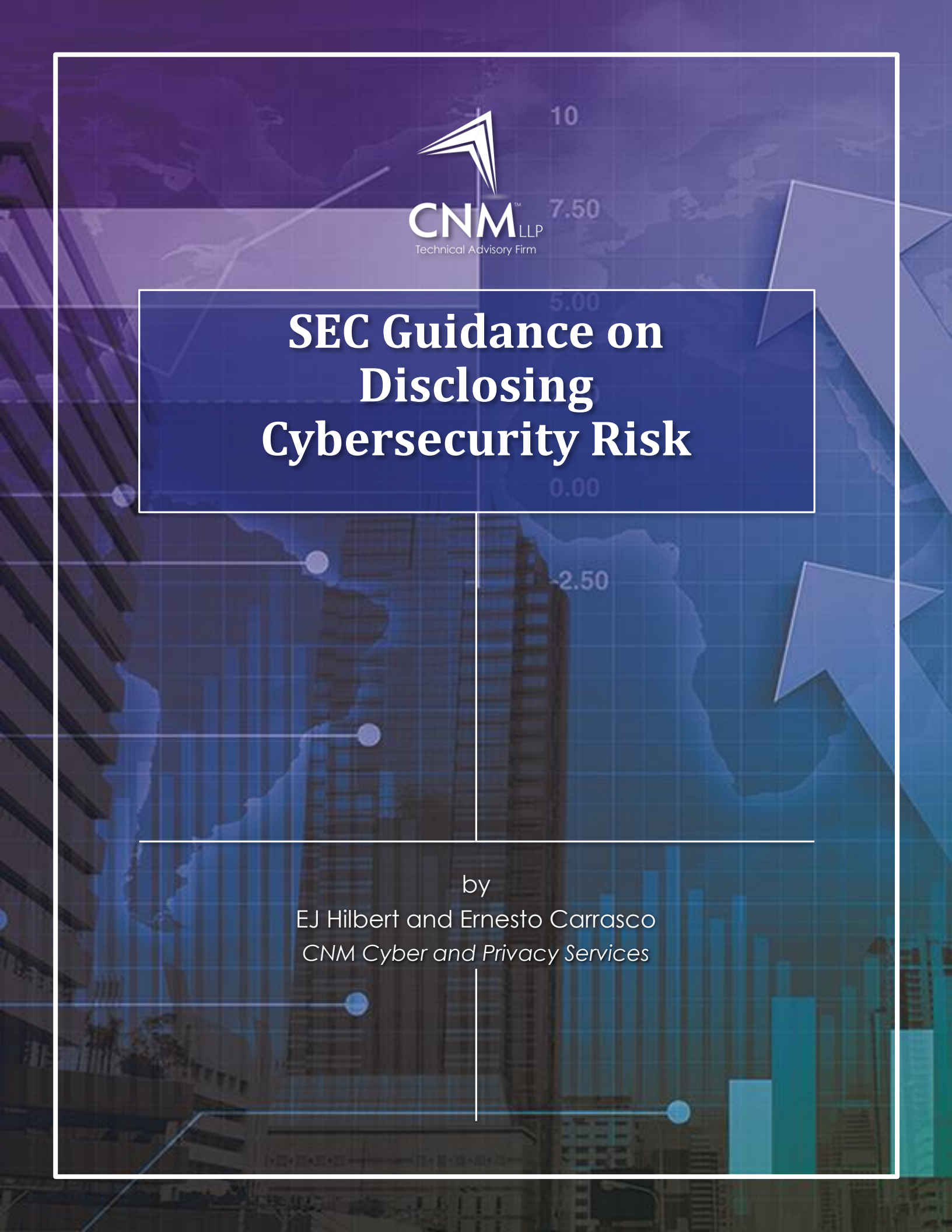


# SEC Guidance on Disclosing Cybersecurity Risk

by
EJ Hilbert and Ernesto Carrasco
*CNM Cyber and Privacy Services*

# "What does the SEC really expect?"

The SEC has recently published updated guidance for disclosing cybersecurity risk within a public company's periodic filings. The latest update details the SEC's views on the essential role a public company's board has on addressing insider trading, mitigating enterprise risk, and the timing of cyber-related disclosures. Based on this information, here are some actionable steps companies should consider.

