Resisting Hindsight Bias: A Proposed Framework for CISO Liability

December 11, 2023

On October 30, 2023, the U.S. Securities and Exchange Commission ("SEC" or "Commission") charged SolarWinds Corporation's ("SolarWinds" or the "Company") chief information security officer ("CISO") with violations of the anti-fraud provisions of the federal securities laws in connection with alleged disclosure and internal controls violations related both to the Russian cyberattack on the Company discovered in December 2020 and to alleged undisclosed weaknesses in the Company's cybersecurity program dating back to 2018.[1] This is the first time the SEC has charged a CISO in connection with alleged violations of the federal securities laws occurring within the scope of his or her cybersecurity functions.[2] In doing so, the SEC has raised industry concerns that it intends to—with the benefit of 20/20 hindsight, but without the benefit of core cybersecurity expertise—dissect a CISO's good-faith judgments in the aftermath of a cybersecurity incident and wield incidents to second guess the design and effectiveness of a company's entire cybersecurity program (including as it intersects with internal accounting controls designed to identify and prevent errors or inaccuracies in financial reporting) and related disclosures and attempt to hold the CISO liable for any perceived failures.

The Commission's approach threatens CISOs with personal liability for their good-faith efforts to fulfill their responsibilities and seemingly imposes broad accountability on CISOs for aspects of a company's security posture and disclosures far beyond a CISO's control. The SEC's decision to target CISOs sets up an untenable internal tension between CISOs and their companies, including potentially forcing CISOs to demand cybersecurity structures, processes and headcount without concern for the appropriate balance of risk, security and business functions. The SEC's approach also threatens to jeopardize national security; undermines the public- and private- partnerships and information sharing encouraged pre- and post-incident by agencies like Cybersecurity and Infrastructure Security Agency ("CISA"), Department of Homeland Security ("DHS"), Department of Defense ("DoD"), Department of Justice ("DOJ") and the

---

1 Complaint, *SEC v. SolarWinds*, No. 23-cv-9518 (S.D.N.Y. Oct. 30, 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf.

2 The SolarWinds CISO was promoted to that position after the relevant period in the SEC's Complaint. During the relevant period, his title was Vice President of Security and Architecture. *Id.*

Federal Bureau of Investigation ("FBI"), as well as by the White House;[3] heightens a victim company's recovery challenges during a live incident; and, most relevant here, may reasonably cause the CISO community to consider whether serving in this essential function is worth running the risk of professional jeopardy even when they make good faith-efforts to devise cybersecurity programs to accurately disclose material elements of those programs and to respond to incidents.

Rather than pursue this fraught path, and to provide the CISO community with clarity and reassurance that their good-faith decisions will not expose them to liability,[4] we believe an urgent need has emerged for a regulatory framework of factors for the SEC to consider when evaluating whether to charge a CISO (or other executive responsible for running a company's cybersecurity program) with violations of the federal securities laws for conduct arising out of his or her CISO duties.

To that end, the CISO Framework described herein proposes that the Commission recognize the critical and evolving nature of the CISO role by focusing the question of CISO liability squarely on whether the CISO made good-faith efforts to perform his or her role. If the answer to that question is yes, CISO liability should never be appropriate, regardless of the Commission's post-mortem view of the merits of the CISO's performance.

---

[3] *See, e.g.*, *Leading cybersecurity officials call for real collaboration between the public, private sectors to fend off threats of cyber threats* (Oct. 21, 2021), https://ocm.auburn.edu/newsroom/news_articles/2021/10/211626-mccrary-institute-hosts-panel.php (noting that at a conference of the "Mount Rushmore" of cybersecurity experts, CISA Director Jen Easterly said that "Cyber security is a team sport. It really matters to have those trusted relationships," and then-White House National Cyber Director Chris Inglis said that "[t]he government needs to shift to a more supportive role, bringing its resources to help secure the private sector."); Christopher Wray, *FBI Partnering with the Private Sector to Counter the Cyber Threat* (Mar. 22, 2022), https://www.fbi.gov/news/speeches/fbi-partnering-with-private-sector-to-counter-the-cyber-threat-032222 (FBI Director Christopher Wray discussing the "critical importance of the FBI and the private sector working together" to address cybersecurity threats); *Statement by President Biden on our Nation's Cybersecurity*, The White House (Mar. 21, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/.

[4] According to a 2023 survey of CISOs conducted by cybersecurity company Proofpoint, more than 62% of CISOs are concerned by the potential to be held personally liable for cyberattacks at their companies, and a similar percentage would not join a company that does not offer insurance to protect them. Phil Muncaster, *CISOs Worried About Personal Liability For Breaches*, INFOSECURITY MAGAZINE (May 9, 2023), https://www.infosecurity-magazine.com/news/cisos-worried-personal-liability/.

