Cooley

SEC Issues New Guidance on Cybersecurity Disclosure and Policies

March 15, 2018

In February, the SEC announced that it had adopted long-awaited new guidance on cybersecurity disclosure. While the new guidance builds on Corp Fin's 2011 guidance on this topic, it carries more weight because it bears the imprimatur of the Commission itself rather than its staff. The guidance itself is not a revelation: its significance is less in what it says than in the fact that the SEC felt compelled to issue it. The message is this – with the increasing importance of cybersecurity and the increasing incidence of cyber threats and breaches, companies need to review the adequacy of their disclosures regarding cybersecurity and consider how to augment their policies and procedures to ensure that information regarding cybersecurity risks and incidents is effectively communicated to management to allow timely decisions regarding required disclosure and compliance with insider trading policies.

The guidance highlights the pervasiveness of, and increasing reliance by companies on, digital technology to conduct their operations and engage with customers and others. That makes companies in all industries vulnerable to the threat of cybersecurity incidents, such as stolen access credentials, malware, ransomware, phishing, structured query language injection attacks and distributed denial-of-service attacks. Whether these incidents are a consequence of unintentional events or deliberate attacks, the SEC cautions that they represent a continuous risk to the capital markets and to companies, their customers and business partners, a risk that calls for more timely and transparent disclosure.

In a published statement, SEC Chair Jay Clayton expressed his view that the guidance "will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors." He encouraged "public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives." He also indicated that Corp Fin will be monitoring cybersecurity disclosures as part of the selective filing review process. Past experience teaches that we can expect to see new staff comments on cybersecurity disclosures (or the lack thereof) in the near future.

Procedures and policies

While the new guidance addresses disclosure obligations under existing laws and regulations (much like the 2011 guidance), the real focus is on cybersecurity policies and procedures, particularly with respect to disclosure controls and procedures and insider trading and selective disclosure prohibitions.

Disclosure controls and procedures

In the guidance, the SEC encourages companies to adopt, and regularly assess compliance with, comprehensive policies and procedures related to cybersecurity, particularly disclosure controls and procedures. "Disclosure controls and procedures" are controls and other procedures designed to ensure that information required to be disclosed in the reports that a company files under the Exchange Act is recorded, processed, summarized and reported within the time periods specified in the SEC's rules and forms and is accumulated and communicated to management to allow timely decisions regarding required disclosure. The guidance urges companies to assess whether their disclosure controls and procedures capture information about cybersecurity risks and

incidents and ensure that it is reported up the corporate ladder to enable senior management to make decisions about whether disclosure is required and whether other actions should be taken. According to the guidance, "[c]ontrols 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. The controls should also ensure that information is communicated to appropriate personnel to facilitate compliance with insider trading policies."

Given that CEO and CFO certifications required as part of periodic reporting address the effectiveness of disclosure controls, the certifying officers will need to take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents. Moreover, the guidance advises, "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 policies

Information regarding cybersecurity risks and incidents may be material nonpublic information, and insiders could violate the antifraud provisions or their own internal company codes of ethics and insider trading policies if they traded company securities on the basis of that information. The SEC advocates that companies put in place prophylactic policies designed to avoid even the appearance of improper trading during the period following an incident – when the company is investigating and determining the facts, consequences and materiality of an incident – and prior to the dissemination of disclosure. Accordingly, companies should be in the habit of analyzing when it would be appropriate to implement trading restrictions and consider imposing restrictions under their insider trading policies once it is known that a cyber incident has occurred that could be material.

Corporate communication policies

The SEC reminds companies that they may have disclosure obligations under Regulation FD in connection with cybersecurity matters. Regulation FD prohibits the selective disclosure of material nonpublic information to certain enumerated persons unless that information has been publicly disclosed within the meaning of Regulation FD. Accordingly, the SEC stated that it 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 timely made.