## Step 1: Disclose Board Risk Oversight

Routinely, Boards of Directors have viewed cyber security as an IT issue, and thus not part of the board's purview. However, Boards are evolving, and this evolution is bringing "change" to how the board perceives their role and responsibilities for cybersecurity. A recent survey taken found 81% of directors believe their Boards' understanding of cyber risks has improved over the last two years[1]. Nearly 60% believe their Boards collectively know enough about the cyber threats to provide adequate oversight. However, only 50% of those directors surveyed reported they were "confident" their companies have protections for a cyber-attack[2]. The Commission believes the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents the company has suffered.

This guidance follows Senators Jack Reed (D-RI), Susan Collins (R-ME), and Mark Warner (D-VA) Cybersecurity Disclosure Act of 2017 (S 536), to promote transparency in the oversight of cybersecurity risks at publicly traded companies[3] and which has recently been re-introduced to Congress on February 28, 2019 as S. 592: Cybersecurity Disclosure Act of 2019[4]. The law, if approved, would require publicly traded companies to annually disclose to the SEC which member of its governing board has expertise or experience in cybersecurity and the details of such experience/expertise. (NIST will be responsible for defining acceptable "experience/expertise.") This bill currently being considered by the Committee on Banking, Housing, and Urban Affairs.

Considering these expectations and the potential regulatory actions, companies should consider taking the following actions:

- Add board members with cybersecurity expertise. Corporate board's members should represent a cross section of the corporation's business interests. As cyber security impacts all aspects of business, board members with expertise in this area are essential to continued business success.
- Develop a cybersecurity oversight committee to identify, manage, and mitigate risks related to cybersecurity, privacy, disaster recovery, incident management, and the protection of critical assets. Ideally, the committee should be composed of two or more Directors who understand emerging technologies and cyber-based risks. The committees' focus should include cyber-based risks and their potential impact on the business as a whole, as well as on various business units. The cybersecurity oversight committee should meet as frequently as necessary and report issues, recommendations, deliberations, and actions to the full Board on a regular basis.
- Establish a "risk-aware culture" from the top down. Senior Management commitment to be risk-aware and conspicuously promote policies and procedures that address and mitigate risks in line with the corporate risk appetite will resonate across the whole enterprise. Employees are more likely to follow the actions of management rather than management words.

[1] Cybersecurity Remains a Top Company Threat for Directors › Directors & Boards, www.directorsandboards.com/news/report-cybersecurity-remains-top-company-threat-directors.
[2] Cybersecurity Remains a Top Company Threat for Directors › Directors & Boards, www.directorsandboards.com/news/report-cybersecurity-remains-top-company-threat-directors
[3] GovTrack.us. (2019). S. 536 — 115th Congress: Cybersecurity Disclosure Act of 2017. Retrieved from https://www.govtrack.us/congress/bills/115/s536
[4] GovTrack.us. (2019). S. 592 — 116th Congress: Cybersecurity Disclosure Act of 2019. Retrieved from https://www.govtrack.us/congress/bills/116/s592


© 2018 CNM LLP.

# "What does the SEC really expect?"

- In addressing corporate security adopt a "Trust but verify" approach. When possible, seek subject matter professionals for independent and objective advice. Using the Internal Audit function in conjunction with an outside cybersecurity specialist, security controls should be tested and validated for effectiveness. Documenting these reviews assist in both educating the Board on discovered issues and protecting the Board when management of a cyber incident is publicly scrutinized. An objective review of cyber risk and security controls should be performed and reported to the Board on a periodic basis.

## Step 2: Improve Risk Management Practices to Meet SEC Requirements

The SEC updated guidance indicates they will place heavy emphasis on the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context[5]. The SEC has also emphasized that companies are expected to publicly disclose details of cyber incidents in a timely manner[6]. Unfortunately, the SEC has given little explanation of what cybersecurity controls are required or what details are required in the disclosures. Given the lack of detail and the different data environments, risks, and vulnerabilities faced by companies, this creates confusion about how affected companies are to comply.

To provide some clarity, companies should consider adopting a risk-based, data-centric approach. This approach focuses on an Integrated Risk Management (IRM) strategy that revolves around the business and the data companies have, where it resides, and how it's being processed, secured, and stored[7]. Managing and presenting the risks of the organization in a business context empowers non-technical business leaders to make more informed strategic decisions when cybersecurity incidents arise[8].