The Outsized and Growing Expectations for CISOs[5]

In the face of increasingly sophisticated cybersecurity threats, including national security concerns and new regulatory requirements, it is no longer sufficient for many companies' information technology ("IT") departments to be expected to handle all cybersecurity issues. Regulators now expect larger organizations to have a dedicated CISO to lead a separate information security function and to oversee, implement and enforce the information security program—both for company security and with respect to the security of its supply chain. CISOs are at the forefront of protecting their companies from emergent cybersecurity threats by implementing and enforcing policies and procedures designed to address the ever-evolving threat landscape, collaborating closely with law enforcement and other governmental authorities to protect national security interests and, at the same time, collating, evaluating and translating information that may need to be reported by others at the company in rapidly evolving situations to investors and the SEC.

CISOs must do all of these things while grappling with significant structural and logistical constraints. The CISO role traverses the broader technology and data worlds and must consider systems, technology and software. Companies' senior management and board members may lack cybersecurity expertise (and may disagree on security priorities and disclosures) and non-security colleagues seeking more efficient ways to complete their work may resist cybersecurity policies and procedures.[6] And even where

---

[5] Companies that experience a cybersecurity incident are increasingly subject to mandatory reporting windows pursuant to federal and state regulatory requirements. *See, e.g.*, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 FR 51896, 88 FR 51943 – 51945 (Aug. 4, 2023) (to be codified at 17 C.F.R pt. 249) (the SEC requires registrants to disclose cybersecurity incidents on Form 8-K within four business days of determining that it is material); Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23, § 500.17 (the New York Department of Financial Services requires notification "as promptly as possible but in no event later than 72 hours" and has amended the requirements twice since 2017); Computer-Security Incident Notification Requirement for Banking Organizations and their Bank Service Providers, 12 C.F.R. § 53.3 (effective April 1, 2022) (federal banking agencies require banking organizations to notify regulators within 36 hours of certain security incidents that materially disrupt or are reasonably likely to materially disrupt a bank's services); GDPR, Regulation (EU) 2016/679, Arts. 33-34 (the EU requires covered entities pursuant to the EU General Data Protection Regulation ("GDPR") to notify data protection authorities within 72 hours of becoming aware of a data breach); Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), 6 U.S.C.A. § 681b (effective September 2025 following rulemaking) (CISA will require organizations that provide critical infrastructure to report cybersecurity incidents within 72 hours from the time the entity reasonably believes the incident occurred and to report ransomware payments no later than 24 hours after the ransom payment has been made).

[6] Only 2.3% of board directors at S&P 500 companies have professional experience in cybersecurity; Rob Sloan, *How Much Cybersecurity Expertise Do Boards Really Have?*, WALL STREET JOURNAL (Sept. 25, 2023), https://www.wsj.com/articles/how-much-cybersecurity-expertise-do-boards-really-have-69f5cb0a, and 74% of employees according to a recent Gartner study were willing to bypass company security policies to help meet a business objective (and 69% said they already had). Gartner Press Release, *Gartner Predicts Nearly Half of*

business and technology are fully aligned, some cybersecurity elements can only be implemented in serial fashion and may require months, if not years, to complete. The SEC's action against SolarWinds' CISO seems to suggest that CISOs will also be held personally responsible for ensuring that all security-related controls required by Section 404(a) of the Sarbanes-Oxley Act of 2002 ("SOX") regarding internal accounting controls are effectively designed and maintained. Effective cyber risk management thus requires a meaningful resource commitment and a cross-functional response that draws resources from the business, compliance, legal, privacy and other functions[7]—but the SEC's enforcement approach nonetheless appears to foist this responsibility first and foremost upon CISOs.

The rapidly increasing regulatory expectations compound a CISO's expanding responsibilities. The DOJ, for example, "is working more closely with victim companies than ever before" and has emphasized that it is "mission critical" that government and industry work together to identify and share information about new risk streams and threat actors."[8]

At the same time, the SEC is increasingly focused on cybersecurity from its own regulatory perspective, as demonstrated by its recently adopted rules on cybersecurity risk management, strategy, governance and incident reporting ("SEC cybersecurity rules") that together impose an unprecedented mandatory cybersecurity disclosure regime including significantly expedited risk and incident disclosure.[9] These disclosure obligations, which were not in place at the time of the Russian cyberattack against SolarWinds, may require crucial CISO involvement and leverage his or her judgment regarding the significance and scope of any risk or incident. Among other things, the new rules will require public companies to:

- Make several disclosures related to cybersecurity risk-management programs in their public filings, including whether and how they assess, identify and manage material

---

Cybersecurity Leaders Will Change Jobs by 2025 (Feb. 22, 2023), https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025.

