Insights on Cybersecurity

4:40 PM – 5:20 PM, April 17, 2024

Changing Seasons: SEC's SolarWinds Complaint Demonstrates Regulator's Aggressive Enforcement on Cybersecurity

- Summary of Individual Charges
- 2020 SUNBURST Supply Chain Cybersecurity Attack
- The SEC's Allegations
- Lessons Learned

Summary of Amicus Brief on Behalf of CISO Community in SEC v. SolarWinds (filed by Freshfields)

- CISOs know there is an inherent level of risk in cybersecurity
- The SEC is sending CISOs conflicting messages on public disclosure obligations
- The SEC's position risks chilling internal discussions and self-assessments in the private sector
- This litigation comes amid a critical shortage of cybersecurity professionals
- The Court must consider the importance of public-private cooperation

SEC Adopts Cybersecurity Disclosure Rule

- Incident Reporting
- Risk Management, Strategy & Governance Disclosures
- Effect on Foreign Private Issuers
- Timeline for Compliance

What Companies Need to Know Heading into the 2024 Proxy Season

- Cybersecurity Risk Oversight
- Material Weakness
- Incident Response Takeaways

White House Releases Roadmap for Increased Cybersecurity Regulation

- Shifting Liability to Private Actors
    - A new liability framework for software products and services (Initiative 3.3.1)
    - Software bill of materials (SBOM) (Initiative 3.3.2)
    - Federal procurement (Initiatives 3.5.1 and 3.5.2)
- Compulsory Federal Standards for Tech and Critical Infrastructure
    - Critical infrastructure security (Initiative 1.1.2)
    - Infrastructure-as-a-Service security (Initiative 2.4.1)
    - CIRCIA (Initiative 1.4.2)

Freshfields

November 8, 2023 | 4 minutes read

Changing Seasons: SEC's SolarWinds Complaint Demonstrates Regulator's Aggressive Enforcement on Cybersecurity


Brock Dahl
Partner


Timothy Howard
Partner


Pamela Marcogliese
Partner

+3 more...

Introduction

Recently, the Securities and Exchange Commission ("SEC") filed a complaint in the Southern District of New York against the SolarWinds Corporation, a network and infrastructure management company, and also named the company's Chief Information Security Officer as an individual in the action. The SEC's complaint alleges that the defendants defrauded investors and customers through internal control failures, as well as a series of misstatements, omissions, and schemes that obscured SolarWinds' deficient cybersecurity practices and the cybersecurity threats it was facing.

The SEC alleges the disclosure deficiencies violated the antifraud provisions of the Securities Act of 1933 and of the Securities Exchange Act of 1934, and the control failures violated the reporting and internal control provisions of the Exchange Act. Finally, while the SEC has recently issued cybersecurity rules that will come into effect in December, these allegations are all founded on existing regulations that do not invoke the requirements of the new rules. We summarize the case below and suggest a number of precautions companies can take in contemplation of this more aggressive SEC posture regarding cybersecurity compliance.

Individual Charges

Notably, the SEC charged not only SolarWinds, but also charged its Chief Information Security Officer, Timothy Brown, with aiding and abetting the alleged corporate violations. During the relevant time period, Brown was the company's Vice President of Security and Architecture and head of its Information Security group. In these roles, Brown was responsible for both SolarWinds' ongoing security efforts and the security architecture within its products.

2020 SUNBURST Supply Chain Cybersecurity Attack

In 2020, SolarWinds disclosed that it had been the victim of a major supply chain cyberattack, now known colloquially as the SUNBURST attack. The attack, widely attributed to Russian state-sponsored hackers, was carried out by accessing SolarWinds' virtual private network ("VPN") through an unmanaged device neither owned nor operated by the company. Using this undetected access, hackers inserted malicious code into software for the SolarWinds' signature Orion products. These products were then delivered to more than 18,000 customers globally, allowing hackers to obtain unauthorized access to the systems of some customers.

