



Cybersecurity Disclosure Readiness: Preparing for the New SEC Regulations

John Hancock
Samita Ali-Khan
Chris Hart

October 10, 2023

Brief Overview of Rules

- The rules aim to enhance the quality and consistency of cybersecurity disclosures
- The rules have two main components:
 - **New Item 1.05** of Form 8-K requires timely disclosure of material cybersecurity incidents
 - **New Item 106** of Regulation S-K requires annual disclosure of cybersecurity risk management, strategy, and governance
- The rules apply to most reporting issuers, with slight accommodations for smaller reporting companies and foreign private issuers
 - The rules do not apply to asset-backed issuers, investment companies, or 40-F filers
 - The rules do apply to business development companies

Brief Overview of Timing

- Annual Reports on Forms 10-K and 20-F
 - Effective for reports for fiscal years ending after **December 15, 2023**
- Current Reports on Forms 8-K and 6-K
 - Generally: effective **December 18, 2023**
 - Smaller reporting companies: effective **June 15, 2024**
- XBRL tagging requirements are effective one year after the initial effective dates (but with no extended compliance for SRCs)
 - Annual Reports on Forms 10-K and 20-F: effective for fiscal years ending after **December 15, 2024**
 - Forms 8-K and 6-K: effective **December 18, 2024** (including SRCs)

Background

- CF Disclosure Guidance, Topic No. 2 – *Cybersecurity* (Oct. 11, 2011)
- *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release No. 33-10459 (Feb. 21, 2018)
- Proposing Release: *Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure*, Release No. 33-11038 (Mar. 9, 2022)
- Adopting Release: *Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure*, Release No. 33-11216 (Jul. 26, 2023)
 - “Commission staff has observed insufficient and inconsistent cybersecurity disclosure notwithstanding the prior guidance.”
 - Adopting release reaffirms that the new rules “supplement” prior guidance, including disclosures in risk factors, MD&A, business and legal proceedings

Motivating Factors

- More cybercriminals
- More reliance on electronic systems
- Increase in remote work
- Increased outsourcing of IT services
- Monetization of cyberattacks
- Increase in "... business interruption, lost revenue, ransom payments, remediation costs, liabilities to affected parties, cybersecurity protection costs, lost assets, litigation risks, and reputational damage"
- Anticipated impact of AI
- Inconsistent and non-existent reporting

Part of Larger Cyber Governance Trend

- Increasing White House Action
 - The Biden Administration has issued a number of Executive Orders regarding cybersecurity practices.
 - While these affect federal agencies, they have trickle-down effects on government contractors.
- Increasing Agency Regulation
 - Other agencies also increasingly involved in governance of cybersecurity (FTC, CFPB).
 - New NIST requirements.
- Increasing State Regulation and Oversight
 - States are creating new comprehensive privacy laws (CA, CO, CT, VA, UT).
 - Some states are also creating robust cybersecurity regulations (NY).
- Increasing International Legislation (EU, UK, India, China, Australia)
- Best Practices
 - Rulemaking and enforcement trends will work to create a set of industry best practices around education and training, internal policies and procedures, and auditing and assessments.

Key Concerns

- Diverts resources and attention mid-crisis
- Publicly exposes network weaknesses
- Conveys more power to bad actors
- Adds complexity to reporting

Form 8-K Cybersecurity Incident Disclosure

- New Item 1.05 of Form 8-K:

“If the registrant experiences a *cybersecurity incident* that is determined by the registrant to be material, describe the material aspects of the *nature, scope, and timing* of the incident, and the material *impact or reasonably likely* material impact on the registrant, including its financial condition and results of operations.”