7 *See, e.g.*, CISA, *Questions Every CEO Should Ask About Cyber Risks* (Feb. 1, 2021), https://www.cisa.gov/news-events/news/questions-every-ceo-should-ask-about-cyber-risks (noting in describing organizational cybersecurity best practices that a company's CEO, with assistance from the CISO, chief information officer "and the entire leadership team . . . should ensure that they know how their divisions affect the company's overall cyber risk"; that regular discussions with the board "regarding these risk decisions ensures visibility to all company decision makers"; and that "[e]xecutives should construct policy from the top down to ensure everyone is empowered to perform the tasks related to their role in reducing cybersecurity risk.").

8 Principal Associate Deputy Attorney General Marshall Miller, *Remarks at the Global Investigations Review Annual Meeting* (Sept. 21, 2023), https://www.justice.gov/opa/speech/principal-associate-deputy-attorney-general-marshall-miller-delivers-remarks-global.

9 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216; 34-97989 (July 26, 2023), https://www.sec.gov/rules/final/2023/33-11216.pdf [hereinafter "SEC Cybersecurity Rules Adopting Release"].

risks; whether the company engages any auditors, consultants or other third parties in connection with such processes; and whether the company has processes to oversee and identify third-party risk. Companies will need to disclose whether any risks for cybersecurity threats, current or historical, have materially affected or are likely to materially affect business strategy, operations or financial conditions.

- Disclose certain information about a material cybersecurity incident within four business days of determining (without unreasonable delay) that a cybersecurity incident is material. In the Form 8-K, companies will be required to disclose material aspects of the nature, scope, timing and reasonably likely material impact of the incident on the company (including its financial condition and results of operations) to the extent the information is known at the time.

The new rules' requirements for disclosures related to senior management's and the board's roles in managing and overseeing cybersecurity also increase expectations for CISOs. To the extent applicable, companies are expected to consider including in their disclosures details about which positions are responsible for managing cybersecurity risks, including the relevant expertise of such persons, the board members responsible for cybersecurity oversight and the process by which the board is informed of cybersecurity risks and management.[10] CISOs will be essential to a company's effective integration of these new SEC cybersecurity governance, risk management, and materiality and disclosure processes and requirements into existing policies and controls.

CISO Liability

Unsurprisingly, both the victim-focused national security workstreams and the more enforcement-focused obligations related to public disclosures and effective internal accounting and disclosure controls can require significant input from CISOs and, as demonstrated by the recent charges against SolarWinds' CISO, expose CISOs to significant potential personal liability.

Even prior to promulgating the new rules, the Commission used its existing tools to bring enforcement actions against companies for allegedly deficient disclosures following cyberattacks.[11] This precedent demonstrated that the Commission will probe

---

[10] *Id.* at 171 (Items 106(c)(1)-(2) of Regulation S-K).

[11] *See, e.g.*, Order, *In re Blackbaud, Inc.*, Securities Exchange Act Release No. 97098 (Mar. 9, 2023), https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf (charging company with making misleading disclosures about a 2020 ransomware attack and imposing a $3 million civil penalty); Order, *In re Pearson plc*, Securities Exchange Act Release No. 92676 (Aug. 16, 2021), https://www.sec.gov/litigation/admin/2021/33-10963.pdf (charging company with making misleading disclosures about a 2018 cyber intrusion and imposing a $1 million civil penalty); Order, *In re First American Fin.*

pre-breach cybersecurity programs and post-breach response, driven by the theory that "cyberattacks often lead to securities law violations."[12] But the SEC's choice to single out CISOs for potential personal liability is a particularly controversial step given that effective cyber risk management requires a cross-functional response and broad ownership that includes the board, management and the legal, compliance, IT and communications departments. For example, CISOs often report to chief information or chief technology officers, reflecting the need to balance security recommendations with the technology needs of a company. The SEC's decision to focus on individuals like CISOs for liability purposes even where they conferred and worked in good faith with other stakeholders in the company undermines the notion that cybersecurity requires a whole-of-company effort.[13]

And, importantly, the ever-evolving nature of cybersecurity means that CISOs must always evaluate the risk posed by any given threat or vulnerability—and the necessity of any remediation or disclosure—based on the imperfect information of the moment, knowing that by the time a risk evaluation is made, the information on which a CISO is basing any decisions will almost certainly have become stale because the threat often has changed. Enforcement actions against CISOs for alleged misconduct related to reasonable decision-making regarding cybersecurity programs and incident response and related disclosures will therefore discourage individuals from candidly communicating about these issues or, even worse, from becoming or continuing to act as CISOs at a time when the position is critically important to safeguard company and customer data to preserve shareholder value—for both business purposes and national security.[14]

Corp., Securities Exchange Act Release No. 92176 (June 14, 2021), https://www.sec.gov/litigation/admin/2021/34-92176.pdf (charging company with disclosure controls failures in connection with a cybersecurity vulnerability made public in 2019 and imposing a $487,616 civil penalty); Order, *In re Altaba Inc., f/d/b/a Yahoo! Inc.*, Securities Exchange Act Release No. 83096 (Apr. 24, 2018), http://www.sec.gov/litigation/admin/2018/33-10485.pdf (charging company with failing to disclose a 2014 cybersecurity breach and imposing a $35 million civil penalty). *See also* Hester M. Peirce, Comm'r, U.S. Sec. & Exch. Comm'n, *Harming Investors and Helping Hackers: Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (July 26, 2023), https://www.sec.gov/news/statement/peirce-statement-cybersecurity-072623 (noting that "cyber risk and the attendant disclosure obligations have been front-and-center for public companies for a long time").