Summarized below are best practices that companies should consider when managing and reporting cybersecurity incidents:

- **Integrated Risk Management (IRM) -** Companies should adopt an Integrated Risk Management (IRM) Approach for Reporting Cybersecurity; IRM fosters a top-down, security-focused, and risk management-based culture throughout the organization, eliminating silos and enabling companies to identify situations where a risk factor in one area affects other areas. Moreover, the SEC 2018 guidance suggest Boards are expected to be involved in managing and discharging their oversite and governance responsibilities with respect to cybersecurity[9].
- **Conduct Regular Risk Assessments -** Given the constantly-changing threat landscape, regular IT risk assessments update risk information that can be consumed by the broader group, to enhance enterprise-wide security policies by tying IT risk to enterprise-wide risk management[10].

[5] Pg. 6 "Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures." SEC Emblem, 21 Feb. 2018, www.sec.gov/news/public-statement/statement-stein-2018-02-21.
[6] See Sections 7 and 10 of the Securities Act; Sections 10(b), 13(a) and 15(d) of the Exchange Act; and Rule 10b-5 under the Exchange Act [15 U.S.C 78j(b); 15 U.S.C. 78m(a); 15. U.S.C. 78o(d); 17 CFR 240.10b-5].
[7] GRC, Continuum. "5 Reasons Why Your Enterprise Should Put IRM Before GRC." 5 Reasons Why Your Enterprise Should Put IRM Before GRC -, 3 Jan. 2018, continuumgrc.com/irm-grc/.
[8] Bresnahan, Ethan. "Shift to Integrated Risk Management and a Risk-Based Lens." CyberSaint Security, www.cybersaint.io/blog/shift-to-integrated-risk-management-and-a-risk-based-lens.
[9] GRC, C. (2018, January 03). 5 Reasons Why Your Enterprise Should Put IRM Before GRC. Retrieved from https://continuumgrc.com/irm-grc/
[10] Bakkar, P., White, P., Irwin, R., Sobel, P. J., Prawitt, D. F., Murdock, D. C., . . . Chambers, R. F. (2018, October). COSO-WBCSD-ESGERM-Guidance-Full. Retrieved April 9, 2091, from https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf


© 2018 CNM LLP.

# "What does the SEC really expect?"

- **Develop Robust Policies and Procedures -** Companies are required to establish and maintain appropriate and effective risk identification, mitigation, and incident disclosure controls and procedures that enable them to make accurate and timely disclosures of material events.
- **Develop a strong Vendor Management program -** Companies need to consider their divisions as part of their third-party ecosystems. This includes understanding the effectiveness of key controls such as security awareness training to mitigate phishing attacks, as well as vulnerability management key organizational systems.
- **Regularly backup all data -** Maintaining backups (e.g., regular backups, storage, and testing of stored data) of critical data is imperative to managing the risks associated with viruses stealing your data and the potential of being a victim in the ransomware game. If the company regularly backs up their data, there is less of a concern the organization's important information will be lost. (Though data storage is relatively inexpensive, it may be improbable to back up all data from all company systems. Therefore, it is important to prioritize data backups by data criticality.)
- **Conduct Regular Employee Security Training -** A recent study showed that 80% - 90% of breaches are caused by employee carelessness[11]. Employees are our biggest security vulnerability. Most hackers break into companies' networks through social engineering schemes and phishing attacks that manipulate the users into sharing their credentials. Senior management most often targeted for these attacks. A well-defined and managed Security Awareness program that is mandatory for all employees enhances personnel security, increases compliance, and saves the organization time, money, and reputation.
- **Implement Multi-Factor Identification -** Multi-Factor authentication (MFA) is the use of a password plus a secondary piece of information to gain access to systems. In short, a user will enter a password which will trigger a request for a second data set, such as a code that has been texted to them, a code from a specialized mobile app/dongle, or biometric scan. The use of MFA significantly increases security because MFA codes are one-time, limited-use data sets that are difficult to capture or duplicate. The user's password is no longer the single point of failure.

[11] Almost 90% of Cyber Attacks are Caused by Human Error or Behavior. (2017, May 07). Retrieved from https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/


© 2018 CNM LLP.