Observations and commentary

- Companies should review their disclosure controls and procedures to ensure that they appropriately address cybersecurity risks and incidents. In developing disclosure controls, companies should be sure to include appropriate escalation procedures for cyber incidents, both for purposes of evaluating the significance of the event and determining whether it is likely to develop into a material event that requires the imposition on insiders of trading restrictions. Boards may want to assign oversight of cybersecurity (including data privacy and protection) to an appropriate committee, often the audit committee or a risk committee.
- In addition, controls should require the input of both IT and business personnel. In previewing the expected guidance in a 2017 presentation, Corp Fin Director William Hinman advocated that, because it may be hard to determine the significance of attacks initially, IT and business personnel should promptly consider the impact of the event together, with an eye toward understanding the business implications.
- SEC Commissioner Kara Stein **expressed similar views** in a recent speech at Stanford. Why, she asked, in light of the general agreement on the importance of cybersecurity, were companies "not doing more to implement robust cybersecurity frameworks and to provide meaningful disclosures regarding the risks of data loss." One possible reason, however, could be that companies "tend to view cyberthreats as a technology problem instead of, more appropriately, a business risk." However, when

cybersecurity is viewed to be simply an "IT" problem, it is then "hoisted on the shoulders of a company's chief information officer. Too often, this has led to a failure to integrate cybersecurity into a firm's enterprise risk management framework. To be sure, some companies are focused on cyberthreats and recognize their potential economic threat. But companies need to do more than simply recognize the problem. They need to heed the calls of their shareholders and treat cyberthreats as a business risk."

- Companies should review their insider trading policies and Regulation FD or similar corporate communication policies to ensure that they address cyber incidents. Insider trading policies should contemplate appropriate trading holds and restrictions in the event a cyber incident has occurred that could be material.

Disclosure obligations

In general

With regard to disclosure, the SEC has continued Corp Fin's principles-based approach and has elected not to adopt more prescriptive new rules – so far at least. Much like the 2011 guidance, the new guidance explains that, although there are no disclosure requirements that specifically refer to cybersecurity risks and incidents, the obligation to disclose material cybersecurity risks and incidents could still arise in the context of many of the disclosure documents required of public companies, including registration statements and periodic and current reports.

In determining whether disclosure regarding cybersecurity risks and incidents is necessary, companies will need to assess the potential materiality of any identified risk and the impact of any incidents. But how is "materiality" assessed in the context of cybersecurity? The SEC notes that the *Basic v. Levinson* test, which involves weighing the probability of an event against the magnitude of its potential impact, is still a relevant part of the analysis. Thus, the materiality of cybersecurity risks or incidents may depend on the likelihood of an incident, the frequency of prior incidents, the impact on operations – particularly with regard to any compromised information, including personally identifiable information, trade secrets or other confidential business information – and the harm that could result, such as harm to reputation, financial performance and customer and vendor relationships. Also at issue are the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-US authorities.

The SEC advises companies to consider revisiting prior disclosures as they may have a "duty to update" (where disclosure becomes false as a result of subsequent developments) or a "duty to correct" (where prior disclosures are determined to have been untrue when made, including, the SEC observes, "if the company subsequently discovers contradictory information that existed at the time of the initial disclosure.")

Although companies are expected to disclose cybersecurity risks and incidents that are material to investors, the SEC makes clear that they are not expected to provide detailed roadmaps or specific technical information about potential system vulnerabilities that would compromise a company's security protections.

While the guidance recognizes that it may take time to investigate and understand the implications of an incident, the need for an investigation will not, by itself, let the company off the hook: "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.

Observations and commentary

- Companies may find some of the guidance here difficult to navigate: providing adequate non-generic disclosure about risk, protections or incidents that does not, at the same, increase the company's exposure or jeopardize cybersecurity efforts could turn out to be a tricky exercise. Similarly difficult may be finding the point at which the company has sufficient factual information about a breach to make disclosure that is timely. There is an inherent tension between the need to disclose promptly to satisfy

requirements to inform investors and the need to keep the matter confidential to allow the investigation to proceed without tipping off the malefactors and to gain a satisfactory understanding of the facts and implications of the incident. This tension requires that companies make a difficult judgment call in every case. That may explain why, although, according to **Audit Analytics**, there were 64 cyber breaches at public companies in 2017, only 24 breaches were disclosed in SEC filings, and the substance of those disclosures varied widely. Companies may want to look to **Chair Clayton's statement** regarding the hack of the SEC's own systems in August 2017. Whether the new guidance provides an impetus for companies to disclose these incidents more frequently remains to be seen.

