GAAP
UPDATE SERVICE

Volume 18, Issue 8
April 30, 2018

INSIDE THIS ISSUE

SEC Disclosures – Cybersecurity Matters

Executive Summary

On February 21, 2018, the Securities and Exchange Commission (SEC) issued interpretive guidance to assist public companies prepare disclosures about their cybersecurity risks and incidents.

The views of the Commission included in this interpretive release reinforce and expand on guidance from the SEC staff published in 2011.

In addition to disclosures in risk factors, MD&A, and the financial statements, the guidance covers disclosure controls and procedures, insider trading, Board oversight, and the selective disclosure prohibitions under Regulation FD, all in the context of cybersecurity risks and incidents. The release is effective as of the date it is published in the Federal Register (February 26, 2018).

Although the SEC's release does not apply to private companies, the information may be useful in connection with preparing private placement offering documents and discussing business risks with a private company's Board members, lenders and shareholders.

Highlights

The SEC disclosure rules for public companies do not explicitly mention cybersecurity. However, in 2011, the SEC Staff published guidance explaining that public companies may be obligated to disclose both cybersecurity risks as well as

Wolters Kluwer

cybersecurity incidents. As a result of that guidance, many companies added cybersecurity disclosures, typically in the form of "risk factors."

The guidance in the February 2018 release, which was unanimously approved by the Commissioners of the SEC, reinforces and expands the prior guidance from the SEC Staff. The Commission's guidance is effective February 26, 2018.

The SEC expects public companies to disclose cybersecurity risks and incidents that are material to investors, including financial, legal, or reputational consequences.

> *"In today's environment, cybersecurity is critical to the operations of companies and our markets... Public companies must stay focused on these issues and take all required action to inform investors about material cybersecurity risks and incidents in a timely fashion."*
>
> *SEC Chairman Jay Clayton*

Key points made in the release include the following:

- *Timely Disclosure* – Companies that become aware of a material cybersecurity risk or incident should make appropriate disclosures in a timely manner. Providing investors with timely information regarding a cybersecurity matter on Form 8-K (Form 6-K for foreign registrants) not only maintains the accuracy and completeness of effective shelf registration requirements but also reduces the risk of selective disclosure of material nonpublic information (Regulation FD) and the risk of insider trading.

  While the SEC acknowledges that a company may need time to ascertain the implications of a cybersecurity event, companies should not necessarily wait until they have all the facts to disclose a cybersecurity incident. An internal or external investigation is not a sufficient basis for avoiding disclosures of a material cybersecurity incident.
- *Materiality* – Materiality of cybersecurity risks or incidents depends on the nature, extent and potential magnitude of those risks or incidents, as well as the range of harm that could be caused. This includes more than just financial harm: it includes harm to a company's reputation and its relationships with customers and vendors.
- *Nature of disclosures* – Disclosures should not be so detailed so as to provide a roadmap to potential hackers but neither should they be boilerplate. The information provided to investors should be tailored to the company's specific cybersecurity risks and incidents.
- *Risk factors* – In the context of risk factors, companies should disclose the risks associated with cybersecurity and cybersecurity incidents, including risks that arise in connection with acquisitions.
- *MD&A* – In crafting the disclosures for management's discussion and analysis (MD&A), companies should consider addressing the costs and risks related to cybersecurity, the costs of combating cyberattacks, and, following a cybersecurity incident, the various financial consequences including diminished future cash flows, impairments of intangible assets (e.g. intellectual property and customer relationship assets), indemnification obligations, increased financing costs and insurance premium increases.

- *Other disclosures* – Companies should not overlook the need for cybersecurity related disclosures in connection with the description of the company's business, legal proceedings, and financial statements. In proxy statements it may be appropriate to discuss the nature of the Board of Directors' role in overseeing the management of cybersecurity risk.
- *Insider trading* – In the event of a cybersecurity incident, companies should take steps to prevent directors, officers and other corporate insiders from trading in company securities until investors are appropriately informed.
- *Disclosure controls and procedures* – Companies should design their disclosure controls and procedures to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel in a timely fashion. This is important not only to enable senior management to make disclosure decisions and certifications, but also to facilitate polices that are designed to prohibit corporate insiders from trading on the basis of material nonpublic information.

Observation – Private Company Considerations

Private companies are not faced with the same investor reporting requirements as public companies, nor do they need to worry about insider trading issues. However, a private company can benefit from the SEC's discussions of (i) governance matters, such as the role of the Board of Directors in overseeing the management of cybersecurity risks, (ii) internal controls that address the prompt reporting of identified risks and incidents to top management, and (iii) the potential effect of cybersecurity incidents on financial statements.

Analysis

2011 SEC Staff Guidance

In 2011, the SEC Staff in the Division of Corporation Finance issued guidance[1] to assist companies in developing disclosures that the Staff believed would be responsive to the increasing risk of cybersecurity incidents.

> *"Traditional cyber risks, including computer viruses and phishing attacks, can target anyone. But it is important to understand the specific vulnerabilities a company faces in their industry and sector, and whether the company understands those vulnerabilities."*
>
> *Audit Analytics, Cybersecurity Disclosures in Risk Factors*

The SEC Staff's guidance discussed the nature of cybersecurity incidents and attacks and explained how federal securities laws apply to these risks and events. It also identified specific potential disclosure obligations that public companies would need to consider as they evaluated their exposure to material cybersecurity risks and attacks.

