SEC Cybersecurity Compliance and Enforcement Landscape

October 24, 2024

GIBSON DUNN

Agenda

01	Refresher: SEC Cybersecurity Rule Adopted July 2023
02	The First Year: SEC Implementation and Industry Practice
03	Spotlight: SEC Enforcement Update
04	Impact of the 2023 Rule: Practical Applications

SEC Cybersecurity Rule Adopted July 2023

01

SEC's Cybersecurity Rule:

The SEC's cybersecurity rule, which became effective on December 18, 2023, (the "2023 Rule") imposes **new reporting obligations** on public companies, including:

Incident Disclosures: Disclose cybersecurity incidents as Item 1.05 of Form 8-K within four days of determining the incident likely has or is likely to have a material impact (or presents a material risk)

Governance: Disclose cybersecurity strategy, governance, oversight, and risk management as Item 106 on Form 10-K

Risk Factors: Disclose cybersecurity-related risk factors on Form 10-K in Item 1A

Key Provisions of the 2023 Rule

Cybersecurity Incident:
An unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing therein.

- **What is an incident?**
  - The 2023 Rule broadened the definition of "cyber incident" to include "a series of related unauthorized incidents."
- **What must be disclosed?**
  - Companies should include the material aspects of the **scope, nature, and timing of the incident**, including the reasonably likely material impact to the company's operations and financial position.
  - Disclosure need not contain technical details regarding the nature of the breach, especially not those that would impede the company's response.
- **What is the timing for disclosure?**
  - Companies should make a materiality determination "without unreasonable delay."
  - Companies should file a Form 8-K announcing the incident within **four days** of determining that the incident is material.
- **Updating disclosures**
  - If a company discloses a cybersecurity incident and subsequently gains additional information that should be disclosed, it should file an amendment to its 8-K within four days of gaining the required information.

Assessing Materiality for Cybersecurity Incidents: Considering Quantitative and Qualitative Factors

A cybersecurity incident is material if "[t]here 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."

The materiality of a cybersecurity incident is a **facts and circumstances determination**, that should consider a **range of qualitative and quantitative factors** informed by the law, facts, professional judgment, and advice of outside counsel.

Illustrative Qualitative Factors:

- Potential harm to a company's reputation
- Potential harm to vendor or customer relationships
- Potential harm to a company's competitiveness
- The possibility of litigation or regulatory action
- The nature of the incident (e.g., access vs extraction)

Illustrative Quantitative Factors:

- The amount of data impacted
- Extent of impact to quarterly results financial results or results of operations
- Extent of current or ongoing business interruptions
- Lost revenue
- Remediation costs
- Regulatory fines
- Increased cybersecurity costs
- Lost assets
- Ransom payments
- Potential liabilities to third parties

SEC Implementation and Industry Practice

02

The Gerding Statement

Key Takeaway: Item 1.05 (which was created as part of the 2023 Rule and titled "Material Cybersecurity Incidents") should only be used to disclose cybersecurity incidents that have been deemed material.

The First Few Months

- **Timing of Disclosure:** There was a strong trend to file quickly after becoming aware of a cybersecurity incident.
- **Overwhelming use of Item 1.05:** During the first few months following the effective date of the 2023 Rule, many companies elected to file Form 8-K disclosures **before** a materiality determination had been made, following up with subsequent filings opining on the materiality of the incident.

Gerding Statement Impact

- On May 21, 2024, the Director of the SEC's Division of Corporate Finance issued a statement (the "Gerding Statement") clarifying **that companies should only disclose cybersecurity incidents under Item 1.05 when an incident was determined to be material.**
  - **The Gerding Statement also articulated that:**
    - the Staff encourages voluntary disclosure of cybersecurity incidents, including incidents for which materiality has not yet been determined (or which are determined to be immaterial); and
    - Item 8.01 (for "Other Events") is appropriate for such disclosures.
- After the Gerding Statement, companies have **primarily filed under Item 8.01** when there is a cybersecurity incident that has not (yet) been determined material.
- There is still a strong trend towards the **quick disclosure of cybersecurity incidents** using Items 8.01 and 1.05.

The Materiality Determination

Key Takeaway: Disclosure outlining a cybersecurity incident's materiality should include detail beyond financial impacts.

