THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 58 No. 9 May 7, 2025

WHO, WHAT, WHEN, WHERE, AND WHY: LESSONS LEARNED FROM THE *SOLARWINDS* LITIGATION

Companies and boards trying to minimize their cybersecurity risks face significant challenges. The risks of a data breach are omnipresent and now present heightened difficulty, given the rise of generative AI. Corporate counsel and compliance professionals must also contend with a fragmented and evolving regulatory landscape. This article draws lessons from the SEC's SolarWinds litigation, focusing on the securities fraud claims that survived the court's ruling on the defendants' motion to dismiss, and examining the conduct and statements that the district court found actionable. This article provides practical recommendations for those seeking to comply with a complex legal landscape and to enhance their cybersecurity programs.

By Olivia S. Choe *

Cybersecurity and data breach risks remain a top concern for corporate counsel.[1] And for good reason. The risk of a cyber incident — which has for some time been an ever-present and a growing threat — now presents heightened difficulty, given the rise of generative AI.[2] The enforcement and litigation landscape is complex and evolving, particularly as a new

[1] Norton Rose Fulbright, Cybersecurity and data privacy: 2025 Annual Litigation Trends Survey, https://www.nortonrosefulbright.com/en/knowledge/publications/4207a081/cybersecurity-and-data-privacy (79% of corporate counsel expect exposure to cybersecurity and data privacy disputes to remain the same or grow in 2025); Baker McKenzie, Global Disputes Forecast 2025, https://www.bakermckenzie.com/en/insight/publications/2025/01/global-disputes-forecast-2025 ("Cybersecurity and data privacy disputes remain the top concern. . . .").

[2] National Cyber Security Centre, The near-term impact of AI on the cyber threat, https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat; Fed. Bureau of Investigation, FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence (May 8, 2024), https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence (May 8, 2024); N.Y. Dep't of Fin. Servs., DFS Superintendent Adrienne A. Harris Issues New Guidance to Address Cybersecurity Risks Arising from Artificial Intelligence (Oct. 16, 2024), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20241016.

* *OLIVIA S. CHOE is a Litigation and Arbitration partner in Milbank LLP's Washington, DC office. From 2022 to 2024, she was the Chief Litigation Counsel for the SEC's Division of Enforcement. Her e-mail address is ochoe@milbank.com. ARMAN RAMNATH and AMNA RASHID contributed to this article. The opinions expressed are those of the author and do not necessarily reflect the views of any past or present employers or clients; the analysis herein is based upon publicly available information and pleadings.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

administration with a starkly different approach to regulation and corporate oversight establishes itself, and as state enforcement authorities set their own agendas. At this particular juncture, I examine recent enforcement and litigation trends and reflect on key lessons learned from the SEC's *SolarWinds* litigation. This article offers practical considerations for companies grappling with how best to tailor their compliance programs in an uncertain and challenging environment. In particular, corporate counsel, cybersecurity professionals, and boards should pay close attention to:

- Prioritizing legal expertise, a key asset in dealing with a patchwork and overlapping set of state and federal regulations.
- Appropriately calibrating escalation procedures to capture internal discussions and harmonizing external communications with internal knowledge.
- Ensuring that the right people are looking in the right places for public statements that may be subject to regulatory scrutiny.

I. A FRAGMENTED REGULATORY LANDSCAPE

Companies navigating a cyber breach, or designing a program to be prepared for one, face a daunting patchwork of federal and state regulation.

At the federal level, reporting companies must be prepared to make disclosures to the SEC under the agency's 2023 rules, both in response to a data compromise and also with respect to management and governance on an annual basis. Depending upon their industry, companies may also be required to make notifications regarding a cyber breach to a variety of other federal agencies, including the Department of Health and Human Services, the Federal Deposit Insurance Corporation,[3] the Federal Housing Administration,[4] the Transportation Security Administration,[5] and the Federal Trade Commission, among others.[6] In addition, the Cybersecurity and Infrastructure Security Agency last year proposed a rule that would impose further reporting obligations on companies in a range of industries falling within "a critical infrastructure sector"; that rule has yet to be finalized and has received a number of comments as well as ongoing public criticism.[7]

Adding to this complex federal regulatory landscape is a growing body of state-level cyber and data privacy regulation. In the absence of federal data privacy legislation, many states have enacted their own consumer privacy laws, a number of which impose requirements upon businesses relating to their cybersecurity programs and cyber incident reporting.[8] In

[3] 12 C.F.R. § 304 subpart C — Computer-Security Incident Notification, https://www.ecfr.gov/current/title-12/chapter-III/subchapter-A/part-304/subpart-C.

