ALSTON & BIRD

WWW.ALSTON.COM

Securities Law / Securities Litigation / Privacy, Cyber & Data Strategy
ADVISORY ■

JULY 31, 2023

SEC Adopts New Cybersecurity Disclosure Rules for Public Companies

by Dave Brown, Kate Hanniford, Kim Peretti, Julie Mediamolle, Cara Peterman, Sierra Shear, Kristen Bartolotta, *and* Kezia Osunsade

On July 26, 2023, the Securities and Exchange Commission (SEC) approved the new cybersecurity disclosure rules for public companies with significant modifications from the draft rules proposed in March 2022. For a more extensive discussion of the proposed cybersecurity disclosure rules, see our previous advisory, "SEC Proposes Sweeping New Cybersecurity Disclosure Rules for Public Companies."

Among the more controversial measures adopted with some revisions from the proposed rule is that the SEC will require disclosure of a material cybersecurity event on Form 8-K within four days of such materiality determination, which must be made "without unreasonable delay," although it provides a limited exception for delay if the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety.

New Disclosure Requirements Highlights

The table below summarizes the new disclosure requirements.

Regulation	Disclosure Requirement
Cybersecurity Risk Management and Strategy (Regulation S-K Item 106(b), Form 10-K)	• Describe the company processes for assessment, identification, and management of material risks from cybersecurity threats • Describe whether any risks from cybersecurity threats have or are reasonably likely to affect the company's business strategy, results of operations, or financial condition
Cybersecurity Governance (Regulation S-K Item 106(c), Form 10-K)	• Describe the board of directors' oversight of cybersecurity threats • Describe management's role in assessing and managing material risks from cybersecurity threats

Regulation	Disclosure Requirement
Material Cybersecurity Incidents (Form 8-K Item 1.05)	• File a Form 8-K to disclose any material cybersecurity incident and describe the incident's nature, scope, timing, and impact (actually or likely) within four business days of determining that the incident is material, unless the Attorney General grants an exception • File an amendment to the Form 8-K with required information that was not determined or was unavailable at the time of the original filing
Form 20-F	• Describe the board of directors' oversight of cybersecurity threats • Describe management's role in assessing and managing material risks from cybersecurity threats
Form 6-K	• Disclose information on material cybersecurity incidents required under the SEC rules or that the company discloses in a foreign jurisdiction

The untimely filing of an Item 1.05 of Form 8-K will not result in loss of Form S-3 eligibility.

Amendments to the Original Form 8-K

The new rules require an amendment to the original Form 8-K to disclose required information not available at the time of filing the original Form 8-K. This amendment should be filed within four business days of the company discovering the information or the information becoming available, without delay.

Additionally, issuers should file an amendment to the Form 8-K to correct previously disclosed information that is later determined to be incorrect or misleading.

The amendment requirement essentially transforms the Form 8-K to the cybersecurity incident disclosure form – but companies will still need to give repetitive disclosure for loss contingencies in footnotes to the financial statements.

The Limited Attorney General Exception

Companies can delay the filing of the Form 8-K for up to 30 days, with the potential of a 60-day extension, if the U.S. Attorney General determines that a disclosure within the four-business-day timeline would pose a "substantial risk" to public safety or national security. Companies would have to request this extension from the U.S. Attorney General.

What Was Not Adopted

Notably, and in a departure from the proposed rule, companies are not required to disclose the material cybersecurity incident's remediation status or technical information about its response to the material cybersecurity incident in the Form 8-K filing. The final rule does not include a requirement for Regulation S-K to specifically disclose the cybersecurity expertise of each board member in its annual reports and generally requires less granular or specific disclosure of a company's cyber-risk management program than was initially proposed. See the table below for a more granular comparison of the proposed and final rules.

Overlapping Governmental Disclosure Requirements

Although the SEC acknowledged the extensive comments generated by the proposed rules and that public companies already may be subject to many other, potentially overlapping or competing cybersecurity reporting requirements, it dismissed these concerns as secondary to the primacy of investor disclosure needs, specifically distinguishing the purpose of SEC public company disclosures from other federal agency rules, including forthcoming Cybersecurity and Infrastructure Security Agency rulemaking pursuant to the federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The final rule release acknowledges the potential for future modifications to SEC rules to harmonize them in accordance with CIRCIA and presumably the National Cybersecurity Strategy.

