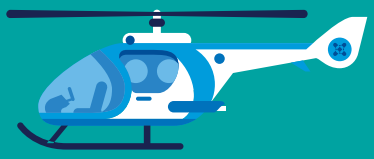
KPMG



# Defining Issues®

## SEC issues guidance on cybersecurity disclosures

February 27, 2018

KPMG reports on the SEC's guidance[1] on cybersecurity disclosures that updates its 2011 guidance[2] but does not add new rules or regulations.

### Applicability

SEC registrants

This guidance does **not** apply to registered investment companies, registered investment advisers, brokers, dealers and self-regulatory organizations because other cybersecurity guidance[3] exists.

### Key facts and impacts

The SEC commissioners approved this new guidance, which strengthens the guidance issued by the Division of Corporation Finance in 2011. The new guidance reinforces existing disclosure requirements related to cybersecurity breaches and adds topics for consideration. The guidance includes the following key topics:

- required disclosure of material information;
- timeliness of disclosures;
- disclosure controls and procedures;
- risk factors;
- MD&A;
- description of business;
- legal proceedings;
- financial statement disclosures;
- board risk oversight;
- insider trading; and
- selective disclosure.

The SEC issued this guidance in response to the increasing significance of cybersecurity incidents. Even though the guidance does not modify or create new SEC rules or regulations, it discusses how companies, both domestic and foreign, might consider cybersecurity matters when preparing disclosures in periodic SEC reports and registration statements.

The SEC does not intend for this guidance to elicit detailed disclosures that might compromise a company's cybersecurity efforts or provide a roadmap to those who may seek to penetrate a company's IT systems, but it continues to encourage disclosure of material information in a timely manner.

The consequences and costs of cybersecurity incidents have continued to rise as companies have increased their reliance on networked systems and the internet.

[1] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459; 34-82746, February, 21, 2018; published in the Federal Register on February 26, 2018

[2] CF Disclosure Guidance: Topic No. 2, Cybersecurity, October 13, 2011

[3] Regulation Systems Compliance and Integrity, Release No. 34-73639, Nov. 19, 2014, and IM Guidance Update, No. 2015-02, April 2015

©2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

These consequences include costs related to remediation, cybersecurity protection, lost revenues, litigation risks, increased insurance premiums, reputational damage and damage to a company's competitiveness, share price and long-term shareholder value.

## Key topics

The guidance discusses a number of key topics with added importance given to required disclosures and the timeliness of providing that information. Additionally, the SEC expanded on its views of cybersecurity disclosure controls and procedures and other effects of cybersecurity incidents on a company's financial statements.

### Required disclosures of material information

When filing disclosure documents with the SEC (e.g. Form 10-K, 10-Q and registration statements) many requirements obligate a company to disclose cybersecurity risks and incidents if they are material, even though Regulation S-X and S-K do not specifically refer to cybersecurity.

Determining whether a cybersecurity incident is material requires judgment, including looking at its nature, extent and potential magnitude. The SEC clarified that it considers an omitted disclosure to be material if there is a substantial likelihood that a reasonable investor would consider the information important when making an investment decision, or it would have significantly altered the total mix of information available. This is consistent with the standard of materiality set by the US Supreme Court.[4]

### Timeliness of disclosures

Once a company has determined that a material incident has occurred, appropriate and timely disclosure is expected. A company that is aware of a material cybersecurity incident or risk should disclose the information promptly and give sufficient notice on Form 8-K or 6-K before it sells securities. An ongoing internal or external investigation is not a valid reason to avoid disclosure. A company may also have a duty to update disclosures if information was omitted or subsequently determined to be untrue.

### Disclosure controls and procedures

The SEC views cybersecurity risk management policies and procedures as key elements of enterprise-wide risk management, as required by federal securities laws.[5]

Cybersecurity disclosure controls and procedures should be included in the company's evaluation of the effectiveness of controls as well as the certifications from the principal executive officer and principal finance officer.

A company should consider whether it has sufficient disclosure controls and procedures to ensure that the relevant information about cybersecurity risks and incidents is appropriately reported to enable senior management to make disclosure decisions and certifications.

The considerations by a company should not be limited only to disclosures; rather they should ensure timely collection and evaluation of information potentially subject to disclosure requirements. A company's controls and procedures should enable it to identify cybersecurity risks and incidents; assess and analyze the effect on the company's business; evaluate the significance associated with the risks and incidents; create open communications between technical experts and disclosure advisors; and make timely disclosures about the risks and incidents.

### Risk factors

The SEC updated this guidance to specify that risk factor disclosures must be specific to the company's situation and should not be general or boilerplate. These disclosures should provide sufficient detail to investors, including disclosing known or threatened incidents, known and potential costs and other consequences. It is not appropriate for companies to disclose cybersecurity as a risk only after an incident has occurred. Risk factors must be updated continually for changing cybersecurity risks.