[4] U.S. Dep't of Hous. & Urb. Dev., Mortgagee Letter 2024-23, Revised Cyber Incident Reporting Requirements (Dec. 2, 2024), https://www.hud.gov/sites/dfiles/OCHCO/documents/2024-23hsgml.pdf.

[5] Transp. Sec. Admin., Security Directive Pipeline-2021-01B, Enhancing Pipeline Cybersecurity (May 29, 2022), https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf.

[6] Fed. Trade Comm'n, Health Breach Notification Rule, https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule.

[7] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23,644 (proposed Apr. 4, 2024) (to be codified at 6 C.F.R. § 226), https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements; James Rundle, *Cyber Reporting Rules Savaged in House Hearing*, Wall St. J., (Mar. 12, 2025), https://www.wsj.com/articles/cyber-reporting-rules-savaged-in-house-hearing-fdb3e39b?reflink=desktopwebshare_permalink.

[8] Last year, 15 states objected to proposed federal consumer privacy legislation that would preempt existing state laws. Off. of Att'y Gen., State of Cal., Statement of Rob Bonta, Att'y Gen., May 8, 2024, https://oag.ca.gov/system/files/attachments/press-docs/General_APRA%20Letter%20to%20Congress%20v1.pdf.

New York, for example, the Stop Hacks and Improve Electronic Data Security Act ("SHIELD" Act) requires companies to develop, implement, and maintain reasonable safeguards to protect private information and requires notification to affected consumers "in the most expedient time possible, consistent with legitimate needs of law enforcement agencies."[9] Massachusetts requires businesses that own or license personal information about Commonwealth residents to "develop, implement, and maintain a comprehensive information security program" and sets forth various standards for such a program.[10] Texas requires businesses and organizations that experience a data breach affecting "250 or more Texans" to report that breach to the Attorney General "as soon as practicably possible and no later than 30 days after the discovery of the breach."[11] California imposes similar obligations.[12] And several state attorneys general have established data privacy units dedicated to enforcing these laws.[13]

In addition to data privacy laws, some state-level financial regulators have adopted rules governing entities falling within their jurisdiction. In late 2023, for example, New York Department of Financial Services ("NYDFS") amended its existing cybersecurity regulations to include enhanced notice requirements relating to cybersecurity incidents and extortion payments. Among other things, the regulations impose "a continuing obligation to update the superintendent with material changes or new information previously unavailable," and "notice and explanation of extortion payment[s] . . . made in connection with . . . cybersecurity event[]" as well "a written description of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment, and all diligence performed to ensure compliance with applicable rules and regulations."[14] The NYDFS regulation also requires covered entities to make management and oversight disclosures.[15] In January 2024, Robinhood entered into a consent order with Massachusetts's securities regulator concluding, among other things, that Robinhood had "failed to maintain and enforce reasonable cybersecurity policies and procedures."[16]

The vigor with which any of these cybersecurity rules will be enforced in the current administration is uncertain, especially at the federal level. At the time that the SEC's cyber rule was adopted, the two Republican commissioners then in the minority dissented,[17] and it has been the subject of ongoing criticism and calls for

[9] Off. of N.Y. State Att'y Gen., Stop Hacks and Improve Electronic Data Security Act ("SHIELD" Act) (2025), https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act#:~:text=The%20law%20requires%20that%20the,needs%20of%20law%20enforcement%20agencies.

[10] Off. of Consumer Affairs & Bus. Regul., Commw. of Mass., 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth, at 17.03(1), https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth/download.

[11] Att'y Gen. of Tex., Data Breach Reporting, https://www.texasattorneygeneral.gov/consumer-protection/data-breach-reporting#:~:text=Texas%20law%20requires%20businesses%20and,the%20discovery%20of%20the%20breach (effective Sept. 1, 2023).

[12] Att'y Gen., State of Cal. Dep't of Just., Data Security Breach Reporting, https://oag.ca.gov/privacy/databreach/reporting (2025).

