SEC Cybersecurity Enforcement After *SolarWinds*

Marc Adesso – Baker Botts L.L.P.
Sarah Dodson – Baker Botts L.L.P.
Rich Sowalsky – Centri Business Consulting, LLC

BAKER BOTTS

Table of Contents

SEC V. SOLARWINDS: BACKGROUND 01

BAKER BOTTS

SEC v. SolarWinds

Background

- SolarWinds suffered a large-scale cyberattack in December 2020
  - Known to be "the largest and most sophisticated attack the world has ever seen."
  - Attackers accessed customer networks, including federal agencies (eg, NSA) and major corporations (eg, Microsoft), and exploited vulnerabilities in the software supply chain.
- In October 2023, SEC filed a lawsuit against SolarWinds and its Chief Information Security Officer (CISO), alleging they defrauded investors by hiding cybersecurity weaknesses during the hack.
  - SEC's first case against a public-company CISO
    - Security professionals concerned that they could face personal liability for their role in flagging potential safety issues.

Complaint Overview

- SolarWinds and its CISO are named defendants in which the SEC alleges they made materially false statements about their information security:
  - In a Security Statement on SolarWinds' website
  - In publicly filed Forms S-1 and 10-K and 10-Q
  - In the Forms 8-K filed after the December 2020 disclosure of the security vulnerability
- SEC alleges SolarWinds' violations are based on representations about:
  - Secure development lifecycle
  - Password management
  - Least access privilege
- Controls violations
  - Internal Control over Financial Reporting
  - Disclosure Controls and Procedure

Closer Look at Public Disclosures

- SEC alleged that SolarWinds made materially false statements about its information security:
  - **Website** (*pre-attack*)
    - Security statement claimed SolarWinds followed security standards published by NIST; SEC said internal communications showed that was untrue

> 5. The Security Statement was materially misleading because it touted the Company's supposedly strong cybersecurity practices. For example, that statement asserted that SolarWinds created its software products in a "secure development lifecycle [that] follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments." And the Security Statement claimed that SolarWinds' "password policy covers all applicable information systems, applications, and databases [and we] enforce the use of complex passwords." It also stated that SolarWinds had "[a]ccess controls to sensitive data in our databases, systems, and environments [that are] set on a need-to know / least privilege necessary basis." All those statements were materially false and misleading.

> 45. SolarWinds' Security Statement contained multiple materially false and misleading statements, assuring the public that SolarWinds followed well-recognized cybersecurity practices when, in reality, the Company's cybersecurity practices fell significantly short of those standards. The Security Statement also omitted information necessary to make the information included, in light of the circumstances, not misleading. The false statements and omissions in the Security Statement fall into four general categories: (1) compliance with the NIST Framework for evaluating cybersecurity practices; (2) using a secure development lifecycle when creating software for customers; (3) having strong password protection; and (4) maintaining good access controls.

Closer Look at Public Disclosures cont'd

- **Forms S-1 and 10-K and 10-Q** (*pre-attack*)
  - SEC accused SolarWinds of omitting known cybersecurity risks, instead relying on generic statements about potential cybersecurity risks

> ***"If we sustain system failures, cyberattacks against our systems or against our products, or other data security incidents or breaches, we could suffer a loss of revenue and increased costs, exposure to significant liability, reputational harm and other serious negative consequences."***

134. Despite internally documenting all the cybersecurity issues and problems discussed above, and despite multiple internal warnings about their severity, SolarWinds neither specifically disclosed the issues nor generally disclosed that known, unremediated issues with NIST compliance, SDL, access controls (including the known VPN vulnerability), or passwords existed. Nor did SolarWinds even disclose Brown's assessment that it was "very vulnerable" to a cyberattack. As a result, SolarWinds' October 18, 2018 Form S-1—and especially the risk disclosure quote above—was materially misleading.

Closer Look at Public Disclosures cont'd

- **Form 8-K** (*post-attack*)
  - The cyber attack "could potentially allow" a data comprise when it allegedly knew its server was compromised
  - It was investigating *whether* a vulnerability was exploited when SolarWinds *knew* a vulnerability was exploited at least three times

"[SolarWinds] has been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, **could potentially allow** an attacker to compromise the server on which the Orion products run….SolarWinds has retained third-party cybersecurity experts to assist in an investigation of these matters, including **whether a vulnerability in the Orion monitoring products was exploited** as a point of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans."

"SolarWinds' investigations into these matters are preliminary and on-going, and SolarWinds is still discerning the implications of these security incidents. During the course of these investigations, SolarWinds may become aware of new or different information. At this time, SolarWinds is unable to predict any potential financial, legal or reputational consequences to the Company resulting from this incident, including costs related thereto. So as not to compromise the integrity of any investigations, SolarWinds is unable to share additional information at this time."

