SUMMARY OF 2018

SEC GUIDANCE

PUBLIC COMPANY CYBERSECURITY DISCLOSURES

This article provides a summary of the Securities and Exchange Commission's recent Statement and Guidance on Public Company Cybersecurity Disclosures [17 CFR Parts 229 and 249]

SUMMARY: The Securities and Exchange Commission recently released a statement on Public Company Cybersecurity Disclosures—providing guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

The release updates and reinforces prior 2011 Guidance by the SEC's Division of Corporation Finance, which provided an overview of specific SEC disclosure obligations that can require companies to consider cybersecurity risks and cyber incidents. Of note is that the SEC itself published the guidance, implying that the guidance carries some weight and should be studied in earnest. It also expands upon the 2011 Guidance by:

- Stressing the importance of comprehensive policies and procedures related to cybersecurity risks and incidents–in particular, as outlined in a company's disclosure controls and procedures
- Reminding Company directors, officers and corporate insiders of the laws and rules relating to insider trading and selective disclosure
- Expanding the existing disclosure guidance to address how the board of directors oversees cybersecurity risk, and management's discussion and analysis of cybersecurity risk and incident reporting
- Discussing the SEC rules and regulations, and SEC form requirements when preparing cybersecurity disclosures

Cybersecurity risks pose serious threats to investors, capital markets, and the country. Observably, the risk-concern is the dependency of the U.S. economy on effective cybersecurity and resiliency which are the life-blood of reliable information and communications technology, systems, and networks.

Financial services have become dependent on digital technology for access to markets, as have investors–both through the same or dependent digital information, communications and network infrastructure and systems. Investors and companies today rely on digital technology to conduct their business operations with customers, partners, vendors and other constituents to be relevant, be competitive, provide value, and continue to innovate. In a digitally connected world, cybersecurity presents ongoing risks and threats to capital markets and to companies operating in all industries–including public companies regulated by the Securities and Exchange Commission.

As companies' exposure to and reliance on networked systems and the Internet have increased, so have the associated risks and frequency of cybersecurity incidents. The concern is that as the interdependencies of networked infrastructures compounds, the risk associated with systemic failures from cyber-attacks, software vulnerabilities, natural disasters or other causes also increases–with the potential to affect society in unanticipated ways. Cybersecurity and resiliency is to data management, technology and infrastructure–what access to food and water are to the body and performance.

Given the frequency, magnitude and cost of cybersecurity incidents, the SEC has emphasized in its guidance that:

- It is critical public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion.

- Disclosure controls and procedures are crucial to a public company's ability to make required disclosure of cybersecurity risks and incidents in the appropriate timeframe.

- Disclosures must aptly discern the impact cyber risk and incidents have on the company's business, financial condition, and operating results, as well as the potential materiality of such risks and incidents.

  Note: the SEC guidance stresses the involvement of executive management and boards in the development and oversight of disclosure controls and procedures—and that a company's directors, and officers remain informed about cybersecurity risks and incidents that the company has faced or is likely to face.

- Directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company.

  Note: The guidance provides a reminder of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and of the obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.

Required Disclosures

Discussing the SEC rules and regulations and SEC form requirements when preparing cybersecurity disclosures requires a slightly deeper dive...

Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure required in registration statements under the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act"). The following are some example reporting scenarios and considerations raised by the recent SEC guidance:

Periodic Reports

Companies are required to file periodic reports to disclose specified information on a regular and ongoing basis. The periodic reports include annual reports on Form 10-K, which requires companies to make disclosures regarding their business and operations, risk factors, legal proceedings, management's

discussion and analysis of financial condition and results of operations ("MD&A"), financial statements, disclosure controls and procedures, and corporate governance. Periodic reports also include quarterly reports on Form 10-Q, which requires companies to make disclosures regarding their financial statements, MD&A, and updated risk factors. Likewise, foreign private issuers are required to make many of these same disclosures in their periodic reports on Form 20-F. The guidance points out that companies must provide timely and ongoing information in these periodic reports regarding material cybersecurity risks and incidents.

Securities Act and Exchange Act Obligations

Securities Act and Exchange Act registration statements require disclosure of all material facts necessary to make the statements not misleading. Note that this guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts–for example, by providing sensitive elements of the company's security protections. However, the SEC does expect companies to disclose cybersecurity risks and incidents that are material to investors, including the affiliated financial, legal, or reputational consequences.

The guidance highlights that 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. The SEC guidance encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters.