[13] The California Department of Justice's Privacy Unit enforces state and federal privacy laws and has brought enforcement actions, including cases against companies alleging misleading statements regarding their cybersecurity programs and misleading post-breach disclosures. Att'y Gen., State of Cal. Dep't of Just., Data Security Breach Reporting, https://oag.ca.gov/privacy/databreach/reporting (2025); Att'y Gen., State of Cal. Dep't of Just., Privacy Enforcement Actions, https://oag.ca.gov/privacy/privacy-enforcement-actions (2025). New York's Attorney General can seek injunctive relief, restitution, and penalties against business entities who violate the SHIELD Act. Stop Hacks and Improve Electronic Data Security Act, *supra* note 20. The Texas

f ootnote continued from previous column…

Attorney General can seek penalties and equitable relief violations of the state's cyber incident notification requirements. Tex. Bus. & Com. Code § 521.151 (2009).

[14] 23 NYCRR 500.17(a)(2), (c), https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf.

[15] *Id.*

[16] Consent Order at 10, *In re Robinhood Fin. LLC*, Dkt. Nos. E-2020-0047, E-2022-0006 (Mass. Sec, Div. Jan. 18, 2024), https://www.sec.state.ma.us/divisions/securities/download/RH-Consent-Order.pdf.

[17] 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/newsroom/speeches-statements/peirce-statement-cybersecurity-072623 (Peirce, dissenting); *id.*, https://www.sec.gov/newsroom/speeches-statements/ uyeda-statement-cybersecurity-072623 (Uyeda, dissenting).

reform.[18] The new administration has announced its intent to exert greater control over interpretations of law; issuance of regulations and guidance; and positions advanced in litigation by agencies, including the SEC.[19] And it has signaled its interest in swiftly eliminating rules that it deems "unlawful, unnecessary, and onerous."[20] Personnel changes may also have an impact on the level of regulation and enforcement at the federal level.[21] The Commission, now led by Chairman Paul Atkins, seems unlikely to follow the aggressive approach taken by the SEC during the Biden administration, when the agency both adopted controversial cybersecurity regulations and brought multiple enforcement actions against issuers who were victims of the SUNBURST attack on SolarWinds, on the theory that their post-breach disclosures were faulty or fraudulent; these cases included the litigated *SolarWinds* action filed in June 2023[22] (discussed in greater detail below) as well as four settled actions announced in October 2024.[23] Given the objections raised in dissent to this most recent batch of enforcement actions by two of the three Republican commissioners, who are now in the majority,[24] and the expressed views of the new Chairman regarding novel enforcement theories,[25] similar actions may be a rarity in the coming months.

On the other hand, the reporting requirements under the SEC's 2023 cyber rule remain in place, and in the first year following its adoption, dozens of issuers filed disclosures with the SEC notifying the Commission and the public that they had experienced a cyber incident. They continue to do so. The agency has also highlighted cybersecurity as an area of priority in examinations for 2025.[26] And within the administration's first month, the SEC announced the creation of a new unit within the Division of Enforcement, the Cyber and Emerging Technologies Unit, which the agency says will focus, among other things, on "[r]egulated entities' compliance with cybersecurity rules and regulations."[27] Indeed, at least one public company has recently reported that it is currently under SEC investigation in connection with a data compromise.[28]

---

[18] Rundle, *supra* n.8.

[19] The White House, Presidential Action, Ensuring Accountability for All Agencies (Feb. 18, 2025), https://www.whitehouse.gov/presidential-actions/2025/02/ensuring-accountability-for-all-agencies/.

[20] The White House, Presidential Action, Directing the Repeal of Unlawful Regulations (Apr. 9, 2025), https://www.whitehouse.gov/presidential-actions/2025/04/directing-the-repeal-of-unlawful-regulations/.

[21] Caitlin Babcock, *US cybersecurity concerns are rising, with China topping the* list, Christian Science Monitor, Apr. 7, 2025, https://www.csmonitor.com/USA/Politics/2025/0407/trump-cybersecurity-congress-china; Oma Seddiq & Mackenzie Hawkins, *Trump Team Plans Mass Firings at Key Agency for AI and Chips (1)*, Bloomberg Gov't, Feb. 19, 2025, https://news.bgov.com/bloomberg-government-news/commerce-agency-to-order-mass-firing-of-chips-ai-staffers; Chris Prentice & Douglas Gillison, *US SEC to see exodus as hundreds take Trump's buyout offers, sources say*, Reuters, Mar. 21, 2025, https://www.reuters.com/world/us/us-sec-see-exodus-hundreds-take-trumps-buyout-offers-sources-say-2025-03-21/.

