SEC issues interpretive guidance on cybersecurity disclosures

What happened?

On February 21, the SEC issued interpretive guidance to assist in the preparation of cybersecurity risks and incidents disclosures. This guidance reinforces and expands the guidance issued by the SEC staff in 2011.

The new guidance does not change any of the SEC’s rules. While it is generally consistent with the 2011 staff guidance, it addresses two additional topics:

- Disclosure Controls and Procedures: Companies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel to enable senior management to make disclosure decisions and certifications.

- Insider Trading: Policies and procedures should be in place to prevent trading on the basis of material non-public information. Companies should consider restrictions on trading while significant cyber incidents are investigated.

The interpretive guidance identifies sections of filings where the disclosure of cybersecurity matters may be appropriate and provides examples of the types of disclosure that should be considered, including the following:

- Risk factors: previous or ongoing incidents, probability of occurrence and potential magnitude, adequacy of preventative actions, and costs to maintain protections

- Description of business: how cybersecurity incidents or risks may materially affect a company’s products, services, relationships with customers or suppliers, or competitive conditions

- MD&A: the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents

- Legal proceedings: theft of customer information that results in material litigation

- Financial statement disclosures: the range and magnitude of the financial statement implications of a cybersecurity incident

- Board risk oversight: if cybersecurity risks are material to a company’s business, the nature of the board’s role in overseeing the management of that risk

Additional cybersecurity disclosures should be considered in periodic reports (e.g., Form 10-K, Form 10-Q, Form 20-F) and registration statements (e.g., Form S-1, Form S-3). The Commission encourages companies to use Form 8-K or Form 6-K to disclose material information pertaining to cybersecurity matters.
Why is this important?

Compliance with the interpretive guidance will ensure companies timely inform investors about the material cybersecurity risks and incidents that the company has faced or is likely to face. Most companies should expect to have increased disclosures in their SEC filings with respect to board risk oversight and cyber breaches, threats, and potential risks.

What's next?

Companies should assess their current cybersecurity risk management policies and procedures, and assess if they have sufficient disclosure controls and procedures in place to ensure relevant information about cybersecurity risks and incidents is processed and reported in their SEC filings. Companies should also consider whether they need to revisit or refresh previous disclosures, including during the process of investigating a cybersecurity incident, and consider filing a Current Report on Form 8-K relating to any material cybersecurity incident.

The new interpretive guidance is applicable to all public companies upon its publication in the Federal Register.

To have a deeper discussion, contact:

Wayne Carnall
Partner
Email: wayne.carnall@pwc.com

Brett Parrish
Partner
Email: brett.parrish@pwc.com

Tarynn Zenk
Senior Manager
Email: tarynn.zenk@pwc.com

Follow @CFOdirect on Twitter.