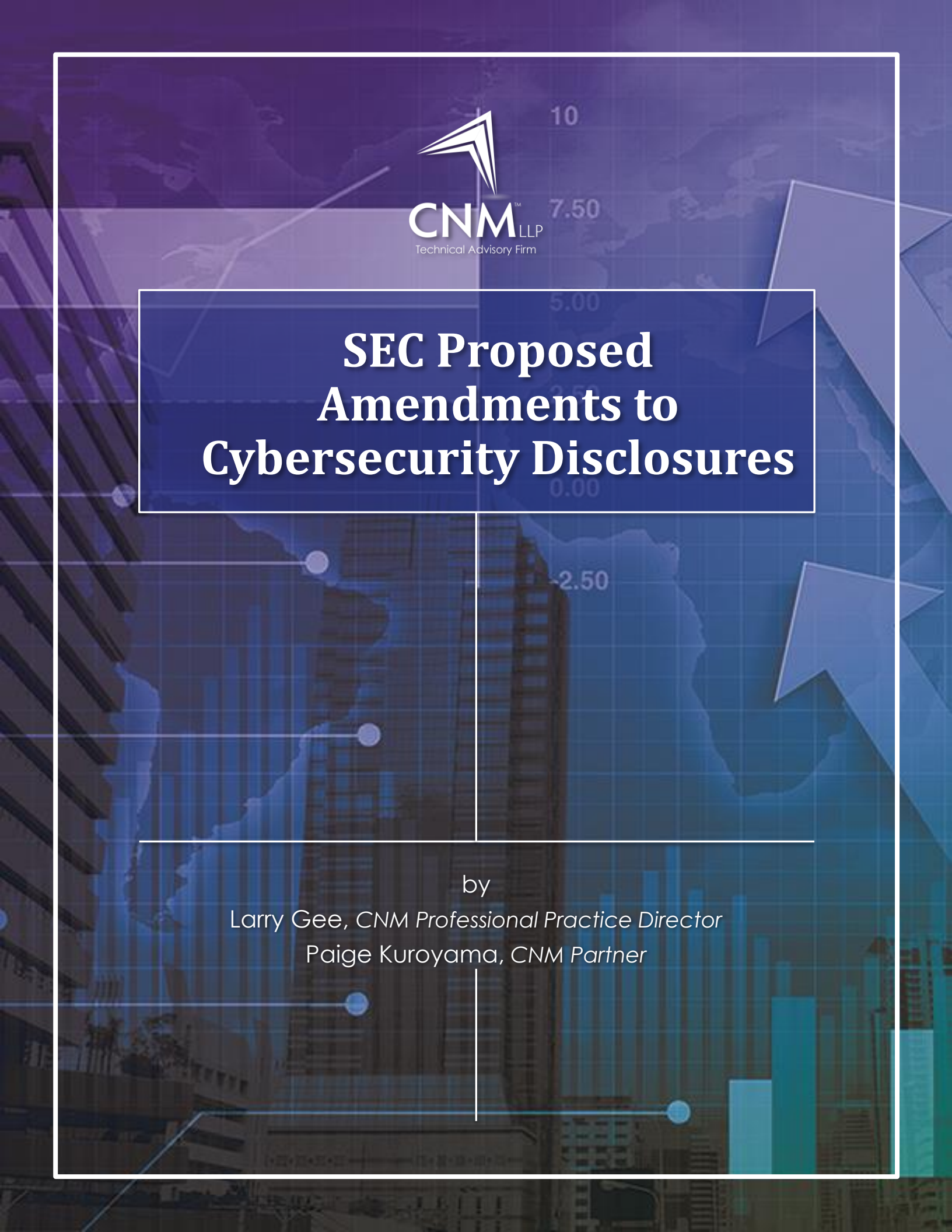

SEC Proposed Amendments to Cybersecurity Disclosures

by
Larry Gee, *CNM Professional Practice Director*
Paige Kuroyama, *CNM Partner*

SEC Proposed Amendments to Cybersecurity Disclosures

Overview

With the number of cybersecurity attacks and the level of sophistication of the attackers increasing rapidly, cybersecurity has become a major area of risk for all companies.