Timing for Form 8-K Disclosures

- A registrant must file a Form 8-K within four business days after it determines that it has experienced a material cybersecurity incident
 - The SEC anticipates some interval before public disclosure: “*disclosure coming due less than a week after discovery should be uncommon*”
 - 4 days is standard for 8-K reporting, but is uncommonly short in the U.S. for breach reporting
- In some cases, the materiality assessment will be very subjective
- The materiality assessment must be made “without unreasonable delay”
 - Registrants may not delay scheduling board or committee meetings beyond the usual time to convene a meeting
 - Registrants may not revise internal upward incident reporting and assessment to delay Form 8-K reporting

Form 8-K – Updating Obligations

- Initial Form 8-K must identify any required information that is “not determined or is unavailable”
- The registrant must file an amendment to disclose the omitted information
- The amendment must be filed within four business days after the registrant (“without unreasonable delay”) determines the information or within four business days after the information becomes available
- NOTE: Registrants should consider the duty to correct prior disclosures that were erroneous or misleading, as well as the duty to update disclosures that have become materially inaccurate and are being relied upon by investors

Delayed Filing for National Security/Public Safety

- Extremely narrow exception to permit delayed reporting for up to 30 days
- Applies only if the United States Attorney General:
 - Determines that disclosure “poses a substantial risk to national security or public safety” and
 - Notifies the SEC in writing
- The delay can be extended with additional determinations and notices by the SEC
 - Up to two additional 30-day periods for either national security or public safety
 - And an additional 60-day period for national security (but NOT public safety)
 - Further delays require an exemptive order from the SEC

Key Defined Terms

- **“Cybersecurity incident”** means 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.”
- **“Cybersecurity threat”** means 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.”
- **NOTES:**
 - A registrant’s “information systems” **include** third-party systems that it uses (e.g., ADP)
 - “Unauthorized” includes “accidental”
 - “Jeopardizes” requires a forward-looking assessment of whether the effect of an incident is or is reasonably likely to be material

What is an “Incident”?

- Data theft or erasure
- Actual data alteration
- Potential data alteration
- Ransomware
- "Accidental exposure"
- Failure to secure a server
- Accidental power loss (impacts "availability")
- Loss of unencrypted laptop or USB drive

- Unauthorized access or use of data by authorized person
- Unauthorized public viewing of laptop screens

But how about...

- Weak, noncompliant passwords?
- Failure to timely remove access from terminated employees?
- Emails to Board members with external email address?

What is “Material”?

- Undefined, but general practice says information is material if:
 - There is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or
 - Disclosure of the information would have been viewed by the reasonable investor as having significantly altered the total mix of information made available.
- Consider facts and circumstances of each incident and registrant's business and industry:
 - The nature, duration and scope of the incident, including the type and amount of data compromised and the potential for reputational harm or competitive disadvantage
 - Remediation costs, lost revenues, increased expenses or impairment of assets
 - Legal, regulatory, or contractual obligations or consequences of the incident, including any potential fines, penalties, lawsuits, or breaches of agreements
 - The registrant's response, including the measures taken to contain, mitigate, and prevent future incidents, and the effectiveness and timeliness of such measures

Examples of Potentially Material Incidents

- Ransomware attack that encrypts critical data for an extended period
- Data theft that expose the registrant to material claims from customers
- Data breach that exposes millions of consumers' private information
- Data breach that triggers material government enforcement action or class action lawsuits
- Data breach where remediation costs (e.g., credit reporting services) are material
- Cyberattack that exposes vulnerability in the registrant's product that requires a recall, update or other modification

Examples of Potentially Material Impacts

- Harm to reputation
- Harm to customer or vendor relationships
- Competitive disadvantages
- Possibility of litigation or regulatory investigations or proceedings

Form 8-K Commentary

- Disclosures cover systems “owned or used” by the registrant (e.g., third-party systems)
- Disclosures are “based on the details available to” the registrant
 - Information that is known or “reasonably available”
- Disclosures should focus on the impact of the incident, not the details of the incident itself
- No need to disclose information that would empower threat actors
- No need to disclose the status of any remediation efforts
- No need to disclose whether data was compromised
- No need to disclose vulnerabilities or remediation/mitigation plan
- Registrants do not have to disclose immaterial “incidents” that are “collectively material”, but multiple “related” attacks may constitute a single reportable “incident”
 - E.g., same attacker or exploitation of the same vulnerability

