

RADICAL NEW CYBER EXPOSURE- DISCLOSURE GUIDANCE FOR PUBLIC COMPANIES

For the Securities and Exchange Commission (SEC) to single out any one area of exposure for specific financial disclosure by public companies is rare, which makes the recent formal guidance from the SEC's Division of Corporation Finance, that public companies disclose cyber attacks,¹ significant - perhaps even a game changer for some public firms.

The SEC took this step in response to a request from several senators for guidelines to address the concern that it was hard for investors to assess security risks if companies failed to disclose data breaches in their public filings. "Intellectual property worth billions of dollars has been stolen by cyber criminals, and investors have been kept completely in the dark. This guidance changes everything." According to the senators, "It will allow the market to evaluate companies in part based on their ability to keep their networks secure."²

As noted in the guidance itself, our "federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision." We now know that this expressly includes information relating to cyber attacks.

WHO IS IMPACTED?

The guidance is for companies preparing the disclosures required for initial public offerings in registration statements under the Securities Act of 1933 and for public firms preparing periodic reports under the Securities Exchange Act of 1934. Those with existing shelf registration statements will need to determine if it is necessary to file a Form 6-K or Form 8-K to disclose the costs and other consequences of material cyber incidents.



WHAT SHOULD BE DISCLOSED?

The SEC's guidance includes an overview of five specific disclosure obligations that may require disclosure of cybersecurity risks and cyber incidents. These disclosures are:

1. Pre-attack Exposure Analysis
2. Cyber Incidents in One's MD&A
3. Exposure to the Firm in Description of Business
4. Legal Proceedings (where they exist)
5. Financial Statement Implication

1. PRE-ATTACK EXPOSURE ANALYSIS

These obligations start prior to any actual attack with disclosure of the *risk of a cyber incident* (if these issues are among the most



significant factors that would make an investment in the company speculative or risky) and the anticipated costs associated with these incidents.³

In determining whether risk factor disclosure is required, public companies must evaluate their cybersecurity risks, taking into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents (which may or may not have been previously disclosed). This evaluation should focus on the probability of cyber incidents occurring and their quantitative and qualitative magnitude, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption.

In this regard, public firms may also weigh the adequacy of their preventative actions taken to reduce cyber risks – in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Cybersecurity risk disclosure must adequately describe the nature of the material risks and specify how each risk affects the firm. Care should be taken here to avoid simply disclosing generic risk factors.⁴ Rather, depending on the particular facts and circumstances both relevant and material to the company, appropriate disclosures may include:

- The aspects of the firm’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences
- Where outsourced functions have material cybersecurity risks, descriptions of those functions and how the company addresses those risks
- Risks related to cyber incidents that may remain undetected for an extended period
- Descriptions of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including the costs and other consequences
- A description of relevant insurance coverage

Importantly, the guidance reiterates “that the federal securities laws do not require disclosure that itself would compromise a registrant’s cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.” But this may be a hard line to establish.

Public companies are required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant’s ability to record, process, summarize and report information that is required to be disclosed in Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.

EXAMPLE GIVEN: If it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a public company’s information systems, a company may conclude that its disclosure controls and procedures are ineffective.

2. CYBER INCIDENTS IN ONE'S MD&A

Under the new guidance, public companies should address cybersecurity risks and cyber incidents in the Management Discussion and Analysis (MD&A) section of their annual report **if** the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend or uncertainty that is reasonably likely to have a material effect on the firm's financial results, liquidity or financial condition.

EXAMPLE GIVEN: If material intellectual property is stolen in a cyber attack and the impact of the theft is likely to be material, then the property that was stolen and the effect of the attack on its results of operations, liquidity, and financial condition should be described. Similarly, if the attack would cause previously reported financial information to no longer be indicative of future operating results or financial condition – this should be mentioned. If it is reasonably likely that the attack will lead to reduced revenues, an increase in cybersecurity protection costs, including those related to litigation, the company should discuss these possible outcomes, including the amount and duration of the expected costs, if material. Alternatively, if the attack did not result in the loss of intellectual property, but prompted the firm to materially increase its cybersecurity protection expenditures, these increased expenditures should be noted.

3. EXPOSURE TO THE FIRM IN DESCRIPTION OF BUSINESS

If one or more cyber incidents materially affect the firm's products, services, relationships with customers or suppliers, or competitive conditions, these should be disclosed in the public company's "Description of Business." In determining whether to include disclosure, the impact on each of their reportable segments should be considered.

EXAMPLE GIVEN: If the company has a new product in development and learns of a cyber incident that could materially impair its future viability, the incident and the potential impact to the extent material should be discussed.

4. LEGAL PROCEEDINGS (WHERE THEY EXIST)

It should not surprise anyone that if there are material pending legal proceedings involving the firm or any of its subsidiaries involving a cyber incident, this information should be disclosed in the "Legal Proceedings" section of the public company's annual report.

EXAMPLE GIVEN: If a significant amount of customer information is stolen, resulting in material litigation, the registrant should disclose the name of the court in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.

5. FINANCIAL STATEMENT IMPLICATIONS

Cyber incidents may have a broad impact on a public company's financial statements, depending on the nature and severity of the potential or actual incident; where material, these must be disclosed

EXAMPLE GIVEN: Estimates of warranty liability, allowances for product returns, capitalized software costs, inventory, litigation, and deferred revenue.

To the extent a cyber incident is discovered after the balance sheet date but before the issuance of the firm's financial statements, companies should consider whether disclosure of a recognized or non-recognized subsequent event is necessary. If the incident constitutes a material non-recognized subsequent event, the financial statements should disclose the nature of the incident and an estimate of its financial effect, or a statement that such an estimate cannot be made.

CONCERNS

With annual report season almost upon us, the exposure analysis of cyber threats and the evaluation of the efficiency of the firm's compensating controls, as called for in the new guidance, puts this issue directly in the c-suite. The position that materiality should be viewed in the aggregate when it comes to incident disclosure means that more incidents are likely to be disclosed. There are multiple, potential impacts from these new disclosures alone, from an enhanced litigation exposure to heightened insurance underwriting scrutiny with possible challenges for companies that disclosed less in their insurance application than appears in their SEC disclosure.

One benefit of the regulation may be an enterprise approach to cyber security and better communication internally about the exposures and controls. The insurance buying process could also be enhanced and for those currently purchasing this insurance, it may take on an additional value as a competitive advantage. For non-public companies, the question is whether the new guidance will raise the bar for how they consider and control the same exposures.

We are all only as good as our reputations, and only time will tell how these new disclosures may impact how others view our organizations.

CONTACTS

Please direct any questions or requests for additional information to your Willis Client Advocate® or ERPublications@willis.com.

For past issues of our publications on other topics of interest, please visit the [Executive Risks website](#).

Executive Risks Alerts and Newsletters provide a general overview and discussion on a wide range of topics. They are not intended, and should not be used, as a substitute for legal advice in any specific situation.

¹ <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

² http://newsandinsight.thomsonreuters.com/Legal/News/2011/10--_October/SEC_asks_companies_to_disclose_cyber_attacks/.

³ Consistent with Item 503(c) of Regulation S-K; and Form 20-F, Item 3.D.

⁴ Here the Commission notes that 503(c) of Regulation S-K already instructs registrants to “not present risks that could apply to any issuer or any offering” and further, to “[e]xplain how the risk affects the issuer or the securities being offered.”