guidance in the Release	Comparison With 2011 Guidance
General disclosure obligations	Provide timely, current, and tailored information regarding material cybersecurity risks and incidents in SEC filings, including current and periodic reports as well as registration statements. For example, if a company identifies a cybersecurity risk or incident that would be material to investors, it should disclose the appropriate information before any offer or sale of securities. A materiality[3] determination about cybersecurity risks and incidents depends on their nature, extent, and potential magnitude as well as on the harm that incidents could cause. The SEC notes that "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." Companies should consider whether they need to revisit or refresh their prior disclosure about incidents as investigations develop.	**Expanded**
Risk factors	Consider the following in determining risks to disclose in connection with cybersecurity and related incidents: • Aspects of the business that are subject to material cybersecurity risks. • Adequacy and costs of preventative and mitigating measures. • Frequency and severity of past incidents. • Probability and significance of future incidents. • Costs to protect or remediate (or both), including insurance (if applicable). • Potential for reputational harm. • Regulatory requirements and compliance costs. • Costs of litigation, investigation, and remediation. It may not be sufficient for a company that had a previous material cybersecurity breach to disclose simply that there is a risk that a breach could occur. The company also may need to discuss the cybersecurity incident and its consequences to provide context for its cybersecurity risks.	**Consistent**

[2] CF Disclosure Guidance: Topic 2, "Cybersecurity."

[3] The release indicates that the SEC considers omitted information to be material as articulated by the U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976) if (1) "there is a substantial likelihood that a reasonable investor would consider the information important" in making an investment decision or (2) disclosure of the information "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."

(Table continued)

Disclosure Type	Guidance in the Release	Comparison With 2011 Guidance
MD&A	Discuss cybersecurity events, trends, or uncertainties that are reasonably likely to have a material effect on the company's results of operations, liquidity, or financial condition, including the potential impact on each reportable segment, if applicable. Consider the myriad costs associated with a cybersecurity event when evaluating the transparency of MD&A disclosures, including, but not limited to, the direct costs of the event, costs associated with implementing preventative measures, and the effect of any possible reputational damage.	**Consistent**
Description of business	Provide appropriate disclosure when any cybersecurity risks or incidents materially affect a company's products, services, relationships with customers or suppliers, or competitive environment.	**Consistent**
Legal proceedings	The requirement to disclose information related to material pending legal proceedings that involve the company or its subsidiaries also extends to litigation related to cybersecurity.	**Consistent**
Financial statement disclosures	A company's financial reporting and control systems should be designed to provide reasonable assurance that information about the range and magnitude of the financial effects of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available. Financial statement disclosures related to the impact of material cybersecurity incidents may include, but are not limited to, information about: • Material costs. • Possible impairment charges. • Revenue and customer incentives. • Warranty claims or obligations. • Contingencies and litigation accruals.	**Consistent**
Board risk oversight[4]	If cybersecurity risks are material to a company's business, the discussion of the board of directors' role in the risk oversight function should include the nature of its responsibilities for overseeing the management of this risk. The SEC believes that "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."	**New**

Connecting the Dots

The SEC acknowledged that it does not expect a company's disclosures to provide a level of detail that could compromise its cybersecurity efforts and that there may be limited information available in the early stages of a cybersecurity incident investigation. Nevertheless, the SEC emphasized that as information becomes available, registrants are responsible for disclosing appropriate information to keep investors informed and must balance the need for timely disclosure with the level of detail they can provide about such incidents. While cooperation with law enforcement during an ongoing investigation of a material cybersecurity incident may be necessary and may affect the scope of disclosure, it would not alone provide a basis for omitting material disclosures.

[4] SEC Regulation S-K, Item 407, "Corporate Governance."