The SEC's Allegations

In detailing the Defendants' alleged wrongful conduct, the SEC alleges a series of actions and omissions, from at least its initial public offering in October 2018 through at least January 12, 2021, to defraud investors. These allegations include purportedly:

- **Ignoring Serious Known Cybersecurity Deficiencies:** the SEC alleged that Brown and other SolarWinds employees knew of serious cybersecurity deficiencies according to internal emails, messages, and documents. These included not developing Orion and other company products in a secure development lifecycle and not addressing access control deficiencies including permitting access to SolarWinds' VPN by unmanaged devices and inadequately stringent password practices.
- **Making Materially False and Misleading Risk Disclosures in SEC Filings:** SolarWinds filed numerous SEC registration statements, forms, and periodic reports that the SEC characterizes as containing inadequate disclosures. The SEC singles out that repeated disclosures of hypothetical, generalized descriptions of cybersecurity risk were insufficient where a company has in fact experienced events and cyberattacks and was aware of known vulnerabilities to its products. The SEC further emphasizes that Brown repeatedly signed sub-certifications representing that all material incidents had been disclosed to company executives responsible for its securities filings while being aware of numerous documented cybersecurity failures. Sub-certifications are not required by any SEC rule or regulation but are used by many companies to assist the company's CEO and CFO in giving their SEC-required certifications of the company's disclosure.
- **Posting Misleading Statements on the SolarWinds Website:** During the relevant period, SolarWinds maintained a Security Statement on its website that articulated cybersecurity practices which the SEC alleges contradicted its internally known practices and deficiencies.

- **Permitting Multiple Internal Control Failures:** The SEC also alleges that SolarWinds lacked sufficient internal accounting controls, failing to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that . . . access to assets is permitted only in accordance with management's general or specific authorization." The complaint further alleges that SolarWinds lacked sufficient safeguards to protect against and detect unauthorized access and appropriate controls to ensure that information regarding potentially material cybersecurity risks, incidents, and vulnerabilities was reported to executives responsible for disclosure.

This case represents the most aggressive posture the SEC has taken to date with respect to purported cybersecurity-related disclosure deficiencies and individuals it asserts were personally liable for those deficiencies.

Lessons Learned

The SEC's complaint against SolarWinds and Brown underscores its interest in companies' cybersecurity practices and disclosures and the individual responsibility that certain executives bear for such practices and disclosures. While the SEC's position remains subject to adjudication, the allegations provide important insights for SEC-registered companies to consider in managing their cybersecurity obligations.

- **The SEC is Prioritizing Cybersecurity Enforcement:** While many might think of insider trading or securities fraud as the usual purview of the SEC, the recent charges and the new cybersecurity rules highlight that the SEC is making cybersecurity a regulatory and enforcement priority. Companies should carefully evaluate their cybersecurity resourcing and governance to reflect this heightened focus. This should include prioritizing executive and board awareness of industry standard cybersecurity practices, consciously evaluating and

documenting resourcing requirements and decisions, and adopting appropriate processes for evaluating and, if appropriate, disclosing cyber events and deficiencies.

- **Accurate Disclosure is Key:** Companies may do well to continuously assess their risk disclosure practices and consciously account for past, material incidents and material vulnerabilities as they do so. Perhaps the most challenging aspect will be understanding the thresholds for considering events and vulnerabilities for inclusion in SEC reporting and the SEC's latest action highlights the value of having defensible processes to support disclosure determinations.
- **Individual Executives Should Be Cognizant of their Responsibilities:** Individual executives and directors, especially those in management positions with oversight of cybersecurity matters, may have legal obligations to respond to, address, assess, and disclose certain cybersecurity-related events and vulnerabilities. They should seek to establish and maintain frameworks designed to promote the reporting up of cyber incidents so that executives and other responsible individuals can be responsive to cybersecurity issues and the company can comply with its disclosure obligations.
- **Mind Your Internal Controls:** As the SolarWinds complaint makes clear, it is imperative that companies attend to internal controls. There is a broadening awareness of market standard security practices that are an increasing expectation of regulators, customers, and the markets. It will be prudent to develop structured mechanisms for assessing and elevating issues pertaining to such controls for the awareness and decision-making of responsible management.

The key theme underlying all of these points is the value in companies' assessing how to support leadership with sufficient procedures to normalize incident and vulnerability assessment and merge those procedures with SEC reporting processes. The latest SEC action is likely to drive a focus on these priorities in the coming term.

Freshfields

February 5, 2024 | 4 minutes read

Freshfields Files Amicus Brief on Behalf of CISO Community in SEC v. SolarWinds


Timothy Howard
Partner


Beth George
Partner


Pamela Marcogliese
Partner

+3 more...