- **Internal materiality determinations** are based on robust and detailed analyses relating to the nature, scope and impact of an incident.
- Public disclosure has not reflected this level of detail. Initial filings tend to eschew detail, **describing the nature and scope of the incident in general terms**.
- Companies also generally assess materiality in light of the **impacts on current / ongoing business operations and financial results / condition**.
- The Staff may **increase pressure** on impacted companies to include more detailed discussions regarding the factors considered in making a materiality determination.

Overall Disclosure Trends

There have been ~80 filings made by ~50 companies.

- After the **Gerding Statement**, there has been a decrease in companies making initial disclosures under Item 1.05.

- **Companies are making multiple disclosures:** an initial disclosure under Item 8.01 before materiality has been determined, followed by an amended 8.01 updating the disclosure, or an Item 1.05 disclosure if materiality has been determined.

- **Recent comment letters and SEC guidance indicate that disclosures that discuss materiality at a high level may not be detailed enough.**
  - The SEC has requested that companies that have disclosed material impact describe all material impacts in future or amended 8-K filings.
  - The SEC has questioned whether companies applied materiality standards under U.S. securities law.
  - The SEC has directly asked for more information from companies.
  - The SEC has made clear that companies should consider both quantitative and qualitative factors in assessing materiality.

- **Delayed Reporting**: Delayed reporting is permitted only under narrow circumstances if the U.S. Attorney General informs the SEC that disclosure would pose a substantial risk to national security or public safety.
  - DOJ has stated that it has delayed disclosure “on a number of occasions” since the 2023 Rule went into effect.
  - As expected, this exemption is narrow and granted sparingly.
  - There is also a delay available for companies subject to the FCC’s reporting requirements.

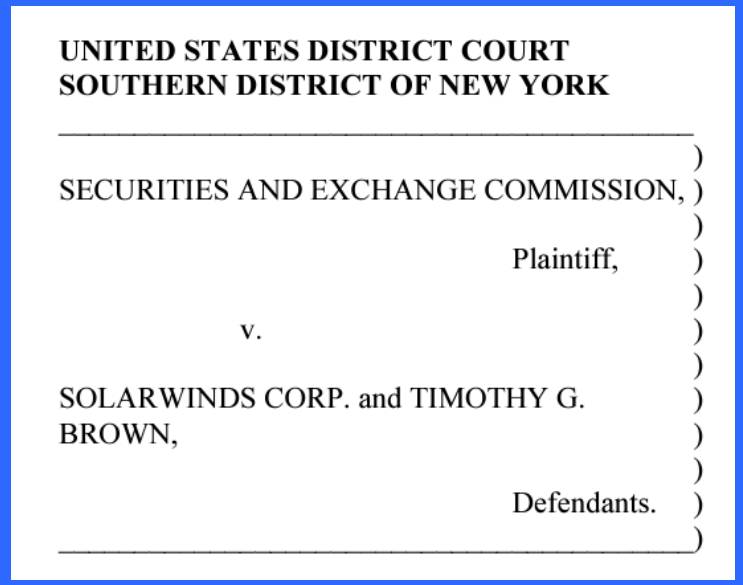
SEC Enforcement Update

03

Patterns from Recent Investigations + Enforcement Actions

- **SEC's Aggressive Stance in Investigating Cybersecurity Incidents**: In these investigations, the SEC has made demands for **potentially privileged information and documents**, including:
  - Inputs and substance of materiality determinations;
  - "Worksheets" or outputs of materiality determinations; and
  - Information and work product from investigations conducted following an incident, even when such investigations occur at the direction of counsel.
- **Recent Enforcement Orders**: The SEC's recent published enforcement orders concerning cybersecurity disclosures have focused on the efficacy of cybersecurity disclosure controls and procedures, especially where **personal information is compromised** without appropriate remediation, escalation, and disclosure.
  - Enforcement action against a real estate settlement services company involved real property-related data, which could contain personal information, such as social security numbers and financial information.
  - Enforcement action against a public company that provides educational publishing and other services to schools and universities involved private data on students, including dates of birth and email addresses.
  - Enforcement action against a public company that manages donor data for non-profits involved unencrypted bank account and social security numbers.
  - Enforcement action against a global provider of business communication and marketing services involved client data, some of which contained personal identification and financial information.

Case Study: The SEC Complaint against SolarWinds and its CISO



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,

Plaintiff,

v.

SOLARWINDS CORP. and TIMOTHY G. BROWN,

Defendants.

