protiviti®
Face the Future with Confidence

SEC Issues Interpretive Guidance on Public Company Cybersecurity Disclosures

February 26, 2018

On Wednesday, February 21, the U.S Securities and Exchange Commission (SEC) published interpretive guidance to assist public companies in preparing their disclosures about cybersecurity risks and incidents. In its guidance, the SEC provides its views about public companies' disclosure obligations under existing law with respect to cybersecurity matters, and also addresses the importance of cybersecurity policies and procedures and the application of disclosure controls and procedures, insider trading prohibitions, and Regulation FD and selective disclosure prohibitions in the context of cybersecurity.

In this Flash Report, we summarize the SEC's guidance and its impact on public organizations. The SEC's release can be found here.[1]

Background

As has been well-documented, cybersecurity is among the most critical risks that organizations need to address today. In its interpretive guidance, the SEC lays out the threat landscape and provides detailed examples of the cybersecurity issues organizations face, ranging from unintentional events to deliberate attacks by insiders or third parties, including cybercriminals, competitors, nation-states and so-called hacktivists. It also details the extensive negative consequences organizations can experience, including but not limited to remediation costs, cybersecurity protection costs, lost revenue, litigation and legal costs and risks, reputational damage and brand erosion. All of this is relevant to investors and a significant cyber breach can result in immediate drops in stock price and sustained loss of shareholder value.

As the SEC sums it up, "Cybersecurity risks pose grave threats to investors, our capital markets, and our country." Accordingly, given the frequency, magnitude and cost of cybersecurity incidents, the SEC views it as critical for public companies to take all required actions to inform investors of material cybersecurity risks and incidents in a timely fashion.

[1] "SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures" Press Release, February 21, 2018, SEC, www.sec.gov/news/press-release/2018-22.

It also issues a specific warning to public company directors, officers and other corporate insiders about trading in advance of any disclosures regarding cyber attacks or other incidents that prove to be material.

This is not the first guidance the SEC has provided with regard to cybersecurity. In October 2011, the SEC's Division of Corporation Finance issued guidance on an issuer's disclosures regarding cybersecurity risks and cyber incidents. This was not a rule, regulation or official statement of the SEC, though those organizations choosing to ignore advice from the staff of the Division of Corporation Finance and failing to assess and disclose material cybersecurity risks would do so at the risk of filing delays and other regulatory action as well as increased exposure to the plaintiff bar.

In its latest guidance, the SEC states that it believes it is necessary to provide further guidance and to reinforce and expand upon the SEC staff's 2011 disclosure guidance. This guidance is relevant not only to public companies, but also to organizations that are planning for or going through an initial public offering. While most private companies likely have cybersecurity defenses in place or are working toward appropriate security protocols, many likely lack the SEC-compliant reporting and disclosure rigor that will be required once they become public.

Overview of New Guidance

In addition to reinforcing the staff's cybersecurity disclosure guidance issued in 2011, the SEC's just-released guidance focuses on two new critical topics: the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents; and, for directors, officers and other company insiders, applicable insider trading prohibitions under the general antifraud provisions of federal securities laws, as well as the obligations of these individuals to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.

The SEC's guidance is summarized below.

Reports and Disclosures

The SEC stresses that companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements (e.g., Form S-1) as well as periodic (e.g., 10-Q, 10-K) and current reports (e.g., 8-K). The SEC makes clear that although these disclosure requirements do not specifically refer to cybersecurity risks and incidents, a number of the requirements impose an obligation to

disclose these risks and incidents depending on a company's particular circumstances. For example:

- **Periodic reports** – Companies must provide timely and ongoing information in periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations.
- **Securities Act[2] and Exchange Act[3] obligations** – 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.
- **Current reports** – The Commission encourages companies to continue to use Form 8-K (or Form 6-K as a foreign filer) to disclose material information promptly, including disclosure pertaining to cybersecurity matters. This practice reduces the risk of selective disclosure, as well as the risk that trading in their securities on the basis of material non-public information may occur.

In addition, with respect to information expressly required by regulation, the SEC notes that 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." The SEC has long considered 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.

Importantly, the SEC emphasizes that it is not suggesting a company should make detailed disclosures that could compromise its cybersecurity defenses or other efforts. The company would not need to 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, the SEC expects companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal or reputational consequences. Also of note, the company may allow itself time to work with law enforcement

[2] Refers to the Securities Act of 1933.
[3] Refers to the Securities Exchange Act of 1934.

and the scope of a disclosure could be affected by an investigation. However, an investigation itself would not be a basis for avoiding the issuance of a disclosure.