Last week, Freshfields and co-counsel Cooley LLP filed an amicus brief in *SEC v. SolarWinds*, No. 23-cv-09518 (S.D.N.Y. Oct 30, 2023) on behalf of Modern Fortis' Secure Policy Coalition, and other organizations and individuals that seek to promote the interests of the cybersecurity community and challenge the SEC's unprecedented theories of liability for companies and Chief Information Security Officers (CISOs).

As discussed in our prior blog post here, the SEC filed its complaint in October 2023 against both SolarWinds and Timothy Brown, the company's CISO, in connection with a 2020 Russian-state sponsored cyberattack that compromised the networks of more than 18,000 SolarWinds customers. The complaint alleges that Mr. Brown and SolarWinds made material misrepresentations and omissions that

"concealed both the Company's poor cybersecurity practices and its heightened—and increasing cybersecurity risks," which allegedly culminated in the 2020 attack. Despite the fact that the company disclosed the risk of cyberattacks and promptly reported the breach in an 8-K filing, the SEC cites various internal communications among Mr. Brown and others at the company—aimed at identifying and resolving cybersecurity issues—as evidence that he and SolarWinds concealed the company's cybersecurity deficiencies from investors.

This action is the first time the SEC has ever sought to hold a CISO personally liable for the content of public corporate disclosures. The outcome carries meaningful consequences for the cybersecurity ecosystem, not only in terms of how companies approach cybersecurity governance and disclosures, but also how they collaborate with government entities to prevent, identify, and control cyberattacks. With this in mind, the amicus brief aims to: (1) educate the Court about the complex risks that CISOs must balance on a daily basis, (2) highlight potential policy implications of imposing personal liability on CISOs, and (3) give voice to concerns within the CISO community about the uncertainties that SEC enforcement could introduce to their compliance efforts. The brief's key issues are summarized below.

CISOs know there is an inherent level of risk in cybersecurity. History and experience show that there is no such thing as perfect security against cyberattacks. As such, a robust cybersecurity program is not one that eliminates every possible risk, but one that promotes transparent communication, both internally and externally. Such communications enable CISOs and their teams to keep abreast of the latest cyber threats, identify vulnerabilities within their own organization, and triage risks using finite resources. In a dynamic environment where bad actors can bring the full weight of a foreign military intelligence operation to bear against a private company, government organizations and industry leaders agree that proper risk management is crucial.

The SEC is sending CISOs conflicting messages on public disclosure obligations. The SEC's attempt to regulate via enforcement action (beyond the requirements of their recently adopted rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure) risks creating substantial uncertainty as to the appropriate level of detail in public disclosures concerning a company's cyber practices and vulnerabilities. The SEC's theory of liability in this action presents CISOs with an impossible choice: either they over-disclose details about a company's security, thereby reducing the risk of personal liability but potentially providing threat actors with information that could be used in an attack; or they minimize the detail of public disclosures, thereby increasing the risk of personal liability but diminishing the chances of tipping off hackers. This potential conflict is all the more puzzling given that the SEC itself emphasized the importance of not providing a "roadmap for threat actors" in its response to public comments on drafts of the recently promulgated incident disclosure rule.

The SEC's position risks chilling internal discussions and self-assessments in the private sector. By citing internal communications among cybersecurity personnel concerning areas of improvement or instances of potential noncompliance with corporate security policies, the SEC risks discouraging the very efforts CISOs and others take to improve company security. In response to this lawsuit, cybersecurity personnel may be deterred from engaging in critical communications to assess and address risk, for fear that an internal email or presentation may be taken out of context and used to argue, via fraud-by-hindsight, that a CISO deliberately misled investors.

This litigation comes amid a critical shortage of cybersecurity professionals. While demand for cybersecurity employees has grown 200 percent in the last 10 years,[1] there remains a dearth of qualified candidates. The risk of personal liability for CISOs under the SEC's novel and aggressive legal theories will exacerbate companies' existing struggle to hire and retain talent.

The Court must consider the importance of public-private cooperation. The government relies on transparent communication both from and within the private sector in order to protect against cyber threats. If the SEC's claim proceeds, CISOs may fear that the information they provide to other companies or to the government in a good faith attempt to shore up national security and/or supply chain resilience will later serve as evidence that they failed to timely disclose to investors a known breach or vulnerability.