Significant SEC activity spurred by December 2020 SolarWinds incident:

- **Inquiry into SolarWinds:**
  - SolarWinds disclosed that the SEC issued Wells notices recommending an enforcement action against SolarWinds and certain current and former SolarWinds executives, including their CFO and CISO.
  - SEC charged SolarWinds and the company's CISO on October 30, 2023 with securities fraud and internal control failures, alleging the company misled investors about its cybersecurity practices and known risks
  - This is the first time an **individual executive has been charged** with a violation of securities laws based on disclosures related to cybersecurity.
- **Industry sweep:**
  - The SEC's inquiry into companies that were potential victims of the cyberattack that compromised SolarWinds Orion demonstrates that companies are under a real threat of **arbitrary enforcement-related investigations**, including attempts by the SEC to **second-guess the response to cybersecurity incidents**.
  - The Staff's initial voluntary request was sent to hundreds of companies across varying industries, and the Staff continued to investigate a smaller subset of companies for years after its initial outreach.
- **Impact:**
  - The SEC complaint and the industry sweep demonstrate a heightened level of scrutiny and aggressiveness by the SEC as it relates to cybersecurity.
    - This is particularly important given the implementation of the 2023 Rule.

SolarWinds: Case Update

On July 18, 2024, the U.S. District Court for the Southern District of New York **largely granted SolarWinds' motion to dismiss** and dismissed most of the SEC's claims against the company and its former Chief Information Security Officer (CISO).

Fraud and False and Misleading Statements

- The court **dismissed most of the claims advanced by the SEC relating to its disclosures**, including SolarWinds' Form 8-K filings, but did **sustain claims** against SolarWinds and its CISO alleging that a **"Security Statement"** posted on its website in 2017 may have been false or misleading.

- The court only allowed the SEC to proceed with claims where the court saw a basis in the arguments that the company, and/or the CISO, had knowledge that public statements were inaccurate at the time that they were made.

    - **The Security Statement:** The court found that the **SEC adequately pled** that the Security Statement posted on SolarWinds' website **contained materially misleading and false representations** as to at least two of SolarWinds' cybersecurity practices: access controls and password protection policies.

    - **Press Releases, Blog Posts, and Podcasts:** The court **dismissed** the SEC's claims that SolarWinds made false and misleading statements related to the 2020 incident in press releases, blog posts, and podcasts explaining that each qualifies as non-actionable corporate puffery.

    - **Pre-Incident Public Filings:** The court **dismissed** each of the SEC's claims that SolarWinds' cybersecurity risk disclosures in its SEC filings did not accurately reflect the risks that the company faced, finding that the risk disclosures sufficiently alerted the investing public of the cybersecurity risks SolarWinds faced and their attendant consequences.

    - **Post-Incident Form 8-K:** The court found that the **SEC did not adequately plead** that the post-incident Form 8-K was materially false or misleading, because the 8-K disclosed the known facts and the information required for reasonable investors.

SolarWinds: Case Update

On July 18, 2024, the U.S. District Court for the Southern District of New York **largely granted SolarWinds' motion to dismiss** and dismissed most of the SEC's claims against the company and its former Chief Information Security Officer (CISO).

Internal Accounting Controls

- The court found that the SEC's **attempt to regulate an issuer's cybersecurity controls through its authority to regulate an issuer's "system of internal accounting controls"** under Section 13(b)(2)(B) of the Exchange Act was **"not tenable,"** and unsupported by the statute, legislative intent, or precedent.
    - The court held that the statute cannot be construed to broadly cover all systems public companies use to safeguard their valuable assets and that the statute's reach is limited as it governs systems of "internal *accounting* controls."
    - In a separate cybersecurity-related case, the SEC entered into a settlement in June 2024 (one month before the court's SolarWinds ruling), on the basis that internal accounting controls-related regulations could encompass traditional IT assets that were unrelated to financial systems or financial/accounting data.
    - The court's SolarWinds decision poses a **significant challenge to the SEC's recent attempts to adopt an expansive reading of its rules relating to internal accounting controls to govern cybersecurity controls**—whether or not such cybersecurity controls are relevant to the production of financial reports.

SolarWinds: Case Update

On July 18, 2024, the U.S. District Court for the Southern District of New York **largely granted SolarWinds' motion to dismiss** and dismissed most of the SEC's claims against the company and its former Chief Information Security Officer (CISO).