Finally, the SEC reminds companies of their fiduciary duty to correct any prior disclosure that is later determined to be untrue at the time it was issued, as well as their duty to update any disclosure that becomes materially inaccurate after it is made. Companies should consider whether they need to revisit or refresh previous disclosures, including during the process of investigating a cybersecurity incident.

Insider Trading Restrictions

The SEC notes that 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. If a company becomes aware of a cybersecurity incident or risk that would be material to its investors, it should make appropriate disclosures timely and sufficiently prior to the offer and sale of securities, and take steps to prevent directors and officers (and other corporate insiders who are aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk.

This particular guidance from the SEC is especially noteworthy, as it comes following well-publicized reports of executives at a number of companies selling stock after they became aware of a major cybersecurity incident but prior to the incident being reported publicly. The SEC clearly is making a statement that it is scrutinizing such practices closely, and companies and their executives better have a good explanation if they occur.

Cybersecurity Risk Factors

Companies are required to disclose the most significant risk factors that make investments in their securities speculative or risky. Under these requirements, companies should disclose the risks associated with cybersecurity and/or cybersecurity incidents if they would be considered relevant to such investments. This includes risks that arise in connection with any acquisition, during which time due diligence directed to the adequacy of security controls is especially critical.

Potential risk factors include but are not limited to the following:

- Occurrence of prior cybersecurity incidents, including their severity and frequency
- Probability of the occurrence and potential magnitude of cybersecurity incidents

- Adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs (note that an assertion as to "adequacy" likely would require an appropriate controls effectiveness assessment based on penetration testing and other assessment techniques as well as a SOC 2 report for service organizations)
- Aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks (e.g., industry-specific risks, third-party risks)
- Costs associated with maintaining cybersecurity protections (e.g., insurance coverage, payments to service providers)
- 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[4]
- Litigation, regulatory investigation and remediation costs associated with cybersecurity incidents

These factors should be considered and documented in the company's risk assessment. Of note, defining "materiality" is critical to the cybersecurity risk assessment process, which is often performed by IT personnel who may not have the same appreciation or understanding of materiality from a broader business perspective.

The SEC also notes that 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. To illustrate its intent, the SEC used an example of a company previously experiencing a material cybersecurity incident involving denial-of-service. In this instance, the SEC noted 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. This means that past incidents involving suppliers, customers, competitors and others may be relevant when crafting a risk factor disclosure to give the disclosure appropriate context in effectively communicating cybersecurity risks to investors.

[4] An example would be the General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, which will become the primary law regulating how companies protect EU citizens' personal data in the spring of 2018.

Management's Discussion & Analysis (MD&A) of Financial Conditions and Results of Operations

As part of their periodic MD&A, companies are obligated to consider in the analysis of their financial condition and operations the cost of ongoing cybersecurity efforts, the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other factors. These factors should be considered for each reportable segment of the company. Issuers also may need to consider other potential costs as noted in the SEC's guidance. Beyond the expected costs related to preventive measures, remediation of deficiencies and the fallout costs from an incident, the SEC points to other costs such as the loss of intellectual property, reputation and competitive advantage.

Companies need to think about this MD&A disclosure and not just view it as check-the-box using the examples provided in the SEC's guidance. For example, if there are significant costs from a loss of system availability or production, a potential loss of life due to cyber risk related to Internet of Things (IoT) technology (such as driverless cars or medical devices), or ransom payments for ransomware, these matters should also be considered.

Financial Statement Disclosures

Cybersecurity incidents and the risks that result therefrom may affect a company's financial statements. The SEC expects a company's financial reporting and control systems to be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident is incorporated into its financial statements on a timely basis.

Board Risk Oversight

An issuer is required to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure. To the extent cybersecurity risks are material to a company's business, the SEC believes this disclosure should include the nature of the board's role in overseeing the management of cybersecurity risks. The SEC states specifically 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 the board is discharging its risk oversight responsibility.

It will be interesting to observe how boards respond to this requirement in ways that investors will find meaningful. For example, will we see disclosure of the nature of the oversight process, extent of board expertise, use of external advisers, and/or formation of

technology or other committees? Alternatively, will we see more companies benchmarking their cybersecurity policies and procedures against a suitable framework? This disclosure and the investor community's reaction to it bears watching.

Disclosure Controls and Procedures

The SEC notes that cybersecurity risk management policies and procedures are key elements of enterprisewide risk management. Thus companies should adopt comprehensive policies and procedures related to cybersecurity and assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosures. 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, enabling senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers and other corporate insiders from trading on the basis of material, nonpublic information about cybersecurity risks and incidents. One key challenge for companies in this area is translating the highly technical aspects of cyber incidents into business terms so that meaningful materiality thresholds can be determined.