[22] Sec. & Exch. Comm'n v. Solarwinds Corp., No. 23-cv-9518-PAE (S.D.N.Y.).

[23] *Avaya Holdings Corp.*, Securities Act Release No. 33-11320, Exchange Act Release No. 34 101398, Admin. Proc. File No. 3-22269 (Oct. 22, 2024), https://www.sec.gov/files/litigation/admin/2024/33-11320.pdf.; *Check Point Software Techs. Ltd.*, Securities Act Release No. 33-11321, Exchange Act Release No. 34-101399, Admin. Proc. File No. 3-22270 (Oct. 22, 2024), https://www.sec.gov/files/litigation/admin/2024/33-11321.pdf; *Mimecast Ltd.*, Securities Act Release No. 33-11322, Exchange Act Release No. 34-101400, Admin. Proc. File No. 3-22271 (Oct. 22, 2024), https://www.sec.gov/files/litigation/admin/2024/33-11322.pdf; *Unisys Corp*., Securities Act Release No. 33-11323, Exchange Act Release No. 34-101401, Admin. Proc. File No. 3-22272 (Oct. 22, 2024), https://www.sec.gov/files/litigation/admin/2024/33-11323.pdf.

footnote continued from previous column…

[24] U.S. Sec. & Exch. Comm'n, Statement Regarding Administrative Proceedings Against SolarWinds Customers (Oct. 22, 2024), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-solarwinds-102224.

[25] SEC Speech: Remarks Before the U.S. Chamber of Commerce Mid-Market Elite Series (Commissioner Paul S. Atkins; August 7, 2008) (the SEC should not be "devising new legal theories to reach behavior that does not clearly violate an existing rule. . . . We should not be playing 'gotcha' with our enforcement powers").

[26] U.S. Sec. & Exch. Comm'n Fiscal Year 2025 Examination Priorities, https://www.sec.gov/files/2025-exam-priorities.pdf.

[27] U.S. Sec. & Exch. Comm'n, SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors (Feb. 20, 2025), https://www.sec.gov/newsroom/press-releases/2025-42.

[28] Martin Braun, *SEC Probes Cyberattack of Detroit Suburb's $30 Million Bond Sale*, Bloomberg, Mar. 11, 2025, https://www.bloomberg.com/news/articles/2025-03-11/sec-probes-cyberattack-of-detroit-suburb-s-30-million-bond-sale.

In this fragmented regulatory landscape, private litigants also play a part. In the wake of a cyber incident, companies must contend with lawsuits raising a host of common law, state statutory, and federal claims, including breach of implied contract, negligence, breach of director fiduciary duties, unfair trade practices, and consumer protection violations, as well as federal securities law claims. In other words, even if the SEC plays a less active role in prosecuting companies who experience cybersecurity incidents in the coming months, companies cannot expect a slowdown in state-level enforcement or private litigation arising from data privacy and cybersecurity issues. In 2024 alone, Meta entered into a $1.4 billion settlement with the Texas Attorney General in connection with its unlawful collection of biometric data, in violation of Texas's privacy laws,[29] and Alphabet entered into a $350 million settlement in a securities class action alleging that Google failed to adequately disclose both a data breach and a vulnerability that had rendered user data accessible to third parties for multiple years.[30]

Cyber threats and regulatory complexity are unlikely to decline; in fact, both will likely increase. Together, they create challenges that make it essential for companies to design robust and nimble cybersecurity compliance programs. In doing so, lessons from the court's ruling in the SEC's *SolarWinds* litigation are instructive.

II. THE *SOLARWINDS* LITIGATION

A. The SEC's Case and Reactions to It

When it was filed in the fall of 2023, the SEC's district court action against SolarWinds and Tim Brown — a company executive who, by the time of filing, had become the company's Chief Information Security Officer ("CISO") — drew sharp reactions. The Wall Street Journal called the case "controversial" and referred to it as "a milestone in [the SEC's] evolving attempt to regulate how public companies deal with cybersecurity."[31] Critics argued the SEC's approach "shift[ed] blame to the victim," noting it was the first time that the agency had filed fraud claims against the victim of a data compromise in federal court and singling out the charges against Brown, a cybersecurity executive who did not "directly oversee or prepare the company's financial statements," as "unusual."[32] As one set of commentators put it: "this is the first time the SEC has sued a company for scienter-based fraud involving cybersecurity failures, the first time the SEC has sued a CISO — or any individual — for their role in cybersecurity failures, and the first time the SEC has sued a company for internal controls failures arising from alleged cybersecurity deficiencies that led to a company's inability to protect its key assets."[33]