THE COURT'S RULINGS 02

BAKER BOTTS

SEC v. SolarWinds: Outcome

- The Court dismissed much, but not all, of the SEC's case against SolarWinds
  - It emphasized that the sufficiency of a company's cybersecurity disclosures cannot be judged by hindsight and must consider the information known at the time
    - May have implications for how the SEC will approach cyber incident litigation against corporate defendants moving forward
- The Court agreed with some of the SEC's pre-attack claims but rejected its allegations regarding post-attack disclosures and internal accounting controls
- Will the parties settle? Litigate? Appeal?
  - Much we don't know

Pre-Attack Claims

- No fraud about the company's risk profile disclosures in its filings
- SEC adequately pled a securities fraud claim based on a "Security Statement" posted on SolarWinds' website pre-Sunburst attack
  - False statements on public websites can sustain securities fraud liability
- Representations about its access controls and password protection policies were materially misleading
  - SolarWinds was "routinely promiscuous" in granting administrative rights to employees and its stated password policy was generally not enforced
- Discovery proceeds only on the Security Statement allegations
- CISO still in the case for his role in drafting Security Statement

Post-Attack Disclosures

- The Court **rejected** the SEC's allegations that SolarWinds' Form 8-K disclosures post-Sunburst attack were materially misleading
  - The court emphasized that SolarWinds made these disclosures at an early stage of its investigation when its understanding of the attack was still evolving
  - The lengthy Form 8-K disclosure captured the severity of the Sunburst attack and provided a comprehensive overview given the information at the time
- The Court also **rejected** the SEC's theory that SolarWinds failed to devise and maintain a system of "internal accounting controls" to cover cybersecurity controls
  - The term "accounting" refers to ***financial accounting***, not every internal system used to guard against unauthorized access

IMPLICATIONS 03

BAKER BOTTS

In Response to *SolarWinds*

- SEC amended Regulation S-P to heighten protections for nonpublic consumer information held by B-Ds, investment companies, RIAs, and TAs
- SEC's approach to cybersecurity-related disclosures and internal controls is evolving
- SEC is focusing on ensuring that companies are transparent about their cybersecurity practices and risks
- "Next case" likely to be litigated against the backdrop of the new SEC rules

Investor Concerns

- Greater scrutiny regarding cybersecurity practices of companies that they invest in
- Heightened awareness of potential financial and reputational damage stemming from inadequate cybersecurity measures
- Emphasis on transparency and disclosure of cybersecurity risks
- Expectation of detailed information about company's cybersecurity policies, procedures, and incidents

Corporate Governance

- Companies must implement comprehensive risk management frameworks
  - Address cybersecurity threats
  - Establish clear lines of communication to report information timely and accurately
- Boards of directors must ensure robust cybersecurity policies and procedures are in place
  - Regular assessments of cybersecurity risks
  - Prompt responses to any identified vulnerabilities or incidents

For CISOs

- In *SolarWinds*, CISO is potentially liable as the primary author of a public company statement, not as a result of his status as CISO, nonetheless CISOs are directly and personally in the crosshairs of the SEC
  - Possibility of being fined personally and prevented from ever holding a senior position within any public company
  - Significant financial consequences
- As a result, CISOs may spearhead training programs with clear guidelines to mitigate cybersecurity risks
- CISOs will seek paid legal fees and indemnification in employment agreements (or separate indemnification agreements altogether)
  - Companies may need to review D&O insurance coverage to determine if CISOs are covered in the event of a regulatory investigation or litigation
- CISOs will benefit from clear and effective communication with senior management about cybersecurity responsibilities

Public-Company Trends Since SEC Disclosure Rule Became Effective

- Reporting companies appear to be more likely to disclose
  - Even if they later determine there was no material impact from the cybersecurity incident
- Initial disclosures are brief and generic
  - No exact numbers and systems impacted are vaguely described
- Initial filings may read like high-level press releases
  - Companies usually state they have taken actions to contain, assess, and remediate the incident
- Updated disclosures
  - Almost half of the companies that have filed 8-K cybersecurity disclosures have updated their initial filings with slightly more information and an update on whether the investigation is closed

RECOMMENDED ACTIONS FOR PUBLIC COMPANIES 04

BAKER BOTTS

Immediate Actions

- Any public company statement that can influence investors can create risk; review material on company website carefully (especially by SEC disclosure team)
- Companies should consider reviewing all public statements about their security posture to make sure they are supported by the evidence, including customer agreements.
- Court credited company for disclosing what it actually knew in an evolving situation. Consider whether and when to amend/update Form 8-K to disclose any information unavailable or later found to be incorrect at the time of the initial filing.
- Regular training around what is appropriate to say in an email or on a Teams chat.
- Secure lines of communication between functional areas v. business units.