# "What does the SEC really expect?"

## Step 3: Understanding "Materiality and Timeliness"

In its latest guidance, the SEC asks public companies to ensure that cyber risks and incidents are analyzed and "promptly" reported, even if some of the material facts may not be available at the time of disclosure[12]. Additionally, the SEC draft Strategic Plan explicitly reiterates the global reach of cybersecurity risk and the technological interdependency in both the U.S. and global securities markets[13]. The implementation of the EU General Data Protection Regulation (GDPR) as of May 25, 2018, significantly widens the scope of regulatory oversight of securities market participants and beyond. Under GDPR non-compliant companies could face a maximum fine of €20m or 4% of annual turnover, whichever is greater[14]. Using the recent Facebook hack in Europe as an example, Facebook who made $40 billion in 2017, could receive a penalty of up to $1.6 billion[15]. Or how about Google? Google was fined €50,000,000 from France's data regulator, citing a lack of transparency and consent in advertising personalization, including a pre-checked option to personalize ads[16]. More recently, Google was fined 1.5 billion euros for antitrust violations in the online advertising market[17]. Aside from media attention, shouldn't they be disclosing this information per SEC guidelines… sure, seems like they should.

In our view, the prompt disclosure of cyber risk serves as a defensive mechanism rather than portraying a negative view of the company's ability to manage cyber risk. Remember, "Bad news isn't wine – it doesn't get better with time". Companies that identify risks, own them, disclose them, and implement measures to manage them increases shareholders confidence. Yahoo, who ultimately agreed to a $35 million fine in April 2018 for not disclosing a massive breach in 2014[19], serves as a reminder of the SEC's focus on data security and the importance of cybersecurity preparedness.

So how do you meet the SEC's breach reporting guidelines? We believe that the general best practices identified above (Step 2), coupled with the following, will help companies describe at a high level the nature of the security breach, provide an estimate of the number of people affected, the categories of affected data, and the remediation efforts taken to prevent future incidents:

[12] "Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures." SEC Emblem, 21 Feb. 2018, www.sec.gov/news/public-statement/statement-stein-2018-02-21. "Under the regulation, the required public disclosure may be made by filing or furnishing a Form 8-K, or by another method or combination of methods that is reasonably designed to effect broad, non-exclusionary distribution of the information to the public." Id. at 3.
[13] Faitelson, Y. (2018, August 13). SEC's New Toughness On Breach Reporting And What It Means For Your IT Compliance. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/08/13/secs-new-toughness-on-breach-reporting-and-what-it-means-for-your-it-compliance/
[14] GDPR Key Changes. (n.d.). Retrieved from https://eugdpr.org/the-regulation/
[15] Schechner, S. (2018, September 30). Facebook Faces Potential $1.63 Billion Fine in Europe Over Data Breach. Retrieved from https://www.wsj.com/articles/facebook-faces-potential-1-63-billion-fine-in-europe-over-data-breach-1538330906
[16] Dillet, R., & Dillet, R. (2019, January 21). French data protection watchdog fines Google $57 million under the GDPR. Retrieved from https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/
[17] Vincent, J. (2019, March 20). Google hit with €1.5 billion antitrust fine by EU. Retrieved from https://www.theverge.com/2019/3/20/18270891/google-eu-antitrust-fine-adsense-advertising
[18] Colin Powell Quotes. (n.d.). Retrieved from https://www.brainyquote.com/quotes/colin_powell_137376
[19] SEC Fines Yahoo $35 Million for Failure to Timely Disclose a Cyber Breach. (2018, April 30). Retrieved from https://www.whitecase.com/publications/alert/sec-fines-yahoo-35-million-failure-timely-disclose-cyber-breach


© 2018 CNM LLP.