A summary of potential disclosure obligations discussed by the SEC Staff in its guidance follows:

- *Risk factors*[2]: Companies should disclose the risk of cybersecurity incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. In determining whether risk factor disclosure is required, companies should evaluate their specific cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. A company may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context.
- *MD&A*[3]: Companies should address cybersecurity risks and incidents 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 registrant's results of operations, liquidity or financial condition.
- *Description of business*[4]: Disclosure should be considered if one or more cyber incidents materially affect a company's products, services, relationships with customers or vendors, or the company's competitive conditions. Such disclosures may also be appropriate at the reportable segment level.
- *Legal proceedings*[5]: If a material pending legal proceeding involves a cyber incident, disclosure may be needed regarding this litigation.
- *Financial statements:* Depending on the circumstances, a company may need to consider the accounting requirements for losses from claims, including litigation, warranties, product recalls, product returns and indemnification obligations; impairments of goodwill, customer-related intangible assets, and capitalized software; customer incentives (to the extent the company offers customers special considerations in order to mitigate damages from a cyber incident); and subsequent events after the balance sheet date but prior to the issuance of the financial statements.
- *Disclosure controls and procedures*[6]: 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 SEC filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.

Observation – Risk Factor Disclosures

According to a report by Audit Analytics, over 88% of Russell 3000 companies disclosed cybersecurity as a risk in their 2015 SEC filings.[7] The report notes that in industries such as retail trade, hotels, and depository institutions, the disclosure rate was in excess of 97%. The disclosure rate for companies in the healthcare industry was over 92%.

In the retail and hotel industries, point-of-sale malware is a commonly mentioned risk. Depository institutions typically address data protection as well as protection against distributed denial-of-service attacks, i.e. attacks that are intended to disrupt online banking services. Companies in the healthcare industry are particularly sensitive to cybersecurity risk because they must comply with specific laws related to the privacy of patient data.

2018 SEC Release

The frequency, magnitude and cost of cybersecurity incidents and attacks led the Commission to conclude that companies needed further guidance to insure that investors are adequately informed about material cybersecurity risks and incidents in a timely fashion. This includes public companies that are subject to material cybersecurity risks even though they have not yet been the target of a cyber-attack.

> *"The cost of lost business [from a data breach] was particularly high for US organizations. This cost component includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill."*
>
> *Ponemon Institute, 2017 Cost of Data Breach Study: Global Overview*

On February 21, 2018, the Commission issued interpretive guidance to assist public companies with the disclosure requirements of federal securities laws related to both cybersecurity risks and cybersecurity incidents (the "2018 SEC Release".)[8]

The 2018 SEC Release reinforces and expands on the specific elements of the 2011 SEC Staff guidance outlined above. It also discusses several topics that were not explicitly addressed previously. Those incremental topics include the following:

- *Materiality:* Because securities laws do not require disclosure of immaterial matters, companies need to carefully evaluate whether a cybersecurity risk or incident rises to the level of "material." The release reminds public companies that the Commission "considers 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."[9]

  In making this assessment, management should consider the nature, extent and potential magnitude (particularly related to compromised information or the business and scope of the company's operations) of the risk or incident. It should also consider the range of harm that the risk or incident could cause.

  Typically, when dealing with questions of materiality, management focuses on quantitative effects, i.e. the "dollar" magnitude of harm. That includes the cost of investigating and remediating the problem, the cost of litigation or regulatory investigations, the cost of new systems or software, the potential for impairment of assets, the cost of fines or penalties, etc. The effect of cybersecurity risks and incidents on financial performance should certainly be considered when assessing materiality. But the 2018 SEC Release notes that the range of harm to be considered in this context should be broader. It should include harm to a company's reputation, its customer and vendor relationships, and the regulatory consequences that might result from the company's failure to have prevented the incident.
- *Cybersecurity policies and procedures:* The 2018 SEC Release notes that cybersecurity risk management policies and procedures are key elements of enterprise-wide risk manage-

ment. Companies should assess whether their disclosure controls and procedures are sufficient to insure that relevant information about cybersecurity risks and incidents is reported to the appropriate personnel so that senior management can make disclosure decisions and certifications. Disclosure controls should not be limited to the disclosures that are specifically required. Rather, the controls should insure timely collection and evaluation of information that is either potentially subject to required disclosure or relevant to an assessment of the need to disclose developments and risks that pertain to the company's business.

The discussion of disclosure controls and procedures in the 2018 SEC Release goes beyond the prior SEC Staff guidance that focused on the effect that cyber-attacks might have on a company's ability to record, process, summarize and report information required in SEC filings.

