



# Corporate Controller & CAO Hot Topics

Cybersecurity Reporting -  
Navigating the New  
Requirements



**Emerging regulations mean that bolstering a company's cybersecurity reporting capabilities is no longer an option, but a requirement. Specifically, the new SEC rules regarding cybersecurity risk management, strategy, governance and incident disclosures are putting pressure on organizations to strengthen their cybersecurity reporting postures. Organizations are focused on enacting policies and procedures to ensure timely reporting of material cyber incidents, should they experience one, in order to comply with the new rules.**

Cybersecurity is no longer solely the responsibility of IT and security teams, but something that many areas of the business have a hand in. New regulations on cyber reporting have brought finance leaders into the process much earlier than ever before as they now play an integral role in responding to cybersecurity incidents. Many mature companies have robust reporting processes in place already and are confident in their cybersecurity capabilities, yet disclosure regulations will require companies to fine tune their processes in order to comply. Materiality is a central component of disclosures and perhaps

the most challenging—accurately determining the impacts of cyber-attacks, many of which are not tangible in nature, requires the input of diverse leaders from many areas of the business, with finance leaders playing an important role.

Given how closely KPMG works with many of the world's leading organizations, we have unique insights into how finance leaders are approaching these topics. Below are three areas that Corporate Controllers and CAOs are focused on as they develop strategies to ensure compliance and efficiency in cybersecurity reporting.



## Cybersecurity Reporting Regulation

The newest SEC rule on cybersecurity disclosure requirements, applicable to public companies, was released at the end of July, and beginning December 18th, companies will need to file a Form 8-K to disclose any material incidents that occur. Filing of the Form 8-K is required within four business days of determining the incident is material. The four-day reporting requirement in the rule has caused some concern, but the SEC has acknowledged that companies are going to need time to gather all the information and perform their materiality assessment. The materiality determination should not be rushed, but there can also not be unreasonable delay after discovery of the incident. If a company files a Form 8-K to report a material incident, it must include information about material aspects of the incident as well as the incident's material impact or reasonably likely material impact on the company. The rules also require a company to file an

amended Form 8-K with any material information pertaining to the incident that becomes available or is determined after the original filing.

Alongside incident reporting, the SEC rules also require disclosures on risk management, strategy, and governance in a company's Form 10-K in a new section (Item 1C) dedicated to cybersecurity. A company must disclose information about any process it has for assessing, identifying and managing material risks from cyber threats, as well as the material effects or reasonably likely material effects of risks from cyber threats and previous cyber incidents. Disclosures must also describe the board of directors' oversight of risks from cyber threats and include information on management—both their roles in assessing and managing risks from cyber threats and their expertise levels.



## Key Challenges

Given the level of transparency required in these new reporting standards, there has been some concern from finance leaders that disclosures could serve as a “roadmap” for bad actors (i.e., to perpetrate future cyberattacks). However, unlike the proposed rules, the final rules represent somewhat scaled-back disclosure requirements—rather than very detailed information that could potentially inform bad actors, the Form 8-K requires only the material aspects of the incident (i.e., the nature, timing, scope, and its material impact to the company). In determining the appropriate level of information to include in disclosures, leaders are focused on striking the right balance between proper disclosures and protecting company processes. Many companies are working with outside legal counsel to help inform policy and governance of cyber threat issues.

Materiality remains a challenging concept for organizations to navigate as they prepare to assess cyber incidents under the new rules. The SEC has not provided any further clarity on materiality, instead reiterating that materiality should continue to be applied as it’s currently defined in the securities law.

Assigning materiality to less tangible things such as the potential cost of a data breach has caused difficulty in reporting. However, the SEC did clarify that material analysis “is not a mechanical exercise” and not limited to quantitative measures. Companies must take into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors when determining materiality. Quantitative measures are more straightforward, while things that might be considered from a qualitative perspective include harm to the company’s competitiveness, harm to its relationships with its customers or vendors, brand dilution, or if there’s a possibility of any sort of litigation or regulatory actions.

