What Management Needs to Know About the New SEC Cybersecurity Disclosure Rules

September 2023

AICPA & CIMA

CAQ

About the Center for Audit Quality

The Center for Audit Quality (CAQ) is a nonpartisan public policy organization serving as the voice of U.S. public company auditors and matters related to the audits of public companies. The CAQ promotes high-quality performance by U.S. public company auditors; convenes capital market stakeholders to advance the discussion of critical issues affecting audit quality, U.S. public company reporting, and investor trust in the capital markets; and using independent research and analyses, champions policies and standards that bolster and support the effectiveness and responsiveness of U.S. public company auditors and audits to dynamic market conditions.

About the Association of International Certified Professional Accountants, and AICPA & CIMA

The Association of International Certified Professional Accountants (the Association), representing AICPA & CIMA, advances the global accounting and finance profession through its work on behalf of 689,000 AICPA and CIMA members, students and engaged professionals in 196 countries and territories. Together, we are the worldwide leader on public and management accounting issues through advocacy, support for the CPA license and specialized credentials, professional education and thought leadership. We build trust by empowering our members and engaged professionals with the knowledge and opportunities to be leaders in broadening prosperity for a more inclusive, sustainable and resilient future.

The American Institute of CPAs (AICPA), the world's largest member association representing the CPA profession, sets ethical standards for its members and U.S. auditing standards for private companies, not-for-profit organizations, and federal, state and local governments. It also develops and grades the Uniform CPA Examination and builds the pipeline of future talent for the public accounting profession.

The Chartered Institute of Management Accountants (CIMA) is the world's leading and largest professional body of management accountants. CIMA works closely with employers and sponsors leading-edge research, constantly updating its professional qualification and professional experience requirements to ensure it remains the employer's choice when recruiting financially trained business leaders.

V 1.1

Contents

What management needs to know about the new SEC cybersecurity disclosure rules

In July of 2023, the SEC adopted rules requiring registrants that are subject to the reporting requirements of the Securities Exchange Act of 1934 to make timely disclosure of material cybersecurity incidents as well as annual disclosure of information regarding their cybersecurity risk management, strategy, and governance. The new annual disclosures will be required starting with annual reports for fiscal years ending on or after December 15, 2023, and will be subject to CEO and CFO Section 302(a) certifications, meaning the assessment of the design and effectiveness of disclosure controls and procedures will need to incorporate the new cybersecurity disclosures. These disclosures cover topics in which the CEO and CFO may not have a high level of expertise. Those responsible for managing cybersecurity (e.g., chief information officer [CIO] or chief information security officer [CISO]) will be providing information for disclosure in SEC filings, requiring a new level of responsibility and accountability. Boards and their relevant committees should also be aware that these new rules require disclosures regarding oversight of cybersecurity risks and consider whether they need to enhance their oversight of the entity's cybersecurity program in light of the new disclosure requirements.

Cybersecurity information disclosed in SEC filings, including information about material cybersecurity incidents and the company's risk management, strategy, and governance, is likely to invite scrutiny by the SEC, investors and others. Inconsistencies between the required cybersecurity disclosures and communications on company websites or other public forums could lead to unwanted negative attention or action by regulators and others.

THE IMPORTANCE OF ACCURATE COMMUNICATIONS

Companies have been subject to SEC enforcement actions regarding cybersecurity disclosures that were inconsistent with facts revealed as a result of cybersecurity events. For example, in 2001 Pearson plc agreed to pay $1 million to settle charges that it misled investors about a 2018 cyber intrusion and had inadequate disclosure controls and procedures when they referred to a data privacy incident as a hypothetical risk, when, in fact, the 2018 cyber intrusion had already occurred.[1]

Certifications regarding disclosure controls and procedures

Section 302(a) of the Sarbanes-Oxley Act of 2002 requires the CEO and CFO (or their equivalent) to certify the financial and other information contained in the registrant's forms 10-K. Among other things, these executives certify that they have designed disclosure controls and procedures (DC&P) to ensure that they are made aware of material information.[2] The controls and processes the entity has in place to manage its cybersecurity disclosures are part of DC&P and should be considered when making certifications.