Related Consequences

- Failure to file a Form 8-K Item 1.05 report will not affect Form S-3 eligibility
- Failure to file a Form 8-K Item 1.05 report will be eligible for the safe harbors under Rule 13a-11(c) and 15d-11(c) for liability under Section 10(b) of the Securities Exchange Act and Rule 10b-5
- Item 1.05 disclosures are filed rather than furnished and are therefore subject to liability under Section 18 (liability to trading securityholders)

Annual Report Disclosure

■ New Item 106 of Regulation S-K:

■ Risk management and strategy disclosure

“Describe 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 processes.”

“Describe 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 condition* and if so, how.”

■ Governance disclosure

Risk Management & Strategy Disclosure Commentary

- Disclosure should address, as applicable:
 - Whether and how the processes are integrated into the registrant's overall risk management systems
 - Whether the registrant uses assessors, consultants, auditors or other third parties (e.g., scope of in-house capacity), without names or description of services
 - Whether the registrant has processes to oversee and identify threats to third-party service providers
 - Whether any “cybersecurity threats” (including previous “cybersecurity incidents”) have materially affected or are reasonably likely to materially affect the registrant and, if so, how
 - ◆ Includes impacts on strategy, results of operations and financial condition
 - ◆ This may require correcting prior Form 8-K disclosures

Governance Disclosure Commentary

■ Disclosure should cover:

- The board's oversight process, including any delegation to committees
- How the board or committee is informed about risks from cybersecurity threats
- Management's role in assessing, identifying and managing material risks from cybersecurity threats, including:
 - ◆ Who has responsibility for cybersecurity risk management, including details about relevant expertise (work experience; degrees and certifications; knowledge, skills and background)
 - ◆ The processes by which they are informed about and monitor prevention, detection, mitigation and remediation of cybersecurity incidents
 - ◆ Whether they report to the board or a board committee about such risks

Changes from Proposed Rules

- Registrants are not expressly required to disclose:
 - Each type of risk or quantifiable risk metrics
 - “Policies” and “procedures” for managing cybersecurity risks
 - ✦ Activities to prevent, detect and minimize the effects of cybersecurity incidents
 - ✦ The frequency of board discussions of cybersecurity risks
 - ✦ Business continuity and recovery plans
 - Cybersecurity training
 - Whether and how cybersecurity is part of business strategy, risk management, financial oversight
 - Whether the registrant has a chief information security officer and to whom the officer reports
 - Whether directors have expertise in cybersecurity, nature of expertise and source of expertise
 - ✦ Some companies may still conclude that board-level expertise is necessary and should be disclosed
 - Results of independent assessments or audits, or use of NIST framework

Inline XBRL Requirements

- Registrants must tag their cybersecurity disclosures in Inline XBRL one year after the applicable initial effective dates
- Inline XBRL tagging applies to both the Form 8-K cybersecurity incident disclosure and the Regulation S-K cybersecurity risk management, strategy, and governance disclosure
 - Block text tagging
 - Quantitative amount tagging

Liability and Enforcement

- Potential enforcement actions
 - False statements
 - Omissions of material facts
- Potential for individual liability under *Caremark* doctrine

Key Takeaways

- Review, test and improve procedures for identifying and responding to cybersecurity incidents
- Create effective communication procedures between the cybersecurity team, legal team supporting cybersecurity, the legal team responsible for securities disclosure, front-line business leaders and the board or relevant board committee
- Carefully document materiality analyses and the reasonableness of the time that it takes to assess materiality
- Revisit engagement of third parties in connection with the risk management process
- Avoid rushed drafting of disclosure and consider existing disclosure

Our Panel



Christopher Escobedo Hart

Partner &
Co-Chair, Privacy & Data Security Practice
chart@foleyhoag.com
617.832.1232



John Hancock

Partner &
Co-Chair, Capital Markets Practice
jhancock@foleyhoag.com
617.832.1201



Samita Ali-Khan

Partner
salikhan@foleyhoag.com
212.812.0357