The facts underlying the case are well-known. In December 2020, SolarWinds — a software company that provides networking software to public and private entities — disclosed that it had been the victim of a massive hack by a nation-state actor. The breach ultimately affected many of SolarWinds's hundreds of customers, including federal agencies. Some of the company's customers were themselves subsequently charged by the SEC with failing to adequately disclose the breach in their own filings.[34]

The SEC's complaint alleged that SolarWinds and Brown were liable for misleading statements and omissions in three different categories: (1) statements touting the company's cybersecurity practices, including in particular a "Security Statement" posted on the company's website for multiple years prior to the massive SUNBURST breach in December 2020; (2) statements regarding the company's cybersecurity made in the company's SEC filings during the same

[29] Att'y Gen. of Tex., *Attorney General Ken Paxton Secures $1.4 Billion Settlement with Meta Over Its Unauthorized Capture of Personal Biometric Data in Largest Settlement Ever Obtained from an Action Brought by a Single State* (July 30, 2024), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture.

[30] Order Granting Motion for Final Approval of Settlement, *In re Alphabet, Inc. Sec. Litig.*, No. 3:18-cv-06245 (N.D. Cal. Sept. 30, 2024), ECF 233-234.

[31] Dave Michaels & Kim S. Nash, *SEC Sues SolarWinds Over 2020 Hack Attributed to Russians*, Wall St. J., Oct. 30, 2023, https://www.wsj.com/finance/regulation/sec-sues-solarwinds-over-2020-hack-attributed-to-russians-70562fb5.

[32] *Id.*

[33] Jennifer Lee, Shoba Pillay & Charles Riely, *SolarWinds Ushers in New Era of SEC Cyber Enforcement*, Law360, Nov. 14, 2023, https://www.law360.com/articles/1766249/solarwinds-ushers-in-new-era-of-sec-cyber-enforcement.

[34] *Avaya Holdings Corp.*, Release No. 33-11320; *Check Point Software Techs. Ltd.*, Release No. 33-11321; *Mimecast Ltd.*, Release No. 33-11322; *Unisys Corp.*, Release No. 33-11323.

period; and (3) an 8-K that SolarWinds filed after discovering the breach, on December 14, 2020.[35]

With respect to the first category of alleged misstatements, the SEC contended that the company's Security Statement — which was available to the public and used to respond to customer inquiries regarding cybersecurity — painted a false picture of the state of the company's cybersecurity practices, including its adherence to the NIST Cybersecurity Framework, a secure development lifecycle in developing its products, and the strength of its password policies and access controls.[36] With respect to the company's pre-breach SEC filings, the complaint alleged that SolarWinds's risk disclosures were too generic and hypothetical, failing to disclose known deficiencies and risks with sufficient specificity.[37] And as to the 8-K that the company filed on December 14, 2020, disclosing the breach, the SEC alleged that the misleading hypothetical disclosures continued, asserting that SolarWinds described itself as determining "whether a vulnerability . . . was exploited" and as "still investigating whether, and to what extent, a vulnerability . . . was successfully exploited," when in fact the company knew it had been.[38]

Based upon these alleged failures, the SEC charged both SolarWinds and Brown with engaging in securities fraud, in violation of Section 17(a) of the Securities Act of 1933 and Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 thereunder, as well as related reporting violations under Section 13 of the Exchange Act. The Commission also charged the company with having deficient disclosure and internal accounting controls, in violation of Rule 13a-15(a) and Section 13(b)(2)(B) of the Exchange Act, respectively.[39]

