# SEC Issues Cyber Incident Disclosure Guidance

On October 13, 2011, the United States Securities and Exchange Commission released guidance from the Division of Corporation Finance (Division) addressing the appropriate disclosure of cybersecurity risks and cyber incidents. The guidance document applies existing SEC disclosure principles to rapidly proliferating cyber incidents and purports to provide guidance "consistent with the relevant disclosure considerations that arise in connection with any business risk." Despite this posture, the guidance suggests heightened scrutiny for such disclosures, and accordingly, reporting entities should carefully review their cybersecurity and cyber incident disclosure practices. The text of the Division's guidance is available here.

The Division said that, consistent with the general principle of "disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision," information related to cybersecurity and cyber incidents may be required as part of each of the following standard disclosures:

- **Risk Factors**. The Division said that in Risk Factor disclosure "registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky." Notably, the Division specifically included those risks arising from outsourcing and, when required for context, threatened cyber incidents.
- **MD&A**. As part of the MD&A, the Division said a registrant should address the costs and consequences of cybersecurity risks and cyber incidents, including potential incidents, when material.
- **Description of Business**. The Division said that in the Description of the Business section of its filings, a registrant should disclose cyber incidents materially affecting products, services, relationships, or competitive conditions on a reportable segment basis.
- **Legal Proceedings**. The Division said that in its "Legal Proceedings" disclosure, a registrant may need to disclose litigation involving a cyber incident.
- **Financial Statement Disclosures**. As part of financial statement disclosures, the Division said cyber incident disclosures may be required due to costs related to prevention and mitigation activities, possible loss contingencies, and impaired assets resulting from a cyber incident.
- **Disclosure Controls and Procedures**. The Division said that registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures and should consider the extent to which cyber incidents pose a risk to a registrant's disclosure controls and procedures.

The Division noted that it is concerned with the full panoply of consequences stemming from cyber incidents, including misappropriation of assets or sensitive information, corruption of data, operational disruption, remediation costs, increased security costs, lost revenues, litigation, and reputational damage.

If you have questions about this guidance or other aspects of cybersecurity or disclosure requirements, please contact the Ropes & Gray attorney who normally advises you.