- *Board risk oversight:* The proxy rules require disclosure of the extent of the Board of Directors' role in the risk oversight of a company. To the extent that cybersecurity risks are material to a company's business, the Commission believes that the disclosure should address the nature of the Board's role in overseeing the management of that risk. This allows investors to assess how the Board is addressing its oversight responsibility in an area that is increasingly important to investors.
- *Insider trading prohibitions in the cybersecurity context:* Because information about a company's cybersecurity risks and incidents may be material nonpublic information, companies should have well designed policies and procedures to prevent trading on the basis of such information. The 2018 SEC Release encourages companies to consider how their codes of ethics and insider trading policies take nonpublic information about cybersecurity risks and incidents into account. Companies should also consider whether and when it may be appropriate to implement restrictions on insider trading in their securities in situations where the investigation and assessment of a significant cybersecurity incident is underway.

  Subsequent to the publication of the 2018 SEC Release, the SEC's Enforcement Division charged an Equifax business unit executive with insider trading related to his knowledge of a massive data breach at his employer prior to the company's public disclosure. According to the complaint, by selling before public disclosure of the data breach, the executive avoided more than $117,000 in losses.[10]
- *Selective disclosure:* Companies should insure compliance with Regulation FD by not selectively disclosing material, nonpublic information regarding cybersecurity risks and incidents to "Regulation FD enumerated persons" (e.g. brokers, dealers, investment advisors, investment companies) before that information is disclosed to the public.
- *Timeliness of disclosure:* The 2018 SEC Release acknowledges that time may be required to identify the implications of a cybersecurity attack or incident. Additionally, companies may not have some material facts at the time of the initial disclosure. However, the Commission explains that an ongoing internal or external investigation would not, on its own, provide a basis for avoiding disclosures of a material cybersecurity incident.

  A company may also need to correct its prior disclosures, either because it subsequently determines that something it initially disclosed is not true or because it initially omitted a material fact. Updates of prior disclosures may be required as well, particularly when there is an ongoing investigation that yields new information.

Because the 2018 SEC Release was effective February 26, 2018, public companies should immediately begin to incorporate the Commission's guidance into their SEC reporting processes and filings.

Observation – Costs of Cybersecurity Incidents

A 2017 study by the Ponemon Institute (sponsored by IBM Security) researched the direct and indirect costs of a data breach in a number of countries, including the US, based on data from over 400 companies that had incurred a material data breach.[11] Almost half of organizations represented in this research identified the root cause of the data breach as a malicious or criminal attack.

Examples of direct costs include forensic experts, outsourced hotline support, crisis management services, legal expenditures, free credit monitoring or identity protection subscriptions and discounts for future products or services. For purposes of the study, indirect costs include in-house investigations and the value of customer loss resulting from turnover or diminished customer acquisition rates.

Endnotes

1 Issued October 13, 2011, available at *https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.*

2 Regulation S-K, Item 503(c).

3 Regulation S-K, Item 303.

4 Regulation S-K, Item 101.

5 Regulation S-K, Item 103.

6 Regulation S-K, Item 307.

7 See Audit Analytics, *"Cybersecurity Disclosures in Risk Factors,"* (January 14, 2016), available at *https://www.auditanalytics.com/blog/cybersecurity-disclosures-in-risk-factors/*.

8 Securities and Exchange Commission Release Nos. 33-10459; 34-82746, *"Commission Statement and Guidance on Public Company Cybersecurity Disclosures"* dated February 26, 2018 (the "2018 SEC Release").

9 Refer to Section II.A.1. of the 2018 SEC Release.

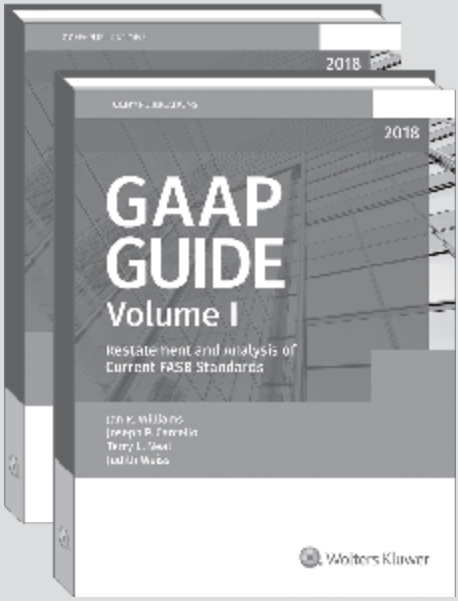
10 Refer to SEC Press Release dated March 14, 2018, *"Former Equifax Executive Charged with Insider Trading"* and related SEC Complaint at *https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf.*

11 See Ponemon Institute LLC, *2017 Cost of Data Breach Study: Global Overview* (June 2017), Benchmark research sponsored by IBM Security, available at *https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states.*

About the Author

This edition of the *GAAP Update Service* was authored by highly credentialed, seasoned CPAs at Financial Reporting Advisors, LLC. Located in Chicago, the firm provides accounting advisory, SEC reporting, litigation support and dispute resolution services. Resumes and more information can be found at www.FinRA.com.

GAAP Guide® (2018)



The most comprehensive resource for understanding and applying GAAP

This edition consistently follows the FASB Accounting Standards Codification® structure, includes practical illustrations, examples and observations and satisfies all AICPA peer review standards and requirements.

To order visit
CCHGroup.com/GAAP or call **800-344-3734**