Evaluating qualitative factors will involve engagement across functions, obviously with cyber teams as well as the CFO, CTO, the general counsel, and possibly external counsels to determine whether an incident is material. Organizations are commonly tasking existing committees with leading the process. In some


instances, new subcommittees are being formed within these committees (e.g., Cyber Incident Disclosure Committee made up of personnel from Legal, Accounting and IT) to focus on materiality determinations. In addition to involving the right functions, companies must also have controls and procedures in place to identify the incident and escalate information about the incident quickly and to the appropriate members of management to make the materiality determinations and make sure that there is timely disclosure. Some organizations are using tabletop exercises and mock scenarios to test responses and ensure that all necessary parties are aligned on the materiality framework.



## Cyber Reporting Preparedness

Organizations are at various levels of preparedness for SEC cybersecurity risk and incident reporting. Large, mature public companies are further along in their cyber-preparedness journeys, with systems, teams, and processes already in place to handle cybersecurity threats and reporting. Preparedness often stems from experience (some companies can average an incident per week, so their teams are more practiced at handling them in a very timely manner) and necessity (companies in highly regulated industries, such as banking or airlines, have existing plans due to reporting and disclosure requirements already being enacted in these industries.) For example, the TSA has stringent disclosure requirements (e.g., cyber-attacks must be reported within 24 hours). So companies in the transportation sector are more ready to comply with the new SEC incident reporting requirements because they already have a response and reporting system in place. The focus for mature organizations is now on fine-tuning their existing plans to match emerging regulations.

Finance leaders anticipate that the latest disclosure process will be a learning experience. While concerns of demonstrating that the materiality determination was made without unreasonable delay were noted, adhering to internal practices and disclosure controls and procedures will show a good faith effort of compliance, which may go a long way with regulators. To prepare, some organizations are carrying out readiness



assessments to gauge whether their teams can handle the new disclosure requirements. Some organizations plan to implement “ratings” scales to determine the severity of threats and assess the company’s ability to respond to them. Other teams have developed cyberthreat playbooks or checklists which lay out the steps and personnel involved in responding to a threat. There is no one-size-fits-all approach, so organizations must develop response plans, controls and procedures that are tailored to their specific cyber threats and company structures.

Governance structures around cybersecurity often take the form of cross-functional audit or risk committees, which may include representation from the business, IT, the legal department, etc., to monitor cybersecurity risks and respond to breaches. In the past, the controller function has

typically not been a part of these groups, but now is being included on disclosure committees. In addition to these shifts at the management level, the new reporting rules introduce more board oversight by requiring that cybersecurity governance structures are reviewed and overseen at the executive leadership and board levels. Some executives are viewing the reporting process as an opportunity to gain more cross-functional efficiencies and transparency, and to break down silos between different IT, Finance, and business functions. Others are taking incidents and reporting on a case-by-case basis and including only those staff who have expertise or a need to know about the issue. In those cases, Finance is often brought in later in the process. Companies need to determine what works best for them given their unique circumstances.

**Finance leaders play a central role in helping their organizations meet the demands of increased cybersecurity regulations. Cyber-attacks are not a question of if, but when, so the work of reporting on and determining the impacts of incidents may become a common, if not routine, part of companies’ operations. Fortunately, many organizations have invested heavily in cybersecurity, and in those cases fine-tuning their reporting is not expected to be a heavy lift. For others, they will need to take a more detailed approach to the new regulation. Ultimately, the increased involvement of CAOs and Controllers, and other areas of the business should serve to further the notion of cybersecurity being an enterprise-wide endeavor, not just an IT initiative.**



### **Additional resources**

[SEC finalizes cybersecurity rules \(kpmg.us\)](#)

[SEC issues guidance on cyber security disclosures \(kpmg.us\)](#)

[Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure](#)

# Contact us



**Dana Foote**  
Audit Head of Markets  
+1 816-802-5229  
dfoote@kpmg.com



**Tim Brown**  
Audit Partner  
+1 212 954 8856  
tdbrown@kpmg.com



**Erin McCloskey**  
Audit Partner  
+1 212 872 5718  
emccloskey@kpmg.com

[home.kpmg/socialmedia](https://home.kpmg/socialmedia)



© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.