



PRIVACY UPDATE

New SEC Guidance on Cybersecurity Risk Disclosures Highlights the Elevated Importance of Information Governance and Data Security Compliance Programs

The Securities and Exchange Commission has issued significant new guidance suggesting that public companies should evaluate disclosure of cybersecurity risks more closely. The guidance was released on October 13 by the Securities and Exchange Commission's Division of Corporation Finance, which is responsible for review of public company filings.

This publication follows Senator Jay Rockefeller's recent request to SEC Chairman Mary Schapiro for issuance of such guidance, and Ms. Schapiro's June response to Senator Rockefeller.¹ In her response, the SEC Chairman indicated that more disclosure of cybersecurity risks could be appropriate. She stated that several existing regulations could require disclosure of *actual* cyber-attacks, but that *potential* cyber-attacks should also be disclosed in some circumstances.

The SEC staff defined cybersecurity as "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access." The staff stated that it was "mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security." It "emphasize[d] that disclosures of that nature are not required under the federal securities laws."

Cyber-attacks can include: gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, causing operational disruption, or causing denial-of-service attacks on websites. The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. The guidance recommends that companies engage in an ongoing review of the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.

The Division repeated the Chairman's statement that, while no existing SEC disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, existing disclosure requirements (including risk factors and management's discussion and analysis) may impose an obligation on public companies to disclose such risks and incidents.

¹ See "SEC Addresses Obligation to Disclose Cyber Threats, and May Consider Issuing Additional Guidance, available at <http://www.sidley.com/sidleyupdates/Detail.aspx?news=4844>.

SEC Guidance and Disclosure Considerations

The SEC staff believes that companies falling victim to successful cyber attacks may incur substantial costs and suffer other negative consequences, including:

- Remediation costs, which may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
- Increased cybersecurity protection costs, which may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence.

The SEC staff expects companies to evaluate their cybersecurity risks, taking into account the following:

- Prior cyber incidents;
- Severity and frequency of prior incidents;
- Cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Probability of cyber incidents occurring;
- Quantitative and qualitative magnitude of those risks;
- Potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data, or operational disruption;
- Adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security;
- Aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- Risks of outsourced functions, including a description of those functions and how the registrant addresses those risks;
- Risks related to cyber incidents that may remain undetected for an extended period;
- Relevant insurance coverage;
- Pending legal proceedings; and
- Conclusions regarding the effectiveness of disclosure controls and procedures.

The SEC's release provides guidance for discussion of cybersecurity in various places within a public company's disclosures, including the Risk Factors, MD&A, Description of Business, Legal Proceedings, Financial Statements, and Disclosure Controls and Procedures. Disclosure may be appropriate prior to any actual incident, as well as during and after an incident.

The SEC advises companies to avoid boilerplate disclosures regarding cybersecurity, and suggests that "Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure."

Information Governance Recommendations

The SEC's new guidance highlights the need for CEOs and Boards of Directors to implement and oversee company-wide information governance and data security compliance programs. Thus, as part of overall board oversight of risk management, CEOs should report regularly to the Boards on their companies' cybersecurity risk profile and corresponding internal information governance systems. Companies should consider some or all of the following steps²:

- Inclusion of cybersecurity in their risk factor disclosures, management discussion and analysis and other SEC filings;
- Development, approval, and implementation of a cybersecurity strategy under the direct supervision of a C-Level officer;
- Assessment of security for trade secret and IP systems in light of foreign and competitive threats;
- Evaluation of their "insider threat" risks, and adopt mitigation strategies to abate the damage that could be caused by Wikileaks-type situations;
- Implementation of enhanced employee training and awareness, which are critical to preventing, detecting, and abating the risks of cyberattacks;
- Preparation of contingency and response plans for inevitable cybersecurity incidents;
- Determination of what government resources are relevant and available to assist internal efforts, and execute a strategy for taking advantage of the government's help before intrusions occur;
- Review of their particular legal and contractual environments to determine if they are subject to any special cybersecurity reporting or safeguard requirements (*e.g.*, government contracts or other customer requirements); and
- Active monitoring of technological, industry, and public policy developments on cybersecurity risks and remedies.

The SEC guidance can be found at the following link: <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

If you have any questions regarding this update, please contact the Sidley lawyer with whom you usually work.

The Privacy, Data Security & Information Law Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers. Sidley provides services in the following areas:

- Privacy and Internet Litigation and Regulatory Advice
- Data Breach, Incident Response, and Cybercrime Advice
- Global Data Protection and Information Security
- International Data Transfer Solutions
- Outsourcing and Cross-Border Issues
- Gramm-Leach-Bliley and Financial Privacy
- HIPAA and Healthcare Privacy

² See "Cybersecurity—It's Not Just About 'National Security' Anymore: 'Directors Desk' and Other Incidents Sound Wake-Up Call for the Executive Suite and Board Room," available at <http://www.sidley.com/sidleyupdates/Detail.aspx?news=4747>.

- Workplace Privacy and Employee Monitoring
- Cyberlaw, E-Commerce, and Internet Issues
- Unfair Competition and Consumer Protection
- Trademark and Copyright Litigation and Counseling
- Website Policies and Domain Name Protection
- Records Retention and Electronic Discovery

To receive future copies of this and other Sidley updates via email, please sign up at www.sidley.com/subscribe

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

www.sidley.com

Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm's offices other than Chicago, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley or the firm.

SIDLEY AUSTIN LLP
SIDLEY