Although there are no certification requirements for the 8-K, SEC rules require that DC&P be designed, maintained and evaluated to ensure full and timely disclosure in current reports.[3] In other words, even though the CEO and CFO do not have to certify DC&P on form 8-K, they are still responsible for establishing controls and procedures to ensure proper disclosure of material cybersecurity incidents and should be comfortable that they are getting complete and accurate information on a timely basis in order to appropriately disclose material cybersecurity incidents.

The information necessary for cyber-related disclosures generally originates with those responsible for managing cybersecurity risks. CEOs and CFOs will need to work with that individual or group of individuals to determine whether current disclosure procedures adequately address information that is required to be disclosed for material cyber incidents as well as cybersecurity risk management strategies and oversight. Some companies may simply need to incorporate existing informal or ad hoc controls and procedures for communicating cyber-related information into the system of disclosure controls and procedures. Other companies may need to build out their existing system of disclosure controls and procedures to include required cybersecurity information.

The information necessary for cyber-related disclosures generally originates with those responsible for managing cybersecurity risks.

Disclosing material cybersecurity incidents

Starting December 18, 2023 (June 15, 2024 for smaller reporting companies) companies will be required to disclose material cybersecurity incidents within four business days of determining that they are material. Although those responsible for managing cybersecurity risks should have already been communicating information about cybersecurity incidents internally or externally due to laws or regulations (including existing SEC requirements), the specificity associated with the new requirements may result in additional scrutiny and responsibility. If information about material incidents is not disclosed, or these disclosures are insufficient, inaccurate, or not timely, the company and individuals within the company may be subject to SEC inquiries or enforcement actions.

As noted above, processes should be in place to ensure those in charge of cybersecurity risk management communicate events to those in charge of SEC disclosures in a timely manner so that the need for disclosure can be evaluated and, if needed, disclosures made. Guidance may be needed to help those who manage cybersecurity risk understand the type of information that needs to be provided to those preparing the disclosures so that those incidents determined to be material for reporting can be appropriately reported.

Determining materiality is key to knowing which cybersecurity incidents need to be disclosed. Both executive management and those responsible for managing cybersecurity risks should be informed and involved in evaluations regarding materiality and whether an incident needs to be disclosed. Various parties (e.g., CISO, CIO, CEO, CFO, legal, board) may have different frames of reference that are relevant for determining whether an incident should be communicated. For example, the SEC's materiality threshold[5] may be different than other thresholds currently used to communicate incidents to other regulatory agencies and affected parties as required by law.[6] It is also important to note that the SEC definition of a cybersecurity incident includes a series of related unauthorized occurrences. This means that disclosure requirements apply if related occurrences are material as a whole, even if each individual occurrence is immaterial.

Companies must make their materiality determinations "without unreasonable delay." For example, the SEC has noted that if the materiality determination is to be made by a board committee, intentionally deferring the committee meeting past the normal time it would take to convene members may constitute an unreasonable delay.[7] Management may want to document who is ultimately responsible for making the materiality determination and criteria for determining what would constitute an unreasonable delay before they identify an incident that could be material.

CYBERSECURITY INCIDENT DISCLOSURES (8-K)[4]

- **Disclose any cybersecurity incident the registrant experiences that is determined to be material, describing:**
  - The material aspects of the nature, scope, and timing of the incident; and
  - The material impact or reasonably likely material impact of the incident on the registrant, including its financial condition and results of operations.
- **Form 8-K must be filed within four business days of determining that an incident is material.**
- **A filing may be delayed if the U.S. Attorney General determines immediate disclosure would pose a substantial risk to national security or public safety.**
- **Information is material if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the total mix of information made available.**

Comparable disclosures are required by foreign private issuers on Form 6-K.

Disclosing cybersecurity risk management and strategy

In addition to disclosing material cybersecurity incidents, the rules require companies to disclose information about their cybersecurity risk management processes and strategy, beginning with the annual report for any period ending on or after December 15, 2023. Management and the SEC disclosure team should work with those responsible for managing cybersecurity risks to ensure they have an adequate understanding of the company's process for identifying, managing, and overseeing cybersecurity risks so that proper disclosure can be made in the 10-K.