It may occur to observers who know the SEC and its rules well that the above guidance applies to any significant risk matter which materially affects an issuer's results of operations and financial position. It's significant that the SEC is making it crystal clear that the guidance applies to cybersecurity. Accordingly, companies are now on notice that they should consider whether the disclosure controls and procedures they design and evaluate will "appropriately record, process, summarize and report the information related to cybersecurity risks and incidents that is required to be disclosed in [SEC] filings." Specifically, 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 advisers, and make timely disclosures regarding such risks and incidents.

Regulation FD and Selective Disclosure

The SEC reminds companies that they may have disclosure obligations under Regulation FD in connection with cybersecurity matters. Companies and persons acting on their behalf should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons before disclosing that same information to the public. The commission expects companies to have policies and procedures to ensure

that any disclosures of material, nonpublic information related to cybersecurity risks and incidents are not made selectively, and that any Regulation FD required public disclosure is made simultaneously (in the case of an intentional disclosure 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.

A Call to Action

In this digital age, it is difficult to imagine any public company not exposed to cyber risk. Therefore, the SEC's new rule applies to virtually every company listed on U.S. exchanges; no industry is immune. Accordingly, as noted by the SEC Chairman, Jay Clayton, the Commission's new rule is intended to "promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors."

Our view is that this guidance is a wake-up call for issuers to evaluate the adequacy of their disclosure controls and procedures in terms of fulfilling their obligations under the securities laws to disclose cybersecurity risks and incidents. In addition, the commission has issued a warning – equivalent to a shot across the bow – for companies to ensure they've got their act together on sales of securities by their executives. The new rules have been issued in the wake of executives of high-profile companies selling company stock *after* the company became aware of a significant cyber incident, but *before* the incident was disclosed to the public. Now that the SEC has spelled it out clearly for all to see that this practice is unacceptable and will not be tolerated in the future, it is reasonable to presume that claims of ignorance or other excuses will likely be given short shrift.

The SEC rule's focus is on the disclosure obligations of a company when it "becomes aware of a cybersecurity incident or risk that would be material to its investors." Just exactly how an issuer becomes aware of such matters is not addressed specifically by the rule. However, the rule implies that an issuer's disclosure controls and procedures must be effective in ensuring that disclosures are sufficient in communicating all material information to investors. While counsel may be the ultimate authority as to what constitutes "sufficiency" under the securities laws, the SEC rule states that issuers should consider whether their disclosure 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." That requirement sets a standard against which issuers can measure the effectiveness of their disclosure controls and procedures.

Accordingly, we recommend management consider the following:

- **Conduct a periodic, robust cybersecurity risk assessment to proactively identify new and emerging cyber threats.** Such assessments should take into consideration the changing cyber threat landscape, the company's "crown jewels," the business outcomes management and the board seek to avoid, the nature of the industry and business model, and the issuer's visibility as a potential target. We believe these assessments are important because many companies have not performed companywide cyber risk assessments with a focus on business outcomes (as opposed to a narrower technical risk assessment).

- **Consider whether there is a sufficient basis for disclosures asserting the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs.** Note that as innovative IT transformation initiatives grow the organization's digital footprint constantly, they outpace the security protections companies have in place. This trend is continuous and without end.

- **Consider whether there is a sufficient basis for disclosures asserting the adequacy of cyber incident response processes.** Our experience is that detective and monitoring controls remain immature across most industries, resulting in continued failure to detect breaches in a timely manner. Accordingly, simulations of likely attack activity should be performed periodically to ensure defenses can detect a breach and respond timely. Our experience in performing such simulations also indicates that too often the companies authorizing the testing fail to detect our test activity.

- **Evaluate the effectiveness of the disclosure controls and procedures in place to provide investors the information they need to understand the issuer's cyber risks and incidents**. For example, the SEC indicates that such controls and procedures should enable management 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."

- **With respect to the disclosure committee, consider engaging the appropriate cybersecurity representatives.** For example, the CISO can serve as either a de facto member or an adviser.

The above recommendations apply to public companies and are not intended to be exhaustive. Issuers may want to consult with legal counsel in evaluating the adequacy of their disclosure controls and procedures as they relate to cybersecurity risks and incidents.

As noted earlier, while most private companies likely have cybersecurity defenses in place or are working toward appropriate security protocols, many likely lack the SEC-compliant reporting and disclosure rigor that will be required once they become public. Accordingly, these entities will need to design disclosure controls and procedures that meet these requirements as part of their public company readiness process.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®