Tailored Disclosures

The SEC expects companies to provide disclosures that are tailored to their particular cybersecurity risks and incidents–a disclosure approach that allows relevant and material information to be disseminated to investors without boilerplate language while preserving completeness and comparability of information across companies. Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

Risk Factors

Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose the most significant factors that make investments in the company's securities speculative or risky. Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among such factors, including risks that arise in connection with acquisitions.

MD&A of Financial Condition and Results of Operations

Item 303 of Regulation S-K and Item 5 of Form 20-F require a company to discuss its financial condition, changes in financial condition, and results of operations. These items require a discussion of events, trends, or uncertainties that are reasonably likely to have a material effect on its operations, liquidity, or financial condition. In addition, companies may consider the array of costs associated with cybersecurity issues, including, but not limited to, loss of intellectual property, immediate costs of the incident, costs associated with implementing preventative measures, maintaining insurance, responding 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 may result. Finally, the SEC expects companies to consider the impact of such incidents on each of their reportable segments such as Description of Business and Legal Proceedings.

Financial Statement Disclosures

Cybersecurity incidents and the risks that result, may affect a company's financial statements. For example, cybersecurity incidents may result in:

- expenses related to investigation, breach notification, remediation and litigation, other professional services;
- loss of revenue, providing customers with incentives or a loss of customer relationship assets value;
- claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties, and insurance premium increases;
- diminished future cash flows, impairment of intellectual, intangible or other assets, recognition of liabilities, or increased financing costs.

The SEC expects a company's financial reporting and control systems to be designed to provide information on the range of the financial impacts from a cybersecurity incident in its financial statements as the information becomes available.

Board Risk Oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company 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. The SEC has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company." A company must include a description of how the board administers its risk oversight function. To the extent cybersecurity risks are material to a company's business, the SEC guidance instructs that this discussion should include the nature of the board's role in overseeing the management of that risk.

Note: The SEC believes disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues, allows investors to assess how a board of directors is discharging its risk oversight responsibility related to cybersecurity.

Disclosure Controls and Procedures

Cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including their relationship to compliance with federal securities laws. The SEC guidance encourages companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. Comprehensive policies and procedures related to cybersecurity should include:

- Procedures to ensure that information required to be disclosed by the company in filed or submitted reports under the Exchange Act are:
  - "recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms," and
  - "accumulated and communicated to the company's management… as appropriate to allow timely decisions regarding required disclosure."

- Policies and procedures to report the information related to cybersecurity risks and incidents that are required to be disclosed in filings. 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 advisors, and make timely disclosures regarding such risks and incidents.

Officer Certifications

Exchange Act Rules 13a-14 and 15d-14 require a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and procedures, and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F require companies to disclose conclusions on the effectiveness of disclosure controls and procedures. These certifications and disclosures should consider the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, 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.

This summary of the recent SEC Guidance on Public Company Cybersecurity Disclosures is probably best ended with the following quote …

"If you think compliance is expensive—try non-compliance."
–Former US Deputy Attorney Gerald Paul McNulty

The full Securities and Exchange Commission's Statement and Guidance on Public Company Cybersecurity Disclosures can be found at: https://www.sec.gov/rules/interp/2018/33-10459.pdf

We welcome your questions and comments and will directly reply or address your questions and comments in future articles. You can contact us at hello@ACGInfoSystems.com.

About the Author(s)

Jay Marqua is CIO of ACG Info Systems Cybersecurity and Information Systems Consulting Practice and Board Advisory Services Consulting Practice. Jay is based in ACGIS Info Systems' Durango, Colorado office. In his professional role supporting and serving Boards and Executive Leadership, Jay has led transformation efforts in the Healthcare, Energy, Financial, Communications, Technology, Software, Logistics, Hospitality and Travel Sectors. The pace and advantage to organizations of technology aligned with high performing teams has steered Jay to his concept, strategy and execution roles in the development of organizations globally. Jay can be reached at jay.marqua@acginfosystems.com

About ACG Info Systems, LLC

ACG Info Systems has developed an Active Cyber Governance Information System (ACGIS) to help organizations actively manage their cybersecurity and resiliency postures. The Active Cyber Governance Information System solution leverages the NIST CSF and US CERT CRR and provides the framework and functional capabilities to actively govern, manage and reduce complexity and risk. The ACGIS provides the functional governance capabilities to apply the principles and best practices of risk management to

improving the cybersecurity and cyber resilience of organizations. The application guides enterprises in matching IT resources to business mission and activities, and enforcing the principals of governance, awareness, security, resiliency, maturity, and accountability on the entire organization—including business unit leads and third-party vendors.