When the New Rules Will Be Effective

The final rules are effective 30 days after the publication of the rule in the *Federal Register* (which can be anywhere between three business days to a week or longer).

The new incident reporting via Form 8-K or 6-K is scheduled to take effect the later of 90 days from publication in the *Federal Register* or December 18, 2023. The updated disclosure requirements will apply to annual reports on Forms 10-K and 20-F for fiscal years ending on or after December 15, 2023.

Smaller reporting companies have 270 days after the publication of the final rule in the *Federal Register* or until June 15, 2024, whichever is later, to comply.

What to Do Now

To prepare for these fourth quarter 2023 compliance dates, companies should review and update their cybersecurity policies and procedures and incident management protocols. Issuers should also consider enhanced incident response training to raise awareness of the disclosure timelines. Additionally, companies should discuss how they plan to determine the materiality of a cybersecurity incident.

Assessing Materiality Following a Cybersecurity Incident

The final rule only requires disclosure of cybersecurity incidents that are "material" under the federal securities laws, i.e., where there exists 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.'" This materiality standard remains unchanged. However, the final rule now requires that the determination must occur without "unreasonable delay" (which is a slight softening from the proposed rule's "as soon as reasonably practicable" timeframe).

The SEC has previously noted that materiality assessments should consider both qualitative and quantitative factors and that this assessment should be holistic and not mechanical. The SEC, however, has otherwise declined to provide further guidance on the threshold for "materiality" in the context of cybersecurity incidents, despite numerous comments requesting such direction.

The few public SEC investigations or enforcement actions related to cybersecurity disclosures to date, however, provide some direction and collectively show that the SEC may consider a variety of factors when assessing the materiality of a cybersecurity incident in hindsight, including the volume and sensitivity of the data impacted, how the threat actor entered the system, whether data was exfiltrated or just accessed,

and how long the threat actor was in the system.[1] If there are business or operational disruptions caused by a cybersecurity incident, the materiality analysis might include various additional factors, such as which systems were disrupted, and in particular, whether the company's financial systems were impacted; the length of time that systems were interrupted; whether any backup systems exist or could be implemented; and potential loss of revenue or other financial impact caused by the disruption.

Additional public SEC enforcement actions involving cybersecurity disclosures will continue to provide further guidance on the factors that companies should consider as they assess the materiality of a cybersecurity incident.

Disclosure of a Company's Cybersecurity Risk Management, Strategy, and Governance

Under the adopted rule amendments, companies must describe their "processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes" in their Form 10-K / 20-F filings. Importantly, "cybersecurity threat" is defined as any potential unauthorized occurrence on *or conducted through* a company's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a company's information systems or any information residing in them. This may incentivize all companies providing information systems as a service to strengthen their know your customer policies.

Additionally, companies must discuss how their cybersecurity processes have been integrated into overall risk management processes, whether the company engages third parties in connection with its cybersecurity risk management processes, and if so, whether the company has a risk management process associated with its third-party service providers.

Companies will be required to disclose their processes for assessing, identifying, and managing material cybersecurity threats, and the material impacts of those threats in their Form 10-K.

Additionally, companies will be required to describe the board's oversight of risks from cybersecurity threats, identify the board committees responsible for overseeing cybersecurity risks, and describe the processes by which the board is informed of cybersecurity risks.

The SEC clarified that this list of disclosures is not exhaustive, and companies should disclose the information necessary for a reasonable investor to understand their cybersecurity processes. In addition to the mandatory disclosures on cybersecurity risk management, the new rules also direct companies to consider disclosing additional information about management's role in overseeing and managing cybersecurity risks, including which members of management and which committees are responsible for managing the company's material cybersecurity risks and their relevant expertise, the process by which responsible people and committees are informed about cybersecurity incidents, and whether the responsible people and committees report cybersecurity risk information to the board.

Foreign Private Issuer Cybersecurity Requirements (Forms 6-K and 20-F)

Foreign private issuers (FPIs) are required to comply with the newly adopted cybersecurity disclosures as well. On Form 6-K, FPIs are required to promptly make the same disclosures required under Item 1.05 of

---

[1] *See, e.g.*, "SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors"; "SEC Charges Pearson plc for Misleading Investors About Cyber Breach."