# "What does the SEC really expect?"

- Risk Factors: Companies should consider where cybersecurity risks and incidents rank in terms of the company's most significant risks, and should include disclosure regarding prior material incidents to the extent such disclosure provides context for the evaluation of cybersecurity risks and sensitive and regulated data, such as credit card numbers, Personal Identifiable Information (PII), and corporate IP exposed or used in an unauthorized way[20].
- MD&A: Companies should carefully consider whether cybersecurity-related risks could represent an event, trend, or uncertainty that has a material effect on results of operations, liquidity, or financial condition. For example, if material intellectual property is stolen in a cyber-attack, and the effects of the theft are reasonably likely to be material, the registrant should describe the property that was stolen and the effect of the attack on its results of operations, liquidity, and financial condition, and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition[21]. Alternatively, if the attack did not result in the loss of intellectual property, but it prompted the registrant to materially increase its cybersecurity protection expenditures, the registrant should note those increased expenditures[22].
- Timeliness: Lengthy ongoing internal or external investigation is not, on its own, an acceptable basis for avoiding disclosure of a material cybersecurity incident[23]. When an incident occurs, companies must have processes in-place to detect, alert, and report it quickly, to ensure that that the details reach the highest levels of the company[24].

## How CNM Can Assist Companies with Cybersecurity

Staying ahead of SEC guidance requires a long-term cyber risk mitigation strategy, and often requires third-party expertise to develop and deploy. As such, CNM operates under the precept that Privacy is Security, and is ready to help our clients in the following ways:

- **Security Awareness Education** – Develop and deploy a continuous training program that will common attacks and their mitigation, as well as the current regulatory security requirements
- **Privacy and Cyber Risk Assessments** – Identify risks and vulnerabilities via pen-testing and systems reviews within our client's enterprises, to showcase gaps and develop mitigation recommendations
- **Security Framework Strategy and Implementation** – Plan and enact a strategy to implement cybersecurity standards, such as ISO 27001 and NIST
- **Policies, Procedures and Governance Evaluation** – Review the current security policies and procedures against best practices, provide recommendation for enhancement, and create new policies as needed
- **Cloud Security Review** – Evaluate the cloud security posture and identify enhancements to the current posture

[20] As part of a materiality analysis, a company should consider the indicated probability that an event will occur and the anticipated magnitude of the event in light of the totality of company activity. Basic v. Levinson, 485 U.S. 224, 238 (1988) (citing SEC v. Texas Gulf Sulphur Co., 401 F. 2d 833, 849 (2d Cir. 1968)). Moreover, no "single fact or occurrence" is determinative as to materiality, which requires an inherently fact-specific inquiry. Basic, 485 U.S. at 236.

[21] Greene, T. (2012, February 03). FAQ About the VeriSign Data Breaches. Retrieved from https://www.csoonline.com/article/2130847/faq-about-the-verisign-data-breaches.html

[22] Cybersecurity. (2011, October 13). Retrieved from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[23] Pg. 12 "Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures." SEC Emblem, 21 Feb. 2018, www.sec.gov/news/public-statement/statement-stein-2018-02-21.

[24] See Sections 7 and 10 of the Securities Act; Sections 10(b), 13(a) and 15(d) of the Exchange Act; and Rule 10b-5 under the Exchange Act [15 U.S.C 78j(b); 15 U.S.C. 78m(a); 15. U.S.C. 78o(d); 17 CFR 240.10b-5]


© 2018 CNM LLP.

# “What does the SEC really expect?”

CNM’s experienced cybersecurity resources will help you balance security technology with your existing resources and sound governance.

For further information or to discuss your cybersecurity issues and needs please contact CNM’s Cyber and Privacy Services leaders, Managing Director E.J. Hilbert and Director Ernesto Carrasco at cyber@cnmllp.com.

## WHO WE ARE

CNM LLP is a technical advisory firm that provides high value, specialized accounting advisory services to a broad client base ranging from startups and mid-market companies to multi-national Fortune 500 companies. As an organization of professionals, our mission is to understand the business of our clients, to help our clients identify their business and financial needs, and to provide the services that will help them achieve their business goals. We are committed to providing the most effective services possible, efficiently and expeditiously, while always maintaining our ultimate focus on our clients' needs and objectives.


© 2018 CNM LLP.

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 | 6 Venture
Suite 365
Irvine, CA 92618
O | 949.299.5582

**New York City**

A | 300 Park Avenue
Suite 12007
New York, NY 10022



Restriction on Disclosure and Use of Information – This material contains confidential and proprietary information of CNM LLP, the unauthorized disclosure of which would provide a competitive advantage to others, as a result the recipient of this document shall not disclose, use, or duplicate this document, in whole or in part, for any purpose other than for the recipient's evaluation of CNM LLP's proposal.





© 2018 CNM LLP.