- With regard to a duty to update, the federal securities laws do not impose on public companies a general affirmative duty to continuously disclose material information. However, that duty will arise as a result of a number of events or circumstances, such as any of the following:
  - to satisfy a company's SEC reporting requirements, such as under the Form 8-K triggering events;
  - to satisfy obligations under a listing agreement with an exchange;
  - when the company or its insiders are trading in the company's securities;
  - when the company learns that a prior statement it made was materially untrue or misleading at the time it was made;
  - when the company is making public disclosure or otherwise speaking publicly and the omission of material information could render that disclosure misleading; or
  - when rumors are in the marketplace that are attributable to the company (although the company is generally not required to respond to conjecture about the company except pursuant to stock exchange guidelines).

Risk factors

Companies should consider whether cybersecurity risks and incidents are among the company's most significant risks, taking into account prior incidents and the probability of occurrence and potential magnitude of future incidents. Among other things, a company's risk factors could appropriately address the adequacy and costs of preventative actions and protections (such as insurance), the possibility of theft of assets (such as intellectual property and personal information), the potential for reputational harm, disruption to operations and loss of revenue, legal and regulatory requirements and, with regard to any incidents, the costs associated with remediation, investigation and litigation.

One important point to consider in crafting risk factors is the need to provide context by including disclosure regarding prior material incidents. As emphasized in the guidance, "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."

As always, the SEC cautions companies to "avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors." Generic disclosure is an issue that applies to all disclosure, but seems to be especially problematic in connection with risk factors.

Observations and commentary

- According to **Audit Analytics**, over 90% of the Russell 3000 include risk factors regarding cybersecurity.
- At a meeting of the SEC's Investor Advisory Committee at the end of 2017, the Committee debated **a discussion draft regarding cybersecurity risk disclosure**. The draft advocated that, when it comes to disclosure of cybersecurity risk, public companies could and should be doing more: "Although under the current regulatory regime companies disclose certain risks or loss events associated with cybercrime, such disclosures often appear to be minimal and/or boilerplate, and do not provide investors with sufficient information on the company's ability to address cybersecurity concerns. The nature of the…past attacks is commonly described in terms so general investors have no ready way of assessing whether those attacks are likely to recur.

Given the gravity of risks associated with cyberattacks, investors have a right to know whether public companies are prioritizing cybersecurity and whether they have directors who can play an effective role in cyber-risk oversight." The draft advocated disclosing "specific, non-proprietary and non-sensitive information" about prior cyberattacks, including "summary information derived from root-causes analyses of how the attacks were or were not successful, to clarify the nature and significance of ongoing risks."

Other disclosure areas

The guidance also advises that companies consider whether cybersecurity or cyber incidents should be included as part of their discussions of MD&A, business, legal proceedings, financial statements and board risk oversight. For example, in MD&A, risks related to cybersecurity could represent an event, trend or uncertainty that is reasonably likely to have a material effect on results of operations, liquidity or financial condition. Likewise, a material cyber incident could cause reported financial information not to necessarily be indicative of future operating results or financial condition. In this analysis, factors to be considered include the cost of cybersecurity efforts and ongoing enhancements, the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents. Other factors may include the potential loss of intellectual property, the costs of insurance, costs related 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 could result from an incident. The impact on reportable segments should also be considered.

With regard to discussions of business operations, companies should consider disclosing incidents or risks that could materially affect their products, services, relationships with customers or suppliers or competitive conditions. That could include, for example, incidents that affect the viability of a new product or theft of customer information that might affect the company's reputation and competitive position.

Companies are required to disclose the extent of their boards' role in risk oversight, including how the board administers that function. If cybersecurity risks are material, the SEC believes that the board's role in oversight of that risk should be discussed, along with the company's cybersecurity risk management program and how the board engages with management on cybersecurity issues.