Form 8-K, including the requirement to amend the form with updates as they are discovered or become available. Similarly, FPIs are required to make the same cybersecurity disclosures as other companies in their Form 20-F.

Structured Data Requirements

Companies are required to tag the disclosures in Inline XBRL with a staggered compliance date of one year. Smaller reporting companies have 270 days after the publication of the final rule in the *Federal Register* or until June 15, 2024, whichever is later, to comply.

Comparison Between the Final Rule and Proposed Rule

The table below compares the main provisions of the proposed rule to the final adopted rule.

Proposed Rule	Adopted Rule	Key Differences
Definitions of Key Terms		
• Cybersecurity Incident – "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."	• Cybersecurity Incident – "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."	• Expanded to include a series of occurrences because a series of related occurrences can collectively have a material impact and trigger disclosure requirements
• Cybersecurity Threat – "any potential occurrence that may result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein."	• Cybersecurity Threat – "any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein."	• Modified to better align with the adopted definition of "cybersecurity incident"

Proposed Rule	Adopted Rule	Key Differences
• Information Systems - "information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of a registrant's information to maintain or support the registrant's operation."	• Information System – "electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations."	• Modified to clarify that the definition does not include hard-copy resources
Reporting Material Cybersecurity Incidents on Form 8-K		
• Disclosure of certain information on Form 8-K within four business days after the company discovers a material cybersecurity incident	• Disclosure of certain information on Form 8-K within four business days after the company discovers a material cybersecurity incident	• No change in the timing of the disclosure due to the narrowing of the required disclosure
• Disclosure of the following information about a material cybersecurity incident: – When the incident was discovered and whether it is ongoing – A brief description of the nature and scope of the incident – Whether any data was stolen, altered, accessed, or used for any unauthorized purpose – The effect of the incident on the company's operations – Whether the company has remediated or is currently remediating the incident	• Disclosure of the following information about the impact of a material cybersecurity incident: – The material aspects of the nature, scope, and timing of the incident – The material impact or reasonably likely material impact on the company, including its financial condition and results of operations	• The required disclosures focus on the impact of the cybersecurity incident, rather than the incident itself • Removal of the disclosure of the cybersecurity incident's remediation status • Clarification that companies do not need to disclose specific or technical information about their planned response to cybersecurity incidents or system vulnerabilities

Proposed Rule	Adopted Rule	Key Differences
• No extension to the four-day reporting timeframe for enforcement delays or an ongoing investigation	• Potential for delay up to 30 days (and a possible 60-day extension) when the Attorney General determines that disclosure poses a substantial risk to national security or public safety	• Creates an opportunity for extension in very limited cases
Providing Mandatory Updates on Material Cybersecurity Incidents		
• Disclosure of material updates on the material cybersecurity incident, previously reported on Form 8-K, in the Form 10-K or 10-Q when the material change/update occurred	• Not adopted	• Material updates to a material cybersecurity incident must be provided in a Form 8-K amendment
• Material additional information includes updates to the following: – The breadth of the cybersecurity incident – Whether any data was compromised – The present and future impact of the cybersecurity incident on the company's business – Present or future measures to remediate the cybersecurity incident – Any changes in the company's policies or procedures as a result of the cybersecurity incident – Other material updates	• Not adopted	• Material updates to a material cybersecurity incident must be provided in a Form 8-K amendment

Proposed Rule	Adopted Rule	Key Differences
Reporting of Individually Immaterial Incidents When Material in the Aggregate		
• Reporting of immaterial individual events that become material collectively in the Form 10-K or 10-Q when the materiality determination is made	• Not adopted	• The definition of a cybersecurity incident was expanded to include a series of related unauthorized events, meaning that immaterial individual events can trigger an 8-K disclosure requirement in the aggregate
• Disclosure of the following information in the Form 10-K or 10-Q: – When the cybersecurity incidents were discovered – Whether the incidents are ongoing – A description of the incidents – Whether the incidents allowed any data to be compromised – The impacts of the incidents on the company's business and actions – Whether the company has remediated the incidents	• Not adopted	• A series of unauthorized events can trigger an 8-K disclosure requirement containing: – The material aspects of the nature, scope, and timing of the incident – The material impact or reasonably likely material impact on the company, including its financial condition and results of operations