* * *

In short, the SEC's claims are novel and may have policy effects extending far beyond any single case. As the Court evaluates the complaint, it should consider the perspectives of cybersecurity personnel who serve as the front line of defense in a rapidly expanding arms race against sophisticated adversaries. Freshfields welcomes the opportunity to give CISOs and other cybersecurity professionals a voice at this crucial juncture in federal cyber regulation.

[1] *Growing the National Cybersecurity Talent Pipeline: Hearing Before the Subcomm. on Cybersecurity & Infrastructure Prot. of the H. Comm. on Homeland Sec.*, 118th Cong. 118-19, 15 (statement of Will Markow) (2023).

Freshfields

July 28, 2023 | 3 minutes read

SEC Adopts Cybersecurity Disclosure Rule


Brock Dahl
Partner


Timothy Howard
Partner


Pamela Marcogliese
Partner

+2 more...

On July 26, 2023, the Securities and Exchange Commission adopted new rules and amendments that enhance and standardize cybersecurity disclosure requirements for registrants and foreign private issuers. As previously illustrated in our June 2022 and March 2022 blog posts, the new rules require companies to disclose and describe material cybersecurity incidents and their impacts, in additional to annual disclosure of information about their cybersecurity governance, strategy, and risk management processes.

Incident Reporting. The Commission's new rules require all U.S. domestic reporting companies to disclose material cybersecurity incidents on the new item 1.05 of Form 8-K, generally within four business days of the company's determination that they experienced such an incident. Consistent with the standing definition of materiality within the securities regime, the rules explain that a

"material" incident is one in which "there is a substantial likelihood that a reasonable shareholder would consider it important."

Amending its March 2022 Proposal, the Commission will require registrants to disclose a narrower set of details on cybersecurity incidents, including:

- Material aspects of the nature, scope, and timing of the incident; and
- Material impact (or reasonably likely material impact) of the incident on the registrant, including its financial condition and results of operations.

However, per the final rule, disclosures regarding an incident's remediation status will not be required. Moreover, contrary to the proposed rule, companies will not be required to assess or report events that are material in the aggregate, which was a particularly challenging concept to interpret in the proposed rule.

Importantly, the rules require that materiality decisions be made "without unreasonable delay," a change from the initial proposal's requirement that a determination be made "as soon as reasonably practicable after discovery of the incident." The SEC intended this change to recognize that companies must have sufficient information on which to base the decision and acknowledged concerns that the prior formulation would result in hasty materiality assessments.

Unlike the proposed rule, the final rules provide for a delay for disclosures for up to thirty days if the "Attorney General determines that the incident disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing." While the Attorney General would likely delegate this authority, this is still a particularly burdensome requirement for the Department to act within such a time frame, and it remains to be seen what the practical effect of this authorized delay will be.

Risk Management, Strategy, and Governance Disclosures. In addition to incident reporting requirements, through Item 106, the new rules add further disclosure requirements to Form 10-K for domestic registrants. Registrants must furnish information on their approach to risk management, strategy, and governance concerning material cybersecurity threats on an annual basis. Registrants will be required to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats. Registrants must also disclose their board of directors' oversight of and management's role and expertise in assessing and managing risks from cybersecurity threats.

The final rules will also require disclosure of whether a registrant makes use of assessors, consultants, auditors, or other third parties in connection with their cybersecurity so that investors are aware of a registrant's level of in-house versus outsourced cybersecurity capacity. However, registrants will not be required to name or describe the services provided by third parties, though registrants may choose to furnish this information.

Foreign Private Issuers. In place of the reporting requirements contained in the updates to Forms 8-K and 10-K for domestic companies, foreign private issuers are required to submit comparable disclosures on Form 6-K for material cybersecurity incidents and on Form 20-F for cybersecurity risk management, strategy, and governance. However, the final rule clarifies that incident disclosures on Form 6-K must be made by FPIs only when both (1) the standard requirements for 6-K reporting are met (namely where info must be made public under its corporate jurisdictional laws, that it must file with any stock exchange, or that it otherwise distributes to security holders) *and* (2) the incident is deemed material.

Compliance Timeline. The final rules will become effective 30 days after the SEC's adopting release is published in the Federal Register, which will likely occur in September. In the meantime, public

companies should consider their risk management practices, with a focus on certain priorities reflected in the new rules, including:

- Reviewing disclosure control policies and procedures for identifying and escalating incidents;
- Performing periodic reviews of the corporate cyber posture and resourcing;
- Strengthening governance and oversight of mission-critical cybersecurity risks;
- Auditing policy framework and implementation practices; and
- Seeking vulnerability assessment and penetration testing to enable necessary remedial efforts.

