

## Cyber Attacks: New SEC Guidance on Cybersecurity Risk Disclosure Requirements

On October 13, 2011, the SEC's Division of Corporation Finance issued "CF Disclosure Guidance: Topic No.2, Cybersecurity," addressing disclosure obligations relating to cybersecurity risks and cyber incidents. Pursuant to the Securities Act of 1933 and the Securities Exchange Act of 1934, publicly-owned companies are required to provide timely, comprehensive and accurate information about risks and events that a reasonable investor would consider important to an investment decision. In light of the increased use of digital technologies in commerce and recent high-profile data breach and cybersecurity related events, the SEC decided to provide guidance regarding what, if any, disclosures should be provided about cybersecurity matters in light of a company's specific facts and circumstances.

### Negative Effects of Cyber Attack

The negative effects of a cyber attack were outlined by the SEC as:

- Remediation costs including liability for stolen assets or information, and repairing system damage. Remediation costs would include incentives offered to customers to maintain the business relationship after the attack.
- Increased cybersecurity protection costs including 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 attract customers following an attack.
- Litigation and reputational damage affecting customer or investor confidence.

### Cybersecurity Disclosures

Depending on a particular company's facts and circumstances, and to the extent such facts and circumstances were material, the SEC indicated that appropriate disclosures might include:

- Discussion of the company's business or operations that give rise to material cybersecurity risks and the potential costs and consequences.
- To the extent the company outsources functions that have material cybersecurity risks, descriptions of those functions and how the company addresses those risks.
- Description of cyber incidents experienced by the company that are individually or in the aggregate, material, including a description of the costs and consequences.

- Risks related to cyber incidents that may remain undetected for an extended period.
- Description of relevant insurance coverage.

The SEC indicated that disclosures should be made in the Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A) "...if 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 or would cause reported financial information not to be necessarily indicative of future operating results or financial condition."

Companies will also need to indicate in a Description of Business disclosure if "...one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions," or in the Legal Proceeding disclosure if a cyber incident is involved in a material pending legal proceeding to which a registrant or any of its subsidiaries is a party.

The SEC was mindful that the disclosure of such information might itself increase the risk that a company might provide a roadmap for those who seek to infiltrate a company's network security and target it for a cyber attack, and indicated that, "[w]hile registrants should provide disclosure tailored to their particular circumstances and avoid generic "boilerplate" disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity."

What Should a Company Do?

To comply with the regulation S-K Item 503(c) requirements for cybersecurity risk factor disclosures, companies will need to evaluate how their internal data security policies and procedures address the particular cybersecurity risks that they face. Companies will need to disclose material past cybersecurity incidents, future risks and any foreseeable consequences resulting from a cybersecurity breach. Recent EDGAR filings with the SEC illuminate how public companies have begun to make cybersecurity disclosures. Below is a short excerpt derived from the BNA Securities Regulation & Law Report of 10-K cybersecurity disclosures made by selected companies in various industries.

**Source:** *BNA Securities Regulation and Law Report*, Vol. 43, No. 41; Pg. 2081-2136, October 17, 2011<sup>1</sup>

Industry	Company	Disclosure
Business Services	Cintas Corp.  Form 10-K July 29, 2011	"We rely extensively on computer systems to process transactions, maintain information and manage our businesses. Disruptions in the availability of our computer systems could impact our ability to service our customers and adversely affect our sales and the results of operation."
Food	Winn-Dixie Stores Inc.  Form 10-K	"Disruptions or compromises in our information technology systems could adversely affect our business operations, our reputation with our customers and our results of operations."

	August 29, 2011	
Healthcare	Vanguard Health Systems Inc.  Form 10-K August 25, 2011	“Our facilities are subject to extensive federal and state laws and regulations relating to the privacy of individually identifiable information.”
Media and Advertising	Intellimax Media Inc.  Form 10-K June 28, 2011	“If the security measures that we use to protect their personal information, such as credit card numbers, are ineffective, our customers may lose their confidence in our websites and stop visiting them. This may result in a reduction in revenues and increase our operating expenses, which would prevent us from achieving profitability.”
Payroll and Data Processing	Paychex Inc.  Form 10-K August 24, 2011	“In the event of a catastrophe, our business continuity plan may fail, which could result in the loss of client data and adversely interrupt operations.”

If you have questions regarding this Alert, please contact the author, **Walter Delacruz** at 212.554.7668/[wdelacruz@mosessinger.com](mailto:wdelacruz@mosessinger.com).

<sup>1</sup> The accompanying chart was excerpted with permission from Securities Regulation & Law Report, 43 SRLR 2109 (Oct. 17, 2011). Copyright by The Bureau of National Affairs, Inc. (800-372-1033) <<http://www.bna.com>>

MOSES & SINGER LLP

Lawyers in the Internet/Technology group engage in landmark litigation, legislative efforts and innovative counseling and drafting that shape the law in this area. We also provide sophisticated corporate and transactional capabilities essential to the success of technology driven ventures. Entrepreneurs and emerging enterprises as well as more established companies expanding into e-commerce and online services benefit from the full range of integrated services offered by our Internet/Technology practice, which includes lawyers specializing in entertainment, advertising, merchandising, intellectual property, litigation, tax, wealth preservation and corporate law.

Since 1919, Moses & Singer has provided legal services to diverse businesses and to prominent individuals and their families. Among the firm's broad array of U.S. and international clients are leaders in banking and finance, entertainment, media, real estate, healthcare, advertising, and the hotel and hospitality industries. We provide cost-effective and result-focused legal services in the following primary areas:

- Accounting Law Practice
- International Trade

- Advertising
- Asset Protection
- Banking and Finance
- Business Reorganization, Bankruptcy and Creditors' Rights
- Corporate/M&A
- Employment and Labor
- Entertainment
- Global Outsourcing and Procurement
- Healthcare
- Hotel and Hospitality
- Income Tax
- Intellectual Property
- Internet/Technology
- Legal Ethics & Law Firm Practice
- Litigation
- Matrimonial and Family Law
- Privacy
- Private Funds
- Promotions
- Real Estate
- Securities and Capital Markets
- Securities Litigation
- Trusts and Estates
- White Collar Criminal Defense and Government Investigations

---

The Chrysler Building  
405 Lexington Avenue  
New York, NY 10174-1299  
Tel: 212.554.7800 Fax: 212.554.7700

2200 Fletcher Avenue  
Fort Lee, NJ 07024  
Tel: 201.363.1210 Fax: 201.363.9210  
Abraham Y. Skoff, Esq.  
Managing Attorney for New Jersey



Moses & Singer LLP is the New York City law firm member of the MSI Global Alliance (MSI). MSI is one of the world's leading international alliances of independent legal and accounting firms, with over 250 member firms in 100 countries - [www.msiglobal.org](http://www.msiglobal.org).

---

**Disclaimer**

Viewing this or contacting Moses & Singer LLP does not create an attorney-client relationship.

This is intended as a general comment on certain developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This contains information that may be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

**Attorney Advertising**

It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.

Copyright © 2011 Moses & Singer LLP  
All Rights Reserved