Recommended Actions for Public Companies

- Regular Risk Assessments
  - Conduct regular risk assessments to identify and address vulnerabilities in the IT infrastructure
    - Assessments should evaluate effectiveness of existing security measures and identify areas for improvement
- Advanced Security Technologies
  - Invest in advanced security technologies such as multi-factor authentication, encryption, and intrusion detection systems to enhance security and protect against data breaches
- Employee Training
  - Train employees on cybersecurity awareness and best practices to avoid phishing attacks and other social engineering tactics

Recommended Actions for Public Companies

- Regulatory Compliance
  - Ensure compliance with relevant data protection regulations and institute applicable organizational safeguards
  - Stay informed about regulatory landscape changes and adjust processes accordingly
- Incident Response Planning
  - Develop and regularly update an incident response plan
    - Consider requiring quarterly 10-Q report updates to be part of the plan
  - Include four business-day requirement for filing an 8-K after identifying a material cybersecurity incident
- Board Oversight
  - Assign a Board committee to oversee cybersecurity risk with members that have sufficient background (optional disclosure of board cybersecurity credentials)
  - This can help ensure appropriate resources are allocated to addressing cybersecurity threats

Recommended Actions for Public Companies

- Vendor Management Program
  - SEC has ramped up its focus on the risks of third-party service providers
    - Companies should be prepared to show careful vetting in the selection of service providers
- Business Continuity Plan
  - Develop a business continuity plan that incorporates cyber risks
- Form 8-K Disclosures
  - Only disclose any **material** cybersecurity incident within four business days of the determination that the incident is material
    - In assessing materiality, companies should determine *if the incident is likely to impact the financial condition of the company and/or results of its operations*
- Form 10-K Cyber Risk Disclosures
  - Create a checklist for 10-K cyber risk disclosures with specific goals for providing sufficient information for investors to make an informed decision

Disclosure of Material Cyber Incidents

05

BAKER BOTTS

Disclosure of Material Cyber Incidents

SEC Requirements (1/2)

- **Form 8-K, Item 1.05:** public companies must disclose via Form 8-K any **material cybersecurity incidents** within **four business days** of determining that the cybersecurity incident is material.

- **July 2024 C&DIs:**
  - Completed attacks don't absolve materiality determination
  - Insurance reimbursement doesn't absolve materiality
  - Amount/size of ransomware payment isn't determinative of materiality
  - Aggregate of immaterial events could become material
    - Item 106(a) of Regulation S-K includes "a series of related unauthorized occurrences"

Disclosure of Material Cyber Incidents

SEC Requirements (2/2)

- **Should Disclose:**
  - Nature of incident (e.g., phishing, malware, misconfiguration, ransomware)
  - Scope of incident (e.g., operations impacted, customers impacted, data impacted)
  - Timing of incident (e.g., discovery date, whether ongoing)
  - Material impact or reasonably likely material impact on the company

- **Should Not Disclose:** specific or technical information about incident response, systems, networks, or potential vulnerabilities in so much detail that it would impede incident response

Disclosure of Material Cyber Incidents

What Constitutes "Material"?

- Companies should consider **"qualitative factors"** in assessing a cyber incident's material impact

- **Examples include:**
  - Amount and sensitivity of data impacted
  - Operational impact (e.g., downtime)
  - Financial impact (e.g., lost profits, lost customers, cost to remediate)
  - Reputational impact (e.g., customer or business partner relationships)
  - Physical impact (e.g., to facilities or infrastructure)
  - Potential for litigation or government enforcement

- Note: materiality will look different for each company. **Create your own threshold test.**

Disclosure of Material Cyber Incidents

Timing of Determination

- Companies must determine materiality **"without unreasonable delay"**
  - SEC lessened this from "as soon as reasonably practical" to avoid pressuring conclusions with insufficient info
  - There may still be instances where a company has incomplete info and yet knows enough to determine materiality, such that the timer begins (e.g., impact to key systems, unauthorized access of much sensitive data)

- Importantly, **date of materiality determination ≠ date of incident discovery**
  - "… in the majority of cases, registrants will have had additional time leading up to the materiality determination, such that disclosure becoming due less than a week after discovery should be uncommon."