12 Tr. of Mot. Hr'g Proceedings at 12, *SEC v. Covington & Burling*, No. 1:23mc-00002-APM (D.D.C. May 12, 2023), ECF No. 36.

13 *See, e.g.*, *Questions Every CEO Should Ask About Cyber Risks*, *supra* note 7.

14 *See, e.g.*, James Rundle, *Cyber Companies and Universities Are Building 'Cyber Talent Hub'*, WALL STREET JOURNAL (July 19, 2022), https://www.wsj.com/articles/cyber-companies-and-universities-are-building-cyber-talent-hub-11658228401 (describing both private- and public-sector concerns that the United States and its allies are falling behind global competitors with respect to cybersecurity skills and training).

The CISO Framework

The CISO Framework proposed herein reflects the principle that the SEC should assess any potential CISO liability through the lens of whether the CISO took actions using good-faith efforts to fulfill his or her CISO-related responsibilities. This should be the beginning and end of the SEC's analysis: even if, in hindsight, a CISO was mistaken or misguided, if he or she acted in good faith in developing the information security program or in executing an incident response, the SEC should decline to pursue individual charges.[15]

Informing this CISO Framework are the adjacent SEC's enforcement actions holding compliance gatekeepers like chief compliance officers ("CCOs") personally liable for alleged compliance failures. Given the parallels in responsibilities and function within a company between CISOs and CCOs, a CISO liability framework should track the Commission's longstanding, bipartisan position on the factors determining the appropriateness of charges against CCOs[16] and the factors set forth in the New York City Bar Association Compliance Committee's 2021 CCO liability framework ("NYC Bar Association's CCO Framework").[17]

On October 24, 2023, the SEC Director of Enforcement Gurbir Grewal reiterated the three "rare" instances in which the Commission typically brings enforcement actions

---

[15] For purposes of this proposal—based on the complaint against SolarWinds' CISO—the charges we expect the SEC might continue to contemplate against CISOs include: (1) violating the antifraud provisions by employing any scheme to defraud or by making, aiding and abetting, or causing material misstatements or omissions about their company's cybersecurity practices or information on the response to or impact of a cybersecurity incident, whether directly in securities filings or other public-facing documents or in sub-certifications that other corporate executives (e.g., CEO, CFO) rely upon for purposes of their own SOX certifications; (2) aiding and abetting or causing internal controls violations by failing to devise and implement internal controls to restrict access to and maintain the security of company or customer data; or (3) aiding and abetting or causing disclosure controls violations by failing to escalate potentially material information to senior management or other disclosure personnel to allow them to make a determination as to whether information is material and requires disclosure.

[16] *See* Luis A. Aguilar, Comm'r, U.S. Sec. & Exch. Comm'n, *The Role of Chief Compliance Officers Must be Supported* (June 29, 2015), http://www.sec.gov/news/statement/supporting-role-of-chief-compliance-officers.html; Daniel M. Gallagher, Comm'r, U.S. Sec. & Exch. Comm'n, *Statement on Recent SEC Settlements Charging Chief Compliance Officers With Violations of Investment Advisers Act Rule 206(4)-7* (June 18, 2015), http://www.sec.gov/news/statement/sec-cco-settlements-iaa-rule-206-4-7.html; *see also* Andrew Ceresney, Dir., Div. of Enforcement, U.S. Sec. & Exch. Comm'n, *2015 National Society of Compliance Professionals, National Conference: Keynote Address* (Nov. 4, 2015), https://www.sec.gov/news/speech/keynote-address-2015-national-society-compliance-prof-cereseney; Gurbir S. Grewal, Dir., Div. of Enforcement, U.S. Sec. & Exch. Comm'n, *Remarks at New York City Bar Association Compliance Institute* (Oct. 24, 2023), https://www.sec.gov/news/speech/grewal-remarks-nyc-bar-association-compliance-institute-102423.