Proposed Rule	Adopted Rule	Key Differences
Cybersecurity Risk Management Disclosures on Form 10-K		
• Disclosure of information about the company's policies and procedures on cybersecurity risk management, including whether the company: – Has a cybersecurity risk assessment program (and, if so, provide a description of the cybersecurity risk program) – Uses third parties in connection with its cybersecurity risk program – Has policies to identify cybersecurity risks with third-party providers – Has contractual provisions and other mechanisms to limit cybersecurity risks with third-party providers – Has taken steps to prevent and mitigate the effects of cybersecurity incidents – Has continuity and recovery plans in place for a cybersecurity incident – Has changed company policies due to prior cybersecurity incidents – Has experienced impacts on its operations or finances due to cybersecurity risks and incidents (and, if so, describe how the company was impacted) – Considers cybersecurity risks as a part of the company's business strategy and financial planning	• Description of the company's processes for assessment, identification, and management of material risks from cybersecurity threats • Disclosure of whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect its business strategy, results of operations, or financial condition • Disclosure of whether and how the previously described cybersecurity processes have been integrated into overall risk management • Disclosure of whether the company engages third parties in connection with its cybersecurity risk management processes • Disclosure of whether the company has processes to oversee and identify material cybersecurity risks associated with its use of third parties	• Narrows elements from the proposed disclosure to protect companies' cybersecurity, while providing material information to investors • Instructs companies to disclose additional information that is necessary for a reasonable investor to understand the company's cybersecurity processes

Proposed Rule	Adopted Rule	Key Differences
Periodic Cybersecurity Governance Disclosures		
• If cybersecurity risks are material to the company's business, the company should disclose the following relating to board oversight: – Which directors are responsible for the oversight of cybersecurity risks – How the board is informed about cybersecurity risks – How frequently the board discusses cybersecurity risks – How the board considers cybersecurity risks as a part of the company's business strategy – If cybersecurity risks are material to the company's business, the company should disclose the following relating to management's relationship with the company's security: • The directors' prior work experience • The directors' certifications or degrees in cyber • Whether the directors have other relevant knowledge, skills, or other background in cyber	• Companies must describe the board's oversight of risks from cybersecurity threats • Companies should, if applicable, identify any board committee or subcommittee responsible for cybersecurity oversight and describe the processes by which the board is informed of the risks • Companies must describe management's role in assessing and managing the company's material risks from cybersecurity threats • Companies should consider disclosing: – Whether and which management positions and committees are responsible for managing material cybersecurity risks and the relevant experience of such persons to determine expertise – The process by which persons responsible for assessing and managing cybersecurity risks report information to the board – Whether the persons responsible for managing and assessing cybersecurity risks report to the board about the risks	• Required disclosure is less granular to protect company cybersecurity, while still providing investors with relevant information

Proposed Rule	Adopted Rule	Key Differences
• If any member of the board is determined to have "cybersecurity expertise," the company should disclose the names of such directors and provide such detail as necessary to fully describe the nature of the expertise	• Not adopted	• N/A, covered in the other governance disclosures
FPI Cybersecurity Disclosures		
• Amend Form 20-F to incorporate parallel cybersecurity disclosures to domestic companies	• Adopted as proposed with modifications consistent with Item 106 of Regulation S-K	• N/A
• Amend Form 6-K to reference material cybersecurity incidents among the items that may trigger a current report on Form 6-K and amend Form 20-F to require updated disclosure regarding incidents previously disclosed on Form 6-K.	• Adopted as proposed with modifications consistent with Item 1.05 of Form 8-K	• N/A

You can subscribe to future advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you would like more information, please feel free to contact one of the attorneys in our **Securities Group**, **Securities Litigation Group**, **Privacy, Cyber & Data Strategy Group**

.

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ +1 404 881 7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32 2 550 3700 ■ Fax: +32.2.550.3719
CHARLOTTE: 1120 South Tryon Street ■ Suite 300 ■ Charlotte, North Carolina, USA 28203-6818 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ +1 214 922 3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 214 922 3400 ■ Fax: 214.922.3899
LONDON: LDN:W ■ 6th Floor ■ 3 Noble Street ■ London ■ EC2V 7DE ■ +44 20 8161 4000
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ +1 213 576 1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ +1 212 210 9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ +1 919 862 2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ +1 415 243 1000 ■ Fax: 415.243.1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA 94304-1012 ■ +1 650 838 2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ +1 202 239 3300 ■ Fax: 202.239.3333