Observations and commentary

- While the guidance was adopted unanimously, some of the SEC Commissioners were not exactly enthused about it, viewing it as largely repetitive of the 2011 guidance – and hardly more compelling. The SEC will be looking at feedback about whether any further guidance or rulemaking is needed.
- Some of that feedback is already here – from two of the Commissioners. In a **published statement**, new Commissioner Robert Jackson expressed his reluctant support for the guidance, which, he said "essentially reiterates years-old staff-level views on this issue. But economists of all stripes agree that much more needs to be done." That includes the White House's own Council of Economic Advisers, which Jackson quoted at length: Companies may tend to underinvest in cybersecurity, the **Council's report** said, but regulators can provide investment incentives through, for example mandatory disclosure requirements. However, "the effectiveness of the SEC's 2011 Guidance is frequently questioned. There are concerns that companies underreport events due to alternative interpretations of the definition of 'materiality'…. There are also concerns that the disclosure requirements are too general and do not provide clear instructions on how much information to disclose, and that they therefore 'fail to resolve the information asymmetry at which the disclosure laws are aimed.'"

  Commissioner Kara Stein likewise "supported the Commission's guidance, but not without reservation." In her **statement,** she indicated that she was "disappointed with the Commission's limited action." While the guidance includes "valuable reminders," she said, the problem "is that many of these reminders were offered by the staff back in 2011. If our staff has already provided guidance regarding cyber-related disclosures, the question, then, is what we, as the Commission, should be doing to add value given seven additional years of insight and experience…. The more significant question is whether this rebranded guidance will

actually help companies provide investors with comprehensive, particularized, and meaningful disclosure about cybersecurity risks and incidents. I fear it will not…. That is why, as I have remarked before, it is imperative that the Commission do more. As we have heard from a variety of commenters since the 2011 staff guidance, guidance, alone, is plainly not enough. This makes it all the more confusing that the Commission more or less reissued that very guidance. Simply put, seven years since the staff guidance was released, despite dramatic increases in cyberattacks and their related costs, there have been almost imperceptible changes in companies' disclosures. This to me strongly suggests that guidance alone is inadequate." These critiques may suggest that the SEC is primed for further rulemaking if the new guidance does not bring improved results.

- According to a study from the NACD, only 19% of corporate directors agreed that their boards have "a high level of understanding" of cyber risks, and a survey from the Harvard Business Review found that only 8% of directors viewed cybersecurity as a "strategic threat." Nevertheless, notably absent from the guidance was a proposed recommendation from the SEC Investor Advisory Committee draft recommendations to require companies to provide disclosure about board cybersecurity expertise, using essentially a "comply or explain" approach. The recommendation would have required information on whether any director "has experience, education, or expertise in cybersecurity, and if not, why a company believes that such board-level resources are not necessary for the company to adequately manage cyber risks." Those advocating the disclosure viewed cybersecurity as analogous to financial statement audit risk in that it is a risk to which all companies are exposed; as a result, like financial expertise, board cyber expertise was appropriate. However, the recommendation was certainly contentious: one committee member viewed board expertise in cybersecurity as a bit like a "melting ice cube." Instead, he argued, the question should be whether adequate resources have been made available to the board. According to **Audit Analytics**, the number of directors of public companies with cybersecurity experience has grown from five in 2012 to more than 20 in 2016.

The SEC has not yet brought a formal enforcement proceeding for failure to make timely disclosure regarding cybersecurity risks and/or cyber incidents. Could an enforcement action be on the horizon? Although the SEC is "not looking to second-guess good faith disclosure decisions," according to the co-director of the SEC's Enforcement Division, she has also **previously warned** that enforcement actions are possible in the right circumstances. The new guidance just might be a warning shot.

If you have any questions about this alert, please contact one of your Cooley team members or one of the attorneys identified here.

Key Contacts

Luke Cadigan Boston	lcadigan@cooley.com +1 617 937 2480

Koji Fukumura San Diego	kfukumura@cooley.com +1 858 550 6008
Kenneth Guernsey San Francisco	kguernsey@cooley.com +1 415 693 2091
Chadwick Mills San Francisco	cmills@cooley.com +1 650 843 5654
Cydney Posner San Francisco	cposner@cooley.com +1 415 693 2132