[17] New York City Bar, *Framework for Chief Compliance Officer Liability in the Financial Sector* (June 2, 2023), https://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/framework-for-chief-compliance-officer-liability.

against a CCO: where he or she (i) "affirmatively participated in misconduct unrelated to the compliance function;" (ii) "misled regulators;" or (iii) "where there was a wholesale failure [] to carry out their compliance responsibilities."[18]

Following that model, we propose that SEC charges against a CISO are only appropriate when the CISO (i) was affirmatively involved in alleged misconduct unrelated to the cybersecurity function;[19] (ii) sought to mislead or obstruct an SEC investigation; or (iii) where there is a "wholesale failure" of the CISO "in carrying out responsibilities that were clearly assigned to" him or her.[20] Because no legitimate debate exists about potential CISO liability in connection with the first two categories, we focus for purposes of this CISO Framework on the "wholesale failure" category.

"Wholesale Failure:" Affirmative Factors in Favor of Liability

What is a wholesale failure, and when can it justify CISO liability? We propose that the following factors should govern Commission consideration of potential charges against a CISO in connection with a "wholesale failure" to perform his or her job function: (i) whether the CISO made a good-faith effort to fulfill his or her responsibilities; (ii) whether the alleged failure related to a fundamental or central aspect of a well-run cybersecurity program at the company; (iii) whether the alleged failure persisted over time; (iv) whether the SEC issued clear rules or guidance related to the alleged failure in advance of the time at which the alleged failure occurred; and (v) whether charging the CISO will help fulfill the SEC's regulatory goals.[21] Only where there is a legitimate question of whether the CISO made a good faith effort to fulfill his or her responsibilities—as demonstrated by the CISO's pursuit of education, engagement and execution around the company's cybersecurity program—should the other factors even be weighed.

---

[18] *Remarks at New York City Bar Association Compliance Institute*, *supra* note 16. Further supporting the conceptual soundness of this CISO Framework, Director Grewal explicitly analogized CISO and CCO liability at the Securities Enforcement Forum 2023 on October 25, 2023. *Keynote Q&A Discussion with SEC Enforcement Director Gurbir Grewal*, https://www.youtube.com/watch?v=K--LOeIDMZM ("I think the takeaway should be, much like we talk about when it comes to CCOs—there was a compliance conference yesterday . . . I think the same holds true for CISOs, what I said there, that this can't be . . . a check the box exercise for you in this role. You really need to think about the risks that your entity is dealing with, you really need to think about the needs of your entities, you really need to tailor your policies and procedures accordingly, and you really need to take the steps to maintain and enforce those policies and procedures. . . . if the CISO is involved in the disclosure process and had a certain level of awareness about certain facts that led him to know that those disclosures were inaccurate, then I think it's fair game, regardless of the title.").

[19] This category is meant to capture misconduct such as theft or insider trading. *See, e.g.*, Complaint, *SEC v. Meadow*, No. 23-civ-05573 (S.D.N.Y. June 29, 2023), https://www.sec.gov/files/litigation/complaints/2023/comp25765.pdf (charging a stockbroker and a CCO with insider trading).

[20] *See 2015 National Society of Compliance Professionals, National Conference: Keynote Address*, *supra* note 16.

[21] The CCO Framework served as guidance for developing these factors. *Framework for Chief Compliance Officer Liability in the Financial Sector*, *supra* note 17.

Prior to charging a CISO for alleged "wholesale failures," the SEC should find that each of these factors was present and be prepared to clearly articulate them in the charging document to provide clear guidance and reassurance to the CISO community that individual liability was justified and was not simply the result of second-guessing good-faith judgments.

Did the CISO make a good-faith effort to carry out his or her responsibilities?
As noted above, the SEC should decline to pursue charges where a CISO made a good-faith effort to develop an information security program or execute an incident response. In assessing whether a CISO acted in good faith to animate the core functions of an information security program, the SEC should look to the fundamentals of proactive compliance recently set out by Director of Enforcement Grewal: education, engagement and execution.[22]

Education is particularly important for CISOs, who face not only changing regulatory obligations but also an ever-evolving threat landscape coming from both individuals and nation-state actors. CISOs can take steps to educate themselves and employees about these developments by, for example, attending cybersecurity conferences to engage with other industry and government professionals and subscribing to newsletters and security bulletins. If engagement by a CCO is an attempt to "really engage with personnel inside [their] company's different business units and to learn about their activities" and risks,[23] a CISO can "engage" by, for example, implementing a risk-assessment and reporting program designed to identify and escalate cybersecurity risks across the enterprise, but ultimately, CISO engagement should be driven by industry standards around CISO best practices, which are constantly evolving. Execution contemplates that a CISO will seek to implement well-designed policies to underpin a cybersecurity program—but execution must be considered in light of the fact that implementing a cybersecurity program is a cross-functional effort involving many stakeholders and the balance of risk against business need.[24]

To be clear, whether a CISO made good-faith efforts to discharge his or her duties cannot be based on ex-post analysis of how well the CISO weighed risks and red flags against the functioning of the business. As the SEC has stated, threat actors have been

---

[22] *See, e.g.*, *Remarks at New York City Bar Association Compliance Institute*, *supra* note 16 (describing one charge against a CCO when, for at least 10 years, the company did not adopt policies and procedures tailored to the firm's business and did not conduct compliance training or annual reviews of its compliance program).