- **Examples of unreasonable delay:**
  - Deferring Board of Directors cyber oversight committee meetings past the normal time
  - Revising existing IRP protocol to support a delayed materiality determination of an ongoing cyber event

Disclosure of Material Cyber Incidents

8-K Amendment

- If a company determines materiality but **does not yet have complete information** regarding an incident's nature, scope, timing, and reasonably likely material impact within four days, it must:

1. **Investigate** that information without unreasonable delay
2. **File an 8-K amendment** within four business days of the info being determined/becoming available

Disclosure of Material Cyber Incidents

National Security Exception

- **Exception:** a company may delay disclosure of a material cyber incident by 30 days if:
  1. The company notifies the U.S. Attorney General of the incident and requests a 30-day delay
  2. The U.S. Attorney General determines that immediate disclosure **"would pose a substantial risk to national security or public safety"**
  3. The U.S. Attorney General **notifies the SEC** of such determination in writing

- The U.S. Attorney General can also argue that further delay is necessary beyond the 30 days, and the SEC will consider such request

- **Considerations for this exception:**
  - This is a fairly high bar / narrow exception
  - It may be difficult to get the U.S. Attorney General to respond within the short four-day timeframe

Disclosure of Material Cyber Incidents

Best Practices

1. **Update your IRP** to include steps like: conducting materiality analysis, contacting the U.S. Attorney General (if applicable), and drafting/filing a Form 8-K

2. Develop a **custom threshold materiality test** and add it to your IRP
   - Consider the qualitative factors most impactful to your company based on its unique size, industry, relationships, and business model. If you already have a severity matrix, that is a great roadmap.

3. **Optimize communication channels** between teams to avoid "unreasonable delay"

4. **Proactively draft communication templates** for 8-K disclosure, 8-K amendment, and U.S. Attorney General letter to be quickly deployed during an incident
   - Disclosures should be carefully drafted to balance timely disclose while not unintentionally exposing weaknesses in your company's cybersecurity profile

5. During an incident, **carefully document:** a) your team's materiality analysis and b) reasonableness of the time it took your team to determine materiality

Annual Disclosure of Cyber Risk and Governance

06

BAKER BOTTS

Annual Disclosure of Cyber Risk and Governance

SEC Requirements

- **Regulation S-K, Item 106(c)(2):** public companies must disclose via Form 10-K their cybersecurity risk management, strategy, and governance.

- Specifically, they must disclose:
  - **Board's role** in overseeing cyber threats (including specific cyber oversight committees, if applicable)
  - **Management's role** in managing cyber threats (including specific positions/committees)
  - Each management position/committee's **specific expertise** in managing cyber threats
  - Processes by which…
    - Management **assesses, identifies, and manages** material cybersecurity risks
    - Management positions/committees are **informed of and monitor** prevention, detection, mitigation, and remediation
    - Board/cyber oversight committee is **notified** of cyber risks
  - Whether **assessors, consultants, auditors, or other third parties** are engaged for such processes
  - Whether processes exist to identify **cyber risks of third-party service providers**
  - Whether and how any cyber threats (including previous incidents) have materially affected the company

Annual Disclosure of Cyber Risk and Governance

Not Required to Disclose

- A company does **not** need to disclose in its 10-K:
  - Specific **cyber policies and procedures** (just high-level processes)
  - Specific **risk types** (e.g., intellectual property theft, fraud, etc.)
  - Specific activities to **prevent, detect, and minimize damage** of cyber incidents
  - **Business continuity, contingency, and recovery plans**
  - Whether the company has a **CISO** (unless this is the specific position responsible for managing cyber incidents)
  - Frequency of the Board's discussions or management's reporting on cyber risk
- These were intentionally excluded from the final SEC cyber rules, to preserve details that could be taken advantage of by a threat actor and thereby increase a company's vulnerability profile

Annual Disclosure of Cyber Risk and Governance

Other Considerations

- Cybersecurity considerations for Regulation S-K sections in 10-K:
  - Significant Risk Factors
  - Management's Discussion and Analysis
  - Description of Business
  - Legal Proceedings
- Financial Statement impact
- Anti-fraud Provisions
  - Exchange Act Section 10(b)/Exchange Act Rule 10b-5

Annual Disclosure of Cyber Risk and Governance

BEST PRACTICES

1. **Identify the management position/committee** in charge of managing cyber threats
   - Ensure individual(s) have sufficient expertise and **document that expertise**

2. Assess your **Board structure for cyber risk oversight** and consider creating a committee

3. Assess your processes for **how to inform** management positions and the Board of cyber threats

4. Assess your processes for **prevention, detection, management, mitigate, and remediation**

5. Proactively draft **description of your cyber risk and governance** for 10-K disclosure
   - This will likely require coordination between various internal teams and the Board

6. Assess your **third-party service providers**—including their cybersecurity processes and your communication channels with each in the event of a cyber incident
   - There is no requirement that a material incident must occur on a company's *own* systems for it to be a required disclosure. You must therefore understand your third parties' cyber risks and how best to obtain incident info.

ANY QUESTIONS?

Marc Adesso – marc.adesso@bakerbotts.com

Sarah Dodson – sarah.dodson@bakerbotts.com

Rich Sowalsky – rsowalsky@centriconsulting.com

AUSTIN
BRUSSELS
DALLAS
DUBAI
HOUSTON
LONDON
NEW YORK
PALO ALTO
RIYADH
SAN FRANCISCO
SINGAPORE
WASHINGTON

bakerbotts.com