In response, on March 9th, the SEC proposed amendments to enhance and standardize disclosures by public companies related to cybersecurity. The amendments are designed to provide investors with better information about a registrant's cybersecurity risk management, strategy, governance, and exposure to cybersecurity incidents. (Proposed Rule)

The proposed amendments would require:

- Current reporting on Form 8-K about material cybersecurity incidents within four days of determining that the incident is material;
- Periodic disclosures regarding, among other things:
  - Updates about previously reported cybersecurity incidents
  - Cybersecurity risk management and strategy
  - Cybersecurity governance;
  - Board of directors' cybersecurity expertise
- Foreign private issuers to provide cybersecurity disclosures;
- Cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL).

Comments on the proposed amendments are due 30 days after posting in the Federal Register or May 9th, whichever is later. Based on that timeline, it is likely that the amendments will be finalized sometime this year.

Background

In 2011, the SEC Division of Corporation Finance issued interpretive guidance providing the Division's views concerning registrants' existing disclosure obligations relating to cybersecurity risks and incidents. In 2018, the SEC issued interpretive guidance to reinforce and expand upon the 2011 staff guidance. That guidance addressed the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the context of cybersecurity. Although disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved since then, the SEC believes that disclosure practices are inconsistent.

The proposed amendments are designed to better inform investors about a registrant's risk management, strategy, and governance, and to provide timely notification of material cybersecurity incidents. The SEC believes that consistent, comparable, and decision-useful disclosures would allow investors to evaluate registrants' exposure to cybersecurity risks and incidents, as well as their ability to manage and mitigate those risks and incidents.

In 2018, the SEC indicated that the test for materiality in the cybersecurity context is the same facts-and-circumstances analysis applicable in other contexts. Information is deemed material if there is a substantial likelihood that a reasonable investor would consider such information important in making an investment decision or a reasonable investor would view the information as significantly altering the total mix of information available. The SEC stated that materiality of cybersecurity risks and incidents will depend on their nature, extent, potential magnitude and range of harm that an incident could cause. While companies may need time to assess the implications of a cybersecurity event and the disclosure may be affected by ongoing investigations, those considerations do not provide a basis to avoid disclosure of a material cybersecurity incident.

SEC Proposed Amendments to Cybersecurity Disclosures

What Should You Do Now?

Registrants need to revisit their current cybersecurity policies and procedures to determine if they are sufficient to comply with the proposal. Now that registrants will disclose their cybersecurity polices and procedures, they will want to ensure that they meet the features that the SEC focuses on and are consistent with their peers. Boards should revisit their oversight roles and structures and assess whether the appropriate amount of time is spent addressing cybersecurity risks during meetings and if there are appropriate channels in place to provide for timely and effective communication. Having a cybersecurity expert on the board would be a premium and the board should assess whether it makes sense, given the registrants' cybersecurity risks, to prioritize candidates with cybersecurity experience.

www.cnmllp.com

Who is CNM?

Founded in 2003, CNM is recognized as one of the premier technical advisory firms in Southern California with Big 4 experience that provides the responsive customer service of a boutique firm. And we're a dynamic team that enlists all our energy to help transform the way your company does business – carefully evaluating your needs, simplifying your financial processes, and passionately solving problems in the most cost-effective way.

Our extensive knowledge of US GAAP, ICFR and SEC reporting skills has given us the ability to assist our clients with transactions that are not only multifaceted, but the capability to implement new or complex accounting standards. We have over 175 partners and employees in our Los Angeles, Orange County, San Diego, and New York City offices. Many of our clients are developed from direct referrals from the Big 4 accounting firms, speaking to the level of quality services we provide.

To learn more about how we can help, visit our website at www.cnmllp.com.

CNM™ LLP
Technical Advisory Firm

Los Angeles

A | 21051 Warner Center Lane
Suite 140
Woodland Hills, CA 91367
O | 818.999.9501

Orange County

A | 15635 Alton Parkway
Suite 450
Irvine, CA 92618
O | 949.299.5582

New York City

A | 264 West 40th Street
19th Floor
New York, NY 10018

San Diego

A | 11622 El Camino Real
Suite 100
San Diego, CA 92130