[23] *Id.*

[24] Execution also does not require perfect compliance. Password policies may be executed, for example, automatically where possible through technical tooling or through training, auditing and remediation—but exceptions and gaps are not evidence of failure to execute.

successful in attacking the "most robust institutions" including the Commission itself.[25] This is because even the most robust institutions can never arrive at a perfect cybersecurity program—no institution will ever be without risk, and how risks are mitigated, addressed or managed requires enterprise-wide judgments based on, among other things, an evaluation of business risk tailored to the organization's "different threats, different vulnerabilities, different risk tolerances."[26]

Did the alleged failure relate to a fundamental or central aspect of a well-run cybersecurity program at the company?

Even where a CISO is alleged to have failed to act in good faith, such a failure still should not be considered a "wholesale failure" sufficient for the Commission to consider whether personal liability may be appropriate unless it relates to a fundamental or central aspect of a company's cybersecurity program. For example, a CISO should generally stay abreast of significant changes in the threat landscape and a failure to do so might, depending on the circumstances, indicate a wholesale failure because it relates to a central aspect of cybersecurity program.

However, before any security concern triggers escalation within an incident response plan, IT and security personnel need to investigate the concern, which might have been reported from any number of sources—including from internal penetration tests, "white-hat" hackers who probe companies' controls and inform them of findings in hopes of a bounty and customer complaints. These employees must investigate complex issues and address novel attacks; a thorough investigation into a security incident will not always result in identification of the root cause or a solution. In this context, while a failure to maintain any process to triage and investigate might indicate a wholesale failure, the failure to identify a root cause or solution to a security concern following a good faith investigation, or to identify that the concern may be a larger red flag than the investigation uncovers, simply cannot be viewed as a per se wholesale failure.[27]

---

[25] Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, *Statement on Cybersecurity* (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20 ("[E]ven the most diligent cybersecurity efforts will not address all cyber risks that enterprises face.")

[26] National Institute of Standards and Technology, *Framework For Improving Critical Infrastructure Cybersecurity V1.1*, at 2 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [hereinafter "NIST CSF"] ("The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework.")

[27] Jeff B. Copeland, *FAIRCON23 Day 2: SEC Talks Cyber Disclosure, Jack Jones Talks Risk 2.0* (Oct. 19, 2023), https://www.fairinstitute.org/blog/faircon23-day-2-cyber-risk-quantification-conference (quoting Chief of the SEC's Crypto Asset and Cyber Unit, David Hirsch: "I don't think there is an expectation on the part of regulators that anyone is going to have perfect visibility and a perfect explanation of what occurred …within 4 days. It's contemplated that it's an iterative process.").

Did the alleged failure persist over time, and did the CISO have multiple opportunities to cure the alleged failure(s)?

In situations where there is an alleged failure to act in good faith that relates to a fundamental aspect of a cybersecurity program, the SEC should consider the extent to which that failure persisted over time and whether the CISO had opportunities to remediate it.

For example, many companies rely on software vendors, which in turn must constantly issue bug fixes and security patches to address vulnerabilities in their own software.[28] Those vendors issue updates and explanations of the updates, and the company must decide whether to install the update, considering whether, in light of the risk profile presented, doing so will be particularly resource-intensive or disruptive to operations. If a CISO is repeatedly warned of an unpatched and actively exploited vulnerability in vendor software and ignores opportunities to patch it where the risk profile presented indicates that a patch is needed and where it is fully feasible to implement without significant business disruption, that may—depending on the broader context—indicate a failure to address a lapse despite the opportunity to do so.

However, not all risks can or should be addressed, and good-faith decisions to accept a persistent risk should not be a basis for liability, even where that risk later manifests.[29] Because cybersecurity resources are always finite, threats are constantly evolving, and cybersecurity is necessarily balanced against other legitimate interests and requires cross-functional coordination and alignment, the aim of a cybersecurity program is "continuous improvement," not perfection.[30] As a result, "insufficient" steps alone should never be the basis for individual liability—*i.e.*, taking steps, even if judged with the benefit of hindsight to have been "insufficient," is not a "wholesale failure."

Did the SEC issue clear rules or guidance related to the alleged failure in advance of the time at which the alleged failure occurred?