Disclosure Controls and Procedures

- The court sided with SolarWinds in rejecting the SEC's claims that the company failed to maintain and adhere to appropriate disclosure controls for cybersecurity incidents. The court was unwilling to accept the SEC's argument that one-off issues—even if the company misapplied its existing disclosure controls in considering cybersecurity incidents—gave rise to a claim that the company failed to maintain such controls.
    - The court acknowledged that SolarWinds had misclassified the severity level of two incidents under its Incident Response Plan (IRP) and failed to elevate a vulnerability to the CEO and CTO for disclosure
    - Without more, these instances did not support a claim that SolarWinds maintained ineffective disclosure controls.
- The decision also calls into question the SEC's ability to rely on claims of inadequate disclosure controls and procedures in similar circumstances, given that the court found that more than a single disclosure failure is required to put the adequacy of a company's disclosure controls and procedures in issue.
- While this fact-based finding provides reassurance that good-faith, day-to-day mistakes at a company may not be actionable, it remains important to design and maintain disclosure controls that provide for appropriate escalation and consideration.

Practical Applications

04

Impact of the Adopted Rule: Practical Application

Key Areas of Focus

Key Areas of Focus:

1. Ensuring that cybersecurity incident response playbooks facilitate appropriate escalation and reporting.
2. Revisiting cybersecurity processes and governance to align with the expectations expressed in the SEC's final rules.
3. Drafting and balancing of competing interests for Form 10-K cybersecurity disclosures.
4. Preparing for an incident: effective cybersecurity incident response and materiality assessments will require advance planning.
5. Responding to a cybersecurity incident.
6. Making a disclosure on Form 8-K in connection with a cybersecurity incident.
7. Preparing for an SEC investigation.

Impact of the Adopted Rule: Practical Application

Review Cybersecurity Incident Response Playbook, Materiality Assessment Framework, Escalation Protocols

1. Ensure that cybersecurity incident response playbooks will facilitate appropriate escalation and reporting:

- Disclosure controls and procedures should provide for effective communication between the relevant internal teams.
- Companies should ensure that disclosure controls and procedures reflect the relevant materiality considerations, including inputs to consider potential reputational harm and damage to customer and vendor relationships.
- Consideration should be given to documenting the materiality analysis and the reasonableness of the time that it takes to assess materiality.
    - Given the accelerated timeline for disclosure of cybersecurity incidents on form 8-K within four business days of determining the incident is material, Companies should evaluate current evaluation and response procedures to ensure that a materiality determination can be made, and that a timely disclosure can be filed.

Practical Tip: Many IRPs are still primarily tailored to technical response—the 2023 cyber rules are requiring a substantive rethink for a number of public companies.

Impact of the Adopted Rule on Companies: Practical Application

Assess Processes for Managing Cybersecurity Risk

2. Companies may wish to revisit their cybersecurity processes and governance to align with the expectations expressed in the SEC's final rules:

- To avoid disclosing processes that lack features addressed in the final rule or that appear less robust than peers, companies should assess processes that will be disclosed.

- Specifically, companies should be aware of the need to describe engagement of third parties in connection with the risk management process, any processes to oversee and identify risks associated with use of third-party service providers, and the delegation of responsibility for cybersecurity risks between the board and management.

Consider incorporating AI utilization and technological developments in the assessment of cybersecurity risk.

Impact of the Adopted Rule on Companies: Practical Application

Careful Drafting of Disclosures and Coordination of New Form 10-K Disclosures with Existing Disclosures

3. Cybersecurity disclosures for Form 10-K will require careful drafting and balancing of competing interests:

- While some of the information now required to be disclosed has historically been disclosed to regulatory agencies and affected customers, the need to publicly disclose the information will subject such information to much greater scrutiny and potential liability as a result of possible regulatory enforcement or litigation.

- These disclosures will require careful drafting to balance the obligation to timely disclose material information (without material omission) while avoiding the unintentional exposure of weaknesses in a company's cybersecurity profile that could be further exploited by malicious actors.

Ongoing Considerations: Review existing disclosures when drafting new discussions for Form 10-K to maintain consistency with past public statements regarding cybersecurity governance and processes and to assess how those disclosures may be enhanced or revised going forward.

Impact of the Adopted Rule on Companies: Practical Application

Materiality determinations do not happen in a vacuum: preparation is key.