With special thanks to summer associate, Ian Allen.

Freshfields

February 23, 2024 | 9 minutes read

2024 Proxy Advisor Guidelines: What Companies Need to Know Heading into the 2024 Proxy Season


Elizabeth Bieber
Partner


Sarah Ghulamhussain
Partner


Peter Liddle
Associate

The two most influential proxy advisor firms, Institutional Shareholder Services (ISS) and Glass Lewis & Co. (Glass Lewis), updated their annual voting policies for annual shareholder meetings in 2024. Both proxy advisory firms' voting guidelines are currently in effect, with ISS' effective for shareholder meetings on or after February 1, 2024, and Glass Lewis' effective for shareholder meetings on or after January 1, 2024. In a departure from prior years, ISS had minimal changes to its voting policies this year with updates only to executive compensation related matters. Glass Lewis, by comparison, took a substantially more expansive approach, focusing on revisions related to executive compensation, cybersecurity considerations and climate and ESG oversight issues for 2024.

Policy changes on executive incentives, compensation & equity ownership.

Executive compensation was the focus of Glass Lewis' 2024 updates. Dominant themes in this year's compensation-related updates from Glass Lewis related to tightening of pre-existing pay governance principles in areas such recoupment policies and executive ownership guidelines, as well as enhanced disclosure of incentive payments based on non-GAAP metrics. Meanwhile, the sole voting policy update from ISS came in the form of a move to case-by-case evaluation of shareholder proposals relating to executive severance, alongside more general updates covered in its compensation related FAQs and other resources detailing its pay-for-performance evaluation methodology.

Clawback provisions

Glass Lewis' updated guidelines state that effective clawback policies should go beyond the new minimum NYSE and Nasdaq listing requirements, which relate solely to recoupment of erroneously paid compensation arising from material financial misstatements. Glass Lewis expects clawback policies authorize companies to recoup incentive compensation from executives when there is evidence of problematic decisions or actions, such as material misconduct, a material reputational failure, material risk management failure, or a material operational failure, the consequences of which have not already been reflected in incentive payments and where recovery is warranted, regardless of whether the executive is terminated with or without cause. The guidelines do not state whether there will be a direct impact on Say-on-Pay vote recommendations if a company fails to adopt such a broader policy. However, Glass Lewis notes that if a company ultimately refrains from pursuing recoupment, it will be expected to provide sufficient rationale for doing so and also explain any alternative remediation measures (such as the exercise of negative discretion on future payments), which will be evaluated on a case-by-case basis. While ISS' guidelines do not address misconduct, ISS (by withholding credit in its Governance QualityScore and Equity

Plan Scorecard) and Glass Lewis continue to express an expectation that recoupment policies provide for recovery of both time-based and performance-based awards.

Executive severance payments and terminations

ISS continues to place increased focus on disclosure regarding severance payments in connection with executive terminations and directs companies to disclose both the type of termination occurring under an applicable employment agreement as well as the provision by which such payments are made. ISS' 2024 Compensation Policies FAQ notes its view that excessive payments made to executives in connection with an apparent voluntary resignation or retirement will be regarded as a "problematic pay practice" that may lead to an adverse Say-on-Pay recommendation. The FAQ cautions against disclosure indicating an executive "stepped down" or that the executive and the board have "mutually agreed" on departure, positing that such statements do not enable investors to fully evaluate severance payments.

Meanwhile, ISS' sole change to its voting policy updates for 2024 revised an existing policy on shareholder proposals seeking to require that executive severance agreements be submitted for shareholder ratification. Aiming to harmonize its analysis of both regular termination severance as well as change-in-control related ("golden parachute") severance, ISS will now recommend voting case-by-case on all such shareholder proposals. Previously, ISS generally recommended a yes vote to shareholder ratification of ordinary severance, unless the proposal required shareholder approval prior to entering employment contracts. Factors ISS said it will consider in this case-by-case analysis for both ordinary severance and change-in-control related severance include whether the company's severance or change-in-control agreements in place have problematic features (such as excessive severance entitlements, single triggers, excise tax gross-ups), whether there are existing limits on cash severance payouts which require shareholder ratification of payments exceeding a certain level, whether there have been any recent

severance-related controversies and the degree of prescriptiveness to the shareholder ratification vote (i.e., does the proposal require shareholder approval even if the severance does not exceed market norms).