Where guidance exists regarding the alleged wholesale failure of a fundamental aspect of a cybersecurity program, such as rules and regulations that clearly highlight regulatory expectations and what would constitute violative conduct, the presence of that guidance

---

[28] In an effort to address the risks that software can pose as transmission vehicles for threat actors, the Biden Administration is developing a software liability framework that would impose liability for technology lacking cyber protections. *See* Dustin Volz, *Biden National Cyber Strategy Seeks to Hold Software Firms Liable for Insecurity*, WALL STREET JOURNAL (Mar. 2, 2023), https://www.wsj.com/articles/biden-national-cyber-strategy-seeks-to-hold-software-firms-liable-for-insecurity-67c592d6.

[29] NIST CSF, *supra* note 26, at 4 ("Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.")

[30] *Id.* at 8, 10 (NIST describes its most rigorous and sophisticated tier of cybersecurity risk-management practices as "Adaptive," not "perfect" and notes that "a process of continuous improvement incorporating advanced cybersecurity technologies and practices" is a characteristic of cyber risk management at that highest tier).

may weigh in favor of liability. But where CISOs and their corporate stakeholder partners work to interpret relevant laws or standards "about which reasonable minds can differ – or laws or rules for which there exists no or little relevant guidance from regulators," individual liability should not be premised upon a view that the CISO's interpretation was "incorrect with the benefit of hindsight."[31] Applying the NYC Bar Association's CCO Framework to CISOs, we suggest that "individual liability should not be used in enforcement actions or settlements intended to introduce a new rule or clarify the interpretation of prior rules."[32]

Does charging the CISO help fulfill the SEC's regulatory goals?[33]

An SEC charge, particularly against an individual, must always serve the SEC's regulatory mission to protect investors. Hindsight determinations of cybersecurity shortcomings that reevaluate decisions that were made by qualified cybersecurity personnel—particularly because the success of a cybersecurity program requires a whole-of-company approach and board-level ownership—threaten to punish good-faith efforts and potentially harm investors (and national security) in the longer term by driving qualified cybersecurity professionals away from CISO positions and chilling necessary internal communication between CISOs and their security teams as well as between CISOs and broader company governance functions.

Now that the SEC has brought its first case against a CISO, CISOs will naturally start to weigh their own potential liability under the federal securities laws in any decision that they make as part of their cybersecurity function.[34] In a field that requires continuous improvement to guard against changing and increasing threats, CISOs may hesitate to have their teams document or report internal practices that can be improved—or to communicate candidly about weaknesses or areas for improvement—fearing that regulators will in hindsight argue that such identified issues demonstrate that the CISO was on notice of the deficiencies and/or that identified weaknesses enabled any subsequent cybersecurity attacks. CISOs may determine that the only safe position is to treat every risk, no matter how remote, as critical, pitting CISOs against other

---

31 *Framework for Chief Compliance Officer Liability in the Financial Sector*, *supra* note 17, at 6.

32 *Id.*

33 As Commissioner, Peirce noted in a 2020 speech on CCO liability, "[j]ust because the Commission *can* do something under our rules does not mean that we *should* do it." Hester M. Peirce, Comm'r, U.S. Sec. & Exch. Comm'n, *When the Nail Fails – Remarks before the National Society of Compliance Professionals* (Oct. 19, 2020), https://www.sec.gov/news/speech/peirce-nscp-2020-10-19.

34 Kim Nash, *Cyber Chiefs Worry About Personal Liability as SEC Sues SolarWinds, Executive*, WALL STREET JOURNAL (Oct. 30, 2023), https://www.wsj.com/articles/cyber-chiefs-worry-about-personal-liability-as-sec-sues-solarwinds-executive-0b69cdf3 ("Chief information security officers are concerned that the steps they take to respond to a cyberattack, or how they communicate internally and publicly about an incident, could leave them open to legal action. 'There's the prospect of real personal liability,' said Brian Fricke, CISO of City National Bank of Florida.")

stakeholders in a constant and untenable battle for resources and unnecessarily escalating every risk.

Given these concerns, the SEC must consider the ultimate effects that investigating and charging CISOs may have on the interests of investors. For example, issuers are expected to disclose "whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes."[35] Companies already face a challenging task when deciding what to disclose about the state of their cybersecurity programs: too much detail can provide a roadmap for attackers looking to capitalize on weaknesses in cybersecurity.[36] The threat of personal liability may push CISOs to advocate for over-disclosure, regardless of the risk. Enforcement actions that have the perverse effect of making companies less safe through over-disclosure will undermine the Commission's regulatory goals.

Taken together, the above-detailed factors would require the SEC to decline to pursue enforcement actions against a CISO where the CISO made good-faith efforts to fulfill his or her responsibilities. Where, however, a CISO is alleged not to have made good-faith efforts to fulfill his or her responsibilities, liability may be warranted if: (i) the alleged failure related to a fundamental or central aspect of a well-run cybersecurity program at the company; (ii) the alleged failure persisted over time; (iii) the SEC issued clear rules or guidance related to the alleged failure in advance of the time at which the alleged failure occurred; and (iv) charging the CISO will help fulfill the SEC's regulatory goals.