4. Preparing for an incident – effective cybersecurity incident response and materiality assessments will require advance planning:

- Create and maintain **documented incident response policies and procedures**, including an incident response plan (IRP), playbooks, contact lists, escalation procedures, and preferred vendor lists.
- Ensure **roles and responsibilities are clearly defined** (e.g., cybersecurity incident response team, incident response leader, legal, outside counsel, digital forensics firm, crisis communications firm, disclosure committee, etc.).
- Develop **a materiality assessment framework** that sets forth procedures to support the assessment of whether a cybersecurity incident is material.
- Regularly conduct **tabletop exercises to test response** and proactively make improvements to policies and procedures, as necessary. Note, it is critical that internal policies employed during an incident are drafted to be user-friendly.

Impact of the Adopted Rule on Companies: Practical Application

Action internal policies and procedures to help ensure a more cohesive and organized crisis response process.

5. Responding to a cybersecurity incident:

- Ensure that discussions about the cybersecurity incident and its materiality are **conducted under privilege and kept confidential**.
    - All communications regarding materiality should include a member of the Company's legal team and outside counsel. Written communications should be marked with "Privileged and Confidential—Prepared at the Direction of Counsel" headers.
    - Engagement of and communications with incident response vendors must be undertaken at the direction of and involve outside counsel.
- Establish an **out-of-band communications method** to be deployed if needed.
- Ensure **investigative activities are documented** by outside counsel and the Company's legal team.
- The materiality determination made by the disclosure committee should be documented by legal in a manner that demonstrates that the **determination was made in accordance with the materiality assessment framework**.
- Ensure that the **materiality assessment itself is conducted under legal privilege**; a non-privileged summary may be maintained for audit purposes.
- Conduct post-incident lessons learned exercises to enhance incident response preparedness materials.

Impact of the Adopted Rule on Companies: Practical Application

Be accurate and be prepared for the SEC to request more information.

6. Making a disclosure on Form 8-K in connection with a cybersecurity incident:

- **Exercise caution** not only in drafting initial 8-K disclosures, cybersecurity risk factors, and the new Item 106, but **also in any public statements regarding the company's cybersecurity practices.**
- **Confirm that assertions made or controls discussed do in fact presently apply to the full environment disclosed.** Any such disclosures or statements should be reviewed by both legal and cybersecurity leadership to confirm accuracy.
- **Materiality assessment procedures should consider whether the incident is part of a series of related incidents that are immaterial individually, but when viewed in the aggregate have a more significant impact.**
- Disclosures of incidents on Form 8-K should be consistent with the full set of facts known at the time.
  - Disclosures should make clear if there is a known connection to prior attacks.
  - Disclosures about alignment with recognized industry cybersecurity standards should be accurate and note any control gaps or other limitations.
- Be prepared to provide sufficient detail about the material impacts and materiality assessment process

Impact of the Adopted Rule on Companies: Practical Application

Preparing for an SEC Investigation

7. Preparing for an SEC Investigation:

What might an SEC investigation reasonably focus on?

- There is no way to predict which cybersecurity incidents will become the focus of future SEC enforcement investigations. However, companies can reasonably expect that an SEC inquiry will follow either:
  - The disclosure of a cybersecurity incident, or
  - Non-disclosure of a cybersecurity incident the SEC believes may have impacted the company, such as after a publicly reported incident believed to impact a range of entities.
- The SEC will also likely focus on the procedures and documentation associated with materiality determinations.

What might the SEC request?

- Inputs and substance of materiality determinations;
- "Worksheets" or outputs of materiality determinations; and
- Information and work product from investigations conducted following an incident, even when such investigations occur at the direction of counsel.
- Information regarding whether and how the company's "disclosure decision-makers" were provided with information regarding cybersecurity incident.

Impact of the Adopted Rule on Companies: Practical Application

Preparing for an SEC Investigation

7. Preparing for an SEC Investigation (Continued):

How can companies best prepare?

- **Companies should create a process for integrating cybersecurity and disclosure functions.**
  - Companies should institute processes for: (1) determining which cybersecurity incidents need to be escalated to the company's "disclosure decision-makers"; and (2) ensuring that the right information is provided in a timely manner.
  - The best defense remains implementing and adhering to a well-documented, tightly reasoned process grounded in actual legal standards.
- **When investigating a cybersecurity incident, companies should ensure processes are in place to protect privilege.**
  - Companies should institute thoughtful privilege protocols to determine what information is disclosed to whom.
  - When establishing engagements with incident response providers, such as forensic investigators, careful consideration should be given towards establishing and protecting appropriate privileges.

GIBSON DUNN