U.S. Risk, LLC

CYBERSECURITY: SEC DISCLOSURE GUIDANCE

The Securities and Exchange Commission has adopted rules surrounding disclosures of material cybersecurity incidents. In addition, requirements for annual disclosures are now in place, as well as rules requiring foreign private insurers to make comparable disclosures.

DISCLOSURE PARAMETERS

Cyber incidents need to be disclosed if they are significant factors that might make an investment in the company speculative or risky. However, disclosure is not required to the detail that would comprise the organization's own cybersecurity. Risks and incidents that should be evaluated for inclusion are:

› Management's Discussion & Analysis of Financial Condition and Results of Operations (MD&A)

Include 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 or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.

Example: *Intellectual property is stolen in a cyber attack, and the effects of the theft are likely to be material. Include a description of the property that was stolen; the effect of the attack on operations, liquidity, and financial; and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition.*

› Description of Business

Include if one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions.

Example: *A new product is in development when the organization learns of a cyber incident that could materially impair its future viability.*

› Legal Proceeding

Include if a material pending legal proceeding to which a registrant or any of its subsidiaries is a party involves a cyber incident.

Example: *A significant amount of customer information is stolen, resulting in material litigation. Disclose the name of the court, date instituted, principal parties, description of the factual basis alleged, and the relief sought.*

› Financial Statement Disclosures

Include cybersecurity risks and cyber incidents, depending on the nature and severity of the potential or actual incident. These can include costs to prevent cyber incidents as well as costs relating to mitigating damages during and after a cyber incident.

Example: *Estimates that may be affected by cyber incidents include warranty liability, allowances for product returns, capitalized software costs, inventory, litigation, and deferred revenue.*

› Disclosure Controls and Procedures

Include if there are any risks in the ability to record, process, summarize and report information that is required for disclosure, or deficiencies in disclosure controls and procedures that would render them ineffective.

Example: *If it is reasonably possible that information would not be recorded properly due to a cyber incident affecting an information system, the conclusion would be that its disclosure controls and procedures are ineffective.*

NEW RULE HIGHLIGHTS

- Registrants must disclose on new Item 1.05 of Form 8-K material cybersecurity incidents.
- This disclosure must include the material aspects of the incident's nature, scope, and timing as well as its material impact or reasonably likely material impact on the registrant.
- This form will generally be due four days after the registrant deems a cybersecurity incident is material.
- Regulation S-K Item 106 has been added requiring registrants to describe their processes for assessing, identifying and managing material risks from cybersecurity threats.
- This includes a description of board of directors' oversight of risks and management's role and expertise in assessing and managing materials risks.
- 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023.
- Form 8-K and 6-K disclosures will be due beginning the later of 90 days after the publication in the Federal Register or December 18, 2023.
- Smaller reporting companies will have an additional 180 days for 8-K disclosures.

CYBERSECURITY: SEC DISCLOSURE GUIDANCE

› Risk Disclosure Inclusions

Risk disclosure must adequately describe the nature of the material risk as well as specify how each risk effects the registrant. It may also need to include:

- *Discussion of aspects of business or operations that give rise to material cybersecurity risks and the potential costs and consequences*
- *Description of any outsourced functions that may have cybersecurity risks and how these risks are being addressed*
- *Description of cyber incidents previously experienced including a description of the cost and other consequences*
- *Risks related to cyber incidents that may remain undetected for an extended period*
- *Description of relevant insurance coverage*

THE BOTTOM LINE

You can rely on us to be a trusted cyber and privacy expert and resource. Bringing us into the process as early as possible is important to help clients assess their exposure in this fast-changing arena and ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.