Mitigating Factors

Even where sufficient affirmative factors are present to warrant the SEC considering whether to charge a CISO, the SEC should next consider mitigating factors.

Did the CISO timely and transparently escalate the issue to other stakeholders?
The Commission should consider whether the CISO timely and transparently escalated known issues to other stakeholders. Having determined that a risk manifested or a breach occurred, the fact that a CISO actively raised the issue to security stakeholders

---

[35] SEC Cybersecurity Rules Adopting Release, *supra* note 9, at 63.

[36] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Exchange Act Rel. No. 34-82746, at 11 (Feb. 26, 2018), https://www.sec.gov/files/rules/interp/2018/33-10459.pdf ("We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident."); *see also* Div. of Corp. Fin., U.S. Sec. & Exch. Comm'n, *CF Disclosure Guidance: Topic No. 2*, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (Oct. 13, 2011) ("We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts -- for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security -- and we emphasize that disclosures of that nature are not required under the federal securities laws.").

like senior management, and/or the board should weigh against personal liability, even where the CISO had previously exhibited a "wholesale failure" to act, as outlined above. Post-breach collaboration and information sharing are critical for a company's compliance with the federal securities laws as well as to collective cybersecurity defense for national security purposes and for raising awareness of other potential targets.[37] Internal escalation of known issues is critical to the success of that collaboration and should be encouraged by considering it as a mitigating factor for a CISO's personal liability.

Did structural or resource challenges hinder the CISO's performance?

The SEC should also consider among potential mitigating factors whether the CISO was operating against structural or resource challenges that may have hindered her or his performance. As noted above, a sound information security program requires a whole-company approach. A CISO cannot be expected to evaluate, educate and execute a functioning program singlehandedly. CISOs require resources, cooperation from internal stakeholders, and decision-making authority, and the SEC should consider whether and how a company's organizational structure affects that coordination or a CISO's empowerment.

Again, personal liability should never be appropriate where a CISO acted in good faith, but even where there is an alleged persistent failure to act in good faith in connection with a fundamental aspect of the cybersecurity program, the SEC should consider the extent to which a CISO had access to sufficient resources and budget to address security issues or was burdened by competing functions and obligations, whether due to insufficient budgeting, staffing, or poorly defined or designated responsibilities—or as a result of a deliberate management decision to embrace a relatively high-risk tolerance.

Similar to how DOJ evaluates the extent to which corporate compliance programs are adequately resourced and empowered to function effectively, the SEC should consider the CISO's support structure and the company's risk posture when contemplating charging a CISO for a wholesale failure.

---

[37] *See* CISA, *Sharing Cyber Event Information Fact Sheet* (Apr. 2022), https://www.cisa.gov/sites/default/files/2022-11/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf. *See also* Lisa Monaco, Dep. Atty. General, *Keynote Address at International Conference on Cyber Security (ICCS) 2022* (July 19, 2022), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-keynote-address-international-conference (describing how the government has been able to disrupt cybercrimes due to "critical reporting from and cooperation with companies who have been victims of cyber-attacks"); Oversight of the U.S. Securities and Exchange Commission, Hearing Before the Comm. on Banking, Housing and Urban Affairs, 115th Cong. 115-134 (Sept. 26, 2017) (testimony of Jay Clayton, Chairman, U.S. Sec. and Exch. Comm'n.), https://www.govinfo.gov/content/pkg/CHRG-115shrg28283/html/CHRG-115shrg28283.htm ("Information sharing and coordination are essential for regulators to anticipate potential cyber threats and respond to [] major cyberattack[s].").

CONCLUSION

Given the SEC's recent charges against the SolarWinds CISO and the discordant public statements made by SEC staff that the Commission does "not second-guess good faith judgments of compliance personnel made after reasonable inquiry and analysis,"[38] we propose the above-described CISO liability framework that turns on whether the CISO made good-faith efforts to execute his or her duties. Imposing such a framework would instill greater transparency, accountability and predictability in the way the SEC contemplates charging CISOs.

* * *

Please do not hesitate to contact us with any questions.

Andrew J. Ceresney
Partner, New York
+1 212 909 6947
aceresney@debevoise.com

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekhar@debevoise.com

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Julie M. Riewe
Partner, Washington, D.C.
+1 202 383 8070
jriewe@debevoise.com

Anna Moody
Counsel, Washington, D.C.
+1 202 383 8017
amoody@debevoise.com

Andreas A. Glimenakis
Associate, Washington, D.C.
+1 202 383 8138
aaglimenakis@debevoise.com

Melissa Muse
Associate, New York
+1 212 909 6882
mmuse@debevoise.com

[38] *Remarks at New York City Bar Association Compliance Institute*, *supra* note 16.