### MD&A

A company is required to disclose any material event, trend or uncertainty that is reasonably likely to have a material effect on its operations, liquidity or financial condition.[6] If there are material costs, or a significant risk of material costs, or other negative consequences associated with a cybersecurity incident, the company should describe these risks in MD&A.

[4] TSC Industries vs. Northway, 426 U.S. 438, 449 (1976)

[5] Regulation S-X Rules, 13a-14, 13a-15, 15d-14, and 15d-15

[6] SEC Regulation S-K, Item 303, Management's discussion and analysis of financial condition and results of operations, and Item 5 of Form 20-F, Operating and financial review and prospects

©2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

The description should include future effects that the known incidents or potential incidents may have on financial information.

For example, if it is reasonably likely that a known cybersecurity incident will lead to reduced revenues or increases in litigation or costs to protect information, a company should discuss these possible outcomes, including the amount and duration of expected costs. This may also require specific discussion about the possibility of assets becoming impaired and critical accounting estimates.

Additionally, the SEC reminded companies that in past years it has released guidance about how to prepare MD&A. It also specified that the effect of the cybersecurity incident should be considered on each reportable segment.

### Description of business

If a cybersecurity incident could materially affect products, services, customer and supplier relationships or competitive position, these effects should be disclosed.[7]

### Legal proceedings

Proceedings related to a cybersecurity incident should be considered for disclosure in the same manner as other legal proceedings.[8] This includes considerations about how loss of customer information could result in material litigation.

### Financial statement disclosures

Cybersecurity incidents could considerably affect a company's financial statements including additional expenses, loss of revenues and diminished future cash flows. The SEC expects a company's financial reporting and control systems to provide reasonable assurance that information about the range and magnitude of financial statement effects from cybersecurity incidents will be incorporated into its financial statements on a timely basis.[9]

### Board risk oversight

Regulation S-K[10] requires a company to disclose the extent of its board of directors' role in risk oversight. To the extent that cybersecurity risks are material to a company's business, the company should include the nature of the board's role in overseeing that risk.

### Insider trading

The SEC considers knowledge of undisclosed cybersecurity risks and incidents (including breaches) to be material nonpublic information that, if they were traded on, would violate the antifraud provisions of insider trading laws. Many companies have adopted preventative measures to address the appearance of insider trading, and they are encouraged to expand these measures to consider cybersecurity incidents.

Additionally, the SEC suggests that restrictions on insider trading may need to be established while significant cybersecurity incidents are investigated. These restrictions may help prevent directors, officers and other corporate insiders from trading on material nonpublic information. The SEC recommends that a company review its code of conduct to determine whether it appropriately considers trading on nonpublic information related to cybersecurity risks and incidents.

### Selective disclosure

A company also may have disclosure obligations under Regulation Fair Disclosure[11] in connection with cybersecurity matters if information is selectively disclosed. Anytime that a company or person acting on its behalf discloses material nonpublic information to certain listed persons it must publicly disclose that information. A company should establish policies and procedures to ensure that information related to cybersecurity risks and incidents is not selectively disclosed.

[7] SEC Regulation S-K, Item 101, Description of business, and Item 4.B of Form 20-F, Business overview

[8] SEC Regulation S-K, Item 103, Legal Proceedings

[9] KPMG's Defining Issues 11-58, SEC Staff Issues Cybersecurity Disclosure Guidance

[10] SEC Regulation S-K, Item 407(h), Board leadership structure and role in risk oversight, and Item 7 of Schedule 14A, Information required in proxy statement

[11] Final Rule: Selective Disclosure and Insider Trading, Release Nos. 33-7881; 34-43154, Aug. 15, 2000

©2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

**KPMG observation**

Since the Division of Corporation Finance issued its 2011 cybersecurity guidance, the SEC staff has commented on companies' cybersecurity disclosures and requested additional information. Examples include:

- information about material cybersecurity incidents including a description of the costs and other consequences;
- revision of the proxy statement to clarify the effect of a cybersecurity breach in which information was stolen from the company's network, including its effect on its business and investors;
- amendment of a disclosure about whether cybersecurity attacks and threats have continued or increased, and if attacks have continued, a description about the potential costs and consequences to the business;
- revision to a risk factor referring to a cybersecurity intrusion as an unlikely event;
- expansion of a disclosure to state that services were inaccessible for a period of time to appropriately disclose that this was the result of a cybersecurity incident; and
- quantification of the costs incurred to increase controls and preventative measures put in place after a cybersecurity incident.

**Contributing authors**
Jon Baker; Melanie Dolan

**KPMG's Financial Reporting View**
**kpmg.com/us/frv**

**kpmg.com/socialmedia**

The descriptive and summary statements in this newsletter are not intended to be a substitute for the potential requirements of the standard or any other potential or applicable requirements of the accounting literature or SEC rules and regulations. Companies applying U.S. GAAP or filing with the SEC should apply the texts of the relevant laws, regulations, and accounting requirements, consider their particular circumstances, and consult their accounting and legal advisors. Defining Issues® is a registered trademark of KPMG LLP.

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.