Executive ownership guidelines

Glass Lewis formalized its expectation that companies should adopt and enforce minimum share ownership rules for named executive officers, with disclosure of the ownership requirements in the Compensation Discussion & Analysis section of the annual proxy statement. For 2024, Glass Lewis has indicated that companies should not count performance-based full value awards or unexercised options under their ownership guidelines without a clear rationale for doing so. ISS has historically taken a more stringent stance by withholding credit under its Governance QualityScore unless unearned performance awards and unexercised options are excluded.

Impact of pay-versus-performance disclosure

As companies approach the second proxy season in which Pay-versus-Performance (PvP) disclosure will be included under Item 402(v) of Regulation S-K, Glass Lewis has revised its guidelines to note that PvP disclosure may be used as part of its supplemental quantitative assessments supporting its primary pay-for-performance grade. ISS has not included a policy statement on how PvP disclosures may be used.

Non-GAAP incentive plan adjustment

Glass Lewis has clarified that adjustments from GAAP to non-GAAP figures in the determination of executive performance metrics may be considered in its assessment of the effectiveness of a company's pay-for-performance strategy. Under its analysis, companies will be expected to include detailed discussions of such adjustments to enable shareholders to reconcile GAAP to non-GAAP results and the corresponding impact on incentive payouts. ISS also added a more

direct FAQ similarly noting that disclosure in the annual proxy statement of line-item reconciliation to GAAP results, when possible, is considered a best practice. In addition, if adjustments materially increase incentive payouts, companies should carefully explain the board's rationale in approving such an adjustments. Under both regimes the absence of such disclosures may adversely impact recommendation of the Say-on-Pay vote. Notably, ISS FAQ's further state that implementation of adjustments that appear to insulate executives from performance failures (particularly at companies with a quantitative pay-for-performance misalignment) will be viewed negatively.

Compensation takeaways

- Continue to evaluate existing clawback policies in connection with the compensation committee's annual risk-assessment, considering whether broader policies may be appropriate.
- Regularly review and evaluate incentive program metrics, and, if applicable, discuss a framework for addressing non-GAAP adjustments in light of anticipated uncertainties.
- Actively plan for anticipated executive transitions and departures in connection with succession planning, and carefully consider disclosures related to any severance or similar payments.

Incident response

Cybersecurity risk oversight

In conjunction with the new Securities and Exchange Commission (SEC) final rules requiring the reporting of material cybersecurity incidents on Form 8-K, Glass Lewis expanded its consideration of cyber risk oversight for companies that have material cyber incidents. In those instances, Glass Lewis will be focusing on the cybersecurity oversight, response and disclosures, including the expectation that periodic updates be communicated to shareholders regarding progress on resolution and remediation. Factors that Glass Lewis expects to be disclosed non-exhaustively include details regarding the timing of fully restored information systems, the

timing of a return to normal operations, resources provided for affected stakeholders and any other relevant information until full remediation is achieved. This expectation goes beyond the requirements of the new Item 1.05 ofForm 8-K, which generally requires description of the material impacts of the incident rather than the remediation plan. While there is an expectation of significant and on-going disclosure, Glass Lewis acknowledges that certain types of information are not appropriate for disclosure, including specific or technical details that could aid the cyberattacker. Rather, Glass Lewis focuses disclosure as a measure to address affected stakeholders. Any perceived deficiency in oversight, response or disclosure could result in recommendations against votes for "appropriate directors."

Material weakness

Glass Lewis focuses on a new approach to material weaknesses, emphasizing that it believes the audit committee has the responsibility to ensure disclosure of remediation plans with sufficient detail and timely remediation efforts. For material weaknesses ongoing for more than one year, Glass Lewis expects annually updated remediation plan disclosure that include sufficiently detailed information regarding the steps necessary to resolve the material weakness, with specific annual disclosure on the steps completed and remaining open action items. Failure to disclose a remediation plan, or material weaknesses ongoing for more than a year without annually updated remediation plan disclosure, will result in Glass Lewis considering recommending against all members of a company's audit committee that served at the time the material weakness was identified. Glass Lewis is silent on impacts for new audit committee members that served during the pendency of a greater than one-year remediation process.