While the new rules provide some specific information that should be disclosed when describing the company's processes for assessing, identifying, and managing material risks from cybersecurity threats, it also notes that the specific information is not all-inclusive and that registrants should also disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes. The AICPA's Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program presents multiple criteria that management may consider when determining what information a reasonable investor may find useful in understanding the company's cybersecurity processes. This framework may also be useful in determining what to communicate with the board or other stakeholders.

RISK MANAGEMENT AND STRATEGY DISCLOSURES (10-K)[8]

+ **The registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those process.**

  Including whether:

  - The described cybersecurity processes have been integrated into the registrant's overall risk management system or process, and if so, how;
  - The registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
  - The registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third- party service provider

  The above list is not all-inclusive. Registrants should additionally disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes.

+ **Whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial conditions and if so, how.**

  Comparable disclosures are required by foreign private issuers on Form 20-F.

Managing Risk from Service Providers

The SEC has noted an increasing number of cybersecurity incidents pertain to service providers.[9] Because of the associated risk, the rules require disclosure of whether the company has processes to oversee and identify the cybersecurity risks associated with its use of any third-party service providers. A System and Organization Controls (SOC) 2® report from a service provider can be an important component of an effective strategy for managing the cybersecurity risks of service providers. While similar in structure and content to the SOC 1® reports used in evaluating internal control over financial reporting, SOC 2 reports provide information for evaluating the internal control of service providers on other matters. The culmination of an examination performed by an independent CPA, a SOC 2 report can address controls relevant to the security, availability and processing integrity of the systems used to provide services to its users and the confidentiality and privacy of the information these systems process. Management can use a SOC 2 report in its evaluation of certain risks associated with doing business with the service provider.

Cybersecurity governance and board oversight

The new SEC requirements include disclosure about both management and the board's oversight of cybersecurity risk. As part of their oversight, the board may evaluate whether the company's cybersecurity risk management program is sufficiently robust, or if there are gaps that should be filled. Management related disclosures include a discussion of the relevant expertise of those members of management responsible for measuring and managing cybersecurity risk.

Management should be prepared to provide support as board members exercise their oversight responsibilities. An open and frequently utilized line of communication between the board and those responsible for managing cybersecuirty risk will make it easier to address cybersecurity concerns real-time and before an incident occurs.

Management may expect questions from the board, such as the following,[11] as the board obtains an understanding of the company's cybersecurity risk management process:

What framework, if any, does management use in designing their cybersecurity risk management program (e.g., NIST CSF, ISO/IEC 27001/27002, SEC cybersecurity guidelines, AICPA Trust Services Criteria)?

+ What framework, if any, does management use in communicating pertinent information about its cybersecurity management program?
+ What processes and programs are in place to periodically evaluate the cybersecurity risk management program and related controls?
+ What cybersecurity policies, processes, and controls are in place to detect, respond to, mitigate, and recover from – on a timely basis – cybersecurity events that are not prevented?
+ In the event of a cybersecurity breach, what controls are in place to help ensure that the IT department and appropriate senior management (including board members charged with governance) are informed and engaged on a timely basis—and that other appropriate responses and communications take place?
+ What policies, processes and controls are in place to address the impact to the company of a cybersecurity breach at significant/relevant vendors and business partners with whom the company shares sensitive information? Do those policies include risk identification and mitigation procedures?
+ Has the company conducted a cyber event simulation as part of its approach to enterprise risk management?

INLINE EXTENSIBLE BUSINESS REPORTING LANGUAGE (XBRL)[10]

All registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement.

DISCLOSING CYBERSECURITY RISK GOVERNANCE (10-K)[12]

+ **Description of the board's oversight of risks from cybersecurity threats and:**
  - Identification of any board committee or subcommittee responsible for such oversight (if applicable); and
  - Description of the process by which the board (or committee) is informed about such risks.