The latter charge elicited some of the most vehement objections. The SEC alleged that SolarWinds's information technology products, source code, and network environment were "among its most important assets;" that its cybersecurity controls were insufficient to protect those assets; and that the company had therefore "failed to devise and maintain a system of internal controls sufficient to provide reasonable assurance that access to the Company's assets was only in accordance with management's general or specific authorization," thereby violating Section 13(b)(2)(B). According to critics, this theory was divorced from the statutory text and legislative history, which they said made clear that "accounting controls" refer to controls relating to financial reporting and the accuracy and reliability of financial statements. The SEC's attempt to graft the term "accounting controls" onto SolarWinds's cybersecurity controls, in the view of critics, amounted to nothing more than a "power grab [that] has left companies in constant peril and uncertainty about how to design their internal control systems, because once 'accounting controls' are no longer about accounting, virtually everything is fair game."[40]

B. The Court's Ruling: Who, What, When, Where, and Why

On July 18, 2024, the district court issued a lengthy opinion handing SolarWinds a partial victory. As the court put it: "the Court denies in part, but grants in large part, the motion to dismiss."[41] The court dismissed all of the SEC's claims of securities fraud based on the company's SEC filings, including its post-breach disclosures, finding that they "impermissibly rely on hindsight and speculation."[42] Indeed, the court dismissed all of the SEC's fraud claims, except for those relating to the Security Statement. The court further dismissed as "ill-pled" the SEC's internal accounting and disclosure controls claims.[43]

The ruling was widely hailed as a victory for the company in the press and among the bar. "Judge in SolarWinds case rejects SEC oversight of cybersecurity controls," announced the Washington Post.[44] One

[35] Amended Complaint, Sec. & Exch. Comm'n v. Solarwinds Corp. and Timothy G. Brown, No. 23-cv-9518-PAE (S.D.N.Y. Feb. 16, 2024), ECF No. 85.

[36] *Id.* at ¶¶ 1–130.

[37] *Id.* at ¶¶ 1–181.

[38] *Id.* at ¶¶ 1–193.

[39] Amended Complaint, Sec. & Exch. Comm'n v. Solarwinds Corp. and Timothy G. Brown, No. 23-cv-9518-PAE (S.D.N.Y. Feb. 16, 2024), ECF No. 85. Brown was also charged with aiding and abetting the company's violations. *Id.* at ¶¶ 206–09.

[40] Brief of Amici Curiae Chamber of Com. of the U.S of Am. and Bus. Roundtable in Support of Defs.' Mot. to Dis. at 4, Sec. & Exch. Comm'n v. Solarwinds Corp. and Timothy G. Brown, No. 23-cv-9518 (S.D.N.Y. Oct. 30, 2023), ECF No. 68-1.

[41] Sec. & Exch. Comm'n v. Solarwinds Corp., 741 F. Supp. 3d 37, 49 (S.D.N.Y. 2024).

[42] *Id.* at 50.

[43] *Id.*

[44] Joseph Menn, *Judge in SolarWinds case rejects SEC oversight of cybersecurity controls*, Wash. Post, July 18, 2024, https://www.washingtonpost.com/technology/2024/07/18/solarwinds-sec-cybersecurity-hack-disclosures/.

attorney called the ruling a victory "by any measure,"[45] while other commentators characterized it as a "blow to SEC cyber enforcement."[46] The court's resounding rejection of the Commission's internal accounting controls claim received particular attention.[47]

But for companies and boards trying to design effective cybersecurity programs and cybersecurity professionals following the case against Brown, the heated wrangling among lawyers over a somewhat arcane provision of the securities laws concerning internal accounting controls — while of tremendous interest to the securities industry bar — may be of somewhat limited practical significance. Of more import may be the part of the case that survived. While the court dismissed most of the SEC's claims, the remaining claims are serious ones: both SolarWinds and Brown still face potential liability for securities fraud in connection with the company's Security Statement. The court sustained both of the SEC's fraud theories as to the Security Statement — that it contained materially misleading statements and omissions, and that it was part of a fraudulent scheme.[48] For the company and for the individual, who continue to litigate against the SEC, a finding of liability under Section 10(b) of the Exchange Act and Section 17(a) of the Securities Act would be highly damaging and carry potentially severe consequences beyond any financial penalties, including certain statutory disqualifications from capital-raising activities for the company, and a possible ban from serving as an officer or director of a public company for the individual.

For those trying to draw lessons from the *SolarWinds* case to minimize risks in their cybersecurity governance regimes, a searching analysis of the surviving portions of the SEC's case is a useful exercise. And that analysis should focus on the basics: who, what, when, where, and why.