Incident response takeaways

- The existence of a cybersecurity incident or material weakness triggers additional scrutiny from Glass Lewis, and to some

extent, having an incident occur despite best-in-class governance measures pre-incident will not prevent negative vote recommendations.

- Glass Lewis is particularly focused on periodic disclosure updates regarding resolution, which is not as prescribed an expectation as for cybersecurity incidents as material weaknesses. The timing, tone, content and substantive disclosure regarding remediation are significant factors for Glass Lewis' consideration.
- Assigning director responsibility is significant for Glass Lewis when there is an incident, whether cybersecurity or material weakness. While it is easier to define the scope of responsibility for a material weakness to the audit committee, Glass Lewis does not provide clarification on who they deem to be an appropriate director for cybersecurity incident purposes. Presumably Glass Lewis will evaluate whether a committee is delegated with cybersecurity oversight, whether any directors are cybersecurity experts, and other relevant factors in its analysis, including the company's disclosure regarding its oversight processes. These considerations add further pressure on companies to appropriately design and structure cybersecurity oversight in a manner that is appropriate for the company and considers relevant skills and experience.

Governance Considerations

Glass Lewis clarified that for both board responsiveness considerations and say-on-pay, when considering a 20% threshold of shareholders that vote against management or say-on-pay, respectively, the 20% threshold includes both votes against and abstentions. While the 20% threshold is consistent with prior treatment, the clarification that Glass Lewis treats abstentions as an "against" vote is a new development.

Board's role in oversight and accountability for climate and other environmental and social issues

Glass Lewis expanded its expectations for climate-related issues from what it considered the "largest, most significant emitters" to the entire S&P 500 index operating in industries where the Sustainability Accounting Standards Board (SASB) determined that the company's greenhouse gas emissions represent a financially material risk (which industries Glass Lewis specifies as generally applicable in its policy). This policy will apply regardless of whether a company reports in alignment with SASB or discloses that the risk is material for the company. The expanded policy will also be applied to companies that Glass Lewis believes emissions, climate impacts or stakeholder scrutiny of such impacts represent an outsized and financially material risk, but the universe of these companies is undefined.

Glass Lewis will assess two aspects of disclosure under its policies. First, it will consider the adequacy of a company's disclosures as compared with the recommendations from the Task Force on Climate-related Financial Disclosures. Second, it will review whether clearly defined board-level oversight responsibility for climate-related issues exists and is disclosed. In instances where Glass Lewis finds disclosures in either of these two areas to be lacking, it may recommend against the chair of the committee or board charged with oversight of climate-related issues. In the absence of such oversight (or the disclosure of such oversight), the chair of the governance committee may receive a negative voting recommendation.

For other environmental and social risks and issues, Glass Lewis clarified that it expects companies to formally delegate oversight through the appropriate committee charter or otherwise specified in appropriate governance documents. Specification of oversight solely in a company's annual proxy statement will not satisfy the new expectations. Glass Lewis' policies already noted that a failure to provide sufficient oversight disclosure risks against votes for the governance committee chair, which is likely to be applied to the governing document expectations, as well.

Environmental and social takeaways

- There is a shift from a focus solely on governance policies, improvements over time and disclosure to layering on codification of board oversight into formal governance documents, as well as a focus on identification of directors tasked with environmental and social oversight responsibilities.
- As with cybersecurity oversight discussed above, Glass Lewis is likely to evaluate a company's own oversight disclosure and director skills when considering which directors may be subject to negative voting recommendations, but the absence of specification will not prevent Glass Lewis from selecting directors to receive a negative voting recommendation.
- As with other environmental and social voting policies from proxy advisory firms and institutional investors, companies can expect that the voting and disclosure policies applicable to a subset of companies will continue to expand in future years. As a result, it is prudent for companies in all indices to understand the expectations on climate-related disclosure and oversight.

It is noted that considerations for companies in this post are not one-size-fits-all and the appropriateness of implementing or amending any policies or disclosure is anticipated to be a facts and circumstances analysis, considering a holistic review of company practices, principles driving the practice, strategic aims and shareholder engagement, among other factors.

Freshfields

July 18, 2023 | 3 minutes read

White House Releases Roadmap for Increased Cybersecurity Regulation


Brock Dahl
Partner


Timothy Howard
Partner


Beth George
Partner

+3 more...