(Continues on p11)

+ Has the company considered cost mitigation/risk transfer options in the form of cyber insurance coverage in the event of a cybersecurity breach?

+ Does the company have adequate staff with appropriate skills to design and operate an effective cybersecurity risk management program?

Given the emphasis on materiality, the board may also ask questions such as the following to understand how materiality of a cybersecurity incident is being evaluated:

+ How do we validate that the process for determining materiality is sound and thoroughly documented?

+ Has the company created a method to track related occurrences to see if they qualify as being material?

CPAs CAN HELP!

Start a conversation with your CPA. In addition to being well versed in SEC disclosure, CPAs understand business and financial risk. Cybersecurity is another type of risk that a business must manage, and CPAs are able to put cybersecurity risks in perspective against other business risks that their clients may be facing. CPAs understand the environment in which businesses operate, and can use their knowledge of the client's industry and local market influences to help offer perspective about how cybersecurity considerations fit with other business risks.

In addition to providing insights regarding cybersecurity disclosures, CPAs can assess and report on cybersecurity processes and disclosures. Obtaining any level of assurance by a CPA involves obtaining an understanding of the processes, systems, and data, as appropriate, and then assessing the findings in order to support an opinion or conclusion. Further, CPAs:

+ Have a long history of and are highly experienced at independently gathering evidence to assess internal controls and the reliability and accuracy of data and information that is used to make decisions and is reported externally.

+ Are required by professional standards to plan and perform assurance engagements with professional skepticism.

+ Are experienced in reporting on compliance with various established standards and frameworks.

+ Are required to maintain a system of quality control that is designed to provide the CPA firm with confidence that its engagement partners and staff complied with applicable standards and the reports issued by the CPA firm are appropriate.

+ Are required to adhere to continuing professional education, independence, ethics and experience requirements, including specialized training.

(Continued from p10)

+ **Management's role in assessing and managing material risks from cybersecurity threats.**

  Including:

  - Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

  - The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and

  - Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors

  The above list is not all-inclusive. Registrants should additionally disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes.

  Comparable disclosures are required by foreign private issuers on Form 20-F.

Additional resources

+ Helping Companies Meet the Challenges of Managing Cybersecurity Risk
+ Cybersecurity Risk Management Oversight: A Tool for Board Members
+ SOC for Cybersecurity: Information for organizations
+ CGMA Cybersecurity Tool
+ AICPA's Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program
+ AICPA's Trust Services Criteria

Endnotes

1 Source: https://www.sec.gov/news/press-release/2021-154
2 Source: https://www.sec.gov/rules/final/33-8124.htm Exchange Act Rules 13a-14 and 15d-14
3 Source: https://www.sec.gov/rules/final/33-8124.htm
4 Source: https://www.sec.gov/rules/final/2023/33-11216.pdf
5 According to the SEC's discussion of the final amendments , "information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have 'significantly altered the 'total mix' of information made available.'" Source: SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Final Rule (pg 80) https://www.sec.gov/rules/final/2023/33-11216.pdf
6 The proposed rule discussion materials noted several cybersecurity incident disclosure requirements adopted by various industry regulators and contractual counterparties and stated that "All of the aforementioned data breach disclosure requirements may cover some of the material incidents that companies would need to report under the proposed amendments, but not all incidents." Source: SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposed Rule (pg 58) https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf
7 Source: SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Final Rule (pg 37) https://www.sec.gov/rules/final/2023/33-11216.pdf
8 Source: https://www.sec.gov/rules/final/2023/33-11216.pdf
9 Source: SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposed Rule (pg 8) https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf
10 Source: https://www.sec.gov/rules/final/2023/33-11216.pdf
11 Cybersecurity Risk Management Oversight: A Tool for Board Members (https://thecaqprod.wpengine.com/wp-content/uploads/2019/03/caq_cybersecurity_risk_management_oversight_tool_2018-04.pdf)
12 Source: https://www.sec.gov/rules/final/2023/33-11216.pdf

CAQ

www.thecaq.org

AICPA® & CIMA®

www.aicpa-cima.com

We welcome your feedback!

Please send your comments or questions to info@thecaq.org