Policies and Procedures	Guidance in the Release	Comparison With 2011 Guidance
DCPs	DCPs should address the identification and escalation of a cybersecurity incident to the appropriate levels within an organization, which would include ensuring that all relevant parties, including a company's IT and business functions, are involved in assessing the potential effect of the breach and related disclosure requirements. The release significantly expands the guidance on consideration of DCPs related to cybersecurity risks. The SEC emphasized that "[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws."	**Expanded**
Disclosures about DCPs[5]	The principal executive officer's and principal financial officer's certifications[6] and a company's disclosures regarding the design and effectiveness of DCPs should take into account the adequacy of controls and procedures for identifying and assessing the impact of cybersecurity risks and incidents. If cybersecurity risks or incidents give rise to deficiencies in DCPs, companies should take that into account when disclosing conclusions about the effectiveness of DCPs.	**Expanded**
Insider trading	Because cybersecurity risks or incidents can constitute material nonpublic information, companies should consider how their codes of ethics and insider trading policies address, prevent, and deter trading that is based on material nonpublic cybersecurity-related information. Companies should also consider whether and, if so, when to implement trading restrictions while assessing and investigating cybersecurity incidents.	**New**
Regulation FD[7] and selective disclosure	Companies should ensure that they do not violate Regulation FD by selectively disclosing material, nonpublic information regarding cybersecurity risks or incidents. They should consider the appropriate policies and procedures to ensure that cybersecurity incidents are not selectively disclosed.	**New**

Other Resources

As calls for greater transparency related to cybersecurity risks have increased, resources such as the following have been developed to help companies both assess their approach to such risk and consider related disclosures:

- In 2017, the AICPA issued a new cybersecurity risk management attestation reporting framework that is intended to help organizations evaluate and report on their cybersecurity risk management program.
- Deloitte's publication, *The Value of Visibility: Cybersecurity Risk Management Examination*, discusses the AICPA framework and a readiness assessment approach to help organizations prepare their response to the current threat environment.
- Deloitte's publication, *Changing the Game on Cyber Risk: The Imperative to Be Secure, Vigilant, and Resilient*, addresses how organizations can reverse the growing gap between security investment and effectiveness.

[5] Required by Exchange Act Rules 13a-14 and 15d-14 and SEC Regulation S-K, Item 307, "Disclosure Controls and Procedures."
[6] Section 302 of the Sarbanes-Oxley Act of 2002 required the SEC 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.
[7] SEC Final Rule Release No. 33-7881, *Selective Disclosure and Insider Trading* (Regulation FD — Fair Disclosure).

Subscriptions

If you wish to receive *Heads Up* and other accounting publications issued by Deloitte's Accounting Services Department, please register at www.deloitte.com/us/accounting/subscriptions.

Dbriefs for Financial Executives

We invite you to participate in *Dbriefs*, Deloitte's webcast series that delivers practical strategies you need to stay on top of important issues. Gain access to valuable ideas and critical information from webcasts in the "Financial Executives" series on the following topics:

- Business strategy and tax.
- Controllership perspectives.
- Driving enterprise value.
- Financial reporting.
- Financial reporting for taxes.
- Governance, risk, and compliance.
- Tax accounting and provisions.
- Transactions and business events.

Dbriefs also provides a convenient and flexible way to earn CPE credit — right at your desk. Subscribe to *Dbriefs* to receive notifications about future webcasts at www.deloitte.com/us/dbriefs.

DART and US GAAP Plus

Put a wealth of information at your fingertips. The Deloitte Accounting Research Tool (DART) is a comprehensive online library of accounting and financial disclosure literature. It contains material from the FASB, EITF, AICPA, PCAOB, IASB, and SEC, in addition to Deloitte's own accounting manuals and other interpretive guidance and publications.

Updated every business day, DART has an intuitive design and navigation system that, together with its powerful search and personalization features, enable users to quickly locate information anytime, from any device and any browser. While much of the content on DART is available at no cost, subscribers have access to premium content, such as Deloitte's *FASB Accounting Standards Codification Manual*, and can also elect to receive *Technically Speaking*, a weekly publication that highlights recent additions to DART. For more information, or to sign up for a free 30-day trial of premium DART content, visit dart.deloitte.com.

In addition, be sure to visit US GAAP Plus, our free Web site that features accounting news, information, and publications with a U.S. GAAP focus. It contains articles on FASB activities and those of other U.S. and international standard setters and regulators, such as the PCAOB, AICPA, SEC, IASB, and IFRS Interpretations Committee. Check it out today!