The White House has released the implementation plan for the key "pillars" in the National Cybersecurity Strategy that was published in March and discussed in our prior blog post. The implementation plan represents another step forward in the Administration's efforts to expand the cybersecurity regulatory footprint and establish or otherwise shift roles, responsibilities, and liabilities, placing greater obligations on critical private sector entities that will require deliberate analysis and management.

I. Key Elements

The plan sets forth 65 initiatives and is particularly notable for the Administration's effort to push certain categories of companies to

bear more responsibility (and liability) for security. While a number of the initiatives place particular responsibilities on various federal agencies, companies should pay particular attention to certain elements that focus on shifting liability to private actors and on emerging compulsory standards for critical infrastructure providers.

1. Shifting Liability to Private Actors.

- **A new liability framework for software products and services (Initiative 3.3.1)** – The plan aims to establish a legislative framework for a liability regime for software products and services, and will pursue that goal through a symposium hosted by the Office of the National Cyber Director to discuss the regime and concomitant standards of care for industry. Legislation would be required to make those standards actionable (in particular through legislative safe harbors that will shape the contours of responsible behavior).
- **Software bill of materials (SBOM) (Initiative 3.3.2)** – The plan pushes for increased transparency into software products and possible vulnerabilities by requiring precise documentation of software used in critical infrastructure through the expanded use of (SBOM, which require software developers to keep a detailed inventory of the components of any new software.) Such records are essential to understanding the origins of code and tracing potential problem sources, as was required when the Log4j vulnerability led to widespread efforts by companies to identify their reliance on such code.
- **Federal procurement (Initiatives 3.5.1 and 3.5.2)** – The plan calls for stricter government review of the execution of security obligations within federal contracts. The Administration anticipates releasing new federal acquisition rules that focus on cybersecurity incident reporting, standardized cybersecurity contract requirements, and secure software. Indeed, even companies that do not directly contract with the government will be impacted by derivative requirements. Critically, the Department of Justice will continue to pursue government

contractors for failing to meet cybersecurity obligations through the Civil Cyber-Fraud Initiative—through which DOJ has already been obtaining multi-million dollar fines against companies for failing to comply with cybersecurity commitments in government contracts under the False Claims Act—and the new acquisition rules will likely provide a broader foundation for such actions.

2. Compulsory Federal Standards for Tech and Critical Infrastructure.

- **Critical infrastructure security (Initiative 1.1.2)** – The National Security Council (***NSC***) will lead the continued regulatory expansion of definitive cybersecurity requirements through all critical infrastructure sectors. The NSC will rely upon regulators to identify potential weaknesses in their sectors, and aims to have security requirements in place halfway through fiscal year 2025.
- **Infrastructure-as-a-Service security (Initiative 2.4.1)** – The plan directs the Department of Commerce to propose rules by the end of the year to implement an executive order establishing risk management standards for Infrastructure-as-a-Service (IaaS) providers and resellers. Given concerns expressed in the strategy released in March, we would expect the rules to focus on know-your-customer requirements and other regulatory means of mitigating the risk that malicious foreign actors pose to accessing and taking advantage of American technology providers.
- **CIRCIA (Initiative 1.4.2)** – Implementation of the Cyber Incident Reporting for Critical Infrastructure Act (***CIRCIA***) continues apace. This initiative directs the Cybersecurity and Infrastructure Agency to take steps towards and finalize implementing regulations for critical infrastructure cyber incident reporting by the end of fiscal year 2025. Among other things, these regulations are expected to have mandatory reporting

requirements for incidents and ransomware payments for companies in covered critical infrastructure sectors.

II. Takeaways

The plan confirms that the Administration will continue to push for aggressive federal regulation of cybersecurity. As legislation emerges shifting liability to the privacy sector, companies involved in software development need to take steps to make sure that the emerging standards are taken into account in the software development process. In addition, all companies, but especially technology providers, those in critical infrastructure sectors, financial institutions, and government contractors, should consider preparing for increased governmental scrutiny by:

- Determining the likelihood that their sector or business will fall within the scope of one or more of these initiatives;
- Assessing risks and potential vulnerabilities, and reviewing and updating governance controls in contemplation of the emerging standards;
- Evaluating procedures for incident reporting and information sharing with an aim towards quickly actionable incident assessment, escalation, and reporting protocols; and,
- Monitoring draft federal acquisition rules and reviewing any federal contract obligations to ensure commercial capabilities are geared towards achieving compliance.

This article has been co-authored by summer associate Anne Klok.