Who: Much of the coverage of the case has referred to Brown as SolarWinds's CISO, and a group of CISOs even filed a proposed amicus brief arguing that the SEC's charges against Brown "give CISOs an incentive to refrain from candid communication," "hamstring CISOs in the arms race by undermining the work of detecting and improving vulnerabilities," and "cause more CISOs to leave their positions."[49] In fact, Brown was until the tail-end of the relevant period the company's vice president of security and architecture and head of information security, who reported to the Chief Information Officer.[50] He did not become the company's CISO until January 2021, after the SUNBURST disclosure.

In finding that the SEC had adequately alleged that Brown engaged in securities fraud, and that Brown's scienter could be properly imputed to SolarWinds, the district court paid little regard to his precise title. Instead, the court focused on the substance of Brown's role. Brown was "responsible for SolarWinds' cybersecurity protocols and the cybersecurity architecture of its products," and had a "duty to monitor SolarWinds' cybersecurity." He served as the company's "cybersecurity spokesperson" and played a "lead role on cybersecurity matters at the company."[51] While he did

[45] James Rundle & Dave Michaels, *SolarWinds Defeats Part of SEC's Fraud Case Over Hack*, Wall St. J., July 18, 2024, https://www.wsj.com/articles/solarwinds-defeats-part-of-secs-fraud-case-over-hack-ec69169a?mod=Searchresults_pos1&page=1; *see also* Jennifer Corso, *SolarWinds Beats Most Claims In SEC's Data Breach Suit*, Law360, July 18, 2024, https://www.laspaw360.com/articles/1859568.

[46] Paul, Weiss, Rifkind, Wharton & Garrison LLP, *SDNY Court Deals Blow to SEC Cyber Enforcement, Dismisses Most Charges Against SolarWinds and Its CISO*, July 23, 2024, https://www.paulweiss.com/practices/litigation/cybersecurity-data-protection/publications/sdny-court-deals-blow-to-sec-cyber-enforcement-dismisses-most-charges-against-solarwinds-and-its-ciso?id=52318; Sullivan & Cromwell LLP, *Court Dismisses Most of SEC's Claims Against SolarWinds and Its CISO*, July 19, 2024, https://www.sullcrom.com/insights/memo/2024/July/Court-Dismisses-Most-SEC-Claims-Against-SolarWinds.

[47] *E.g.*, FCPA Professor, *Court rejects SEC's broad internal controls enforcement theory*, July 18, 2024, https://fcpaprofessor.com/court-rejects-secs-broad-internal-controls-enforcement-theory/; Sullivan & Cromwell, *supra* note 45, Paul, Weiss *supra* note 45; Shelly Heyduk, Mia Gonzalez & Michele Wein Layne, *Lessons from Recent SEC Cyber Enforcement Actions*, Law360, Aug. 15, 2024, https://www.law360.com/articles/1870241/lessons-from-recent-sec-cyber-enforcement-actions.

[48] SolarWinds, 741 F. Supp. 3d at 78–88.

[49] *Proposed Brief for Chief Information Security Officers & Cybersecurity Organizations as Amici Curiae in Support of Defendants' Motion to Dismiss*, *SEC v. SolarWinds Corp.*, No. 1:23-cv-09518 (S.D.N.Y. Mar. 29, 2024), ECF No. 96-1, at 16–17 (proposed).

[50] SolarWinds, 741 F. Supp. 3d at 50–51; Amended Complaint at 1, 20, Sec. & Exch. Comm'n v. SolarWinds Corp. and Timothy G. Brown, No. 23-cv-9518-PAE (S.D.N.Y. Feb. 16, 2024), ECF No. 85.

[51] SolarWinds, 741 F. Supp. 3d at 85–86.

not sign or certify the company's filings and did not even review the precise language used in those filings, Brown was knowledgeable enough that he was "among the people responsible for the technical content and accuracy of the [company's] risk disclosure."[52]

The court's attention to the specific nature of Brown's role at the company indicates that his specific level of seniority did not shield him from, but instead ultimately exposed him to, liability. Brown was still low enough in the organization that he remained sufficiently "in the weeds" to receive detailed information about cybersecurity issues and thus to be aware "of the substantial body of data that impeached the Security Statement's content as false and misleading," but was senior enough to have some responsibility for the company's disclosures. That level of knowledge meant that Brown — who created and approved the Security Statement (discussed in greater detail below), disseminated it to customers, and allowed it to remain in place for years, "in the face of company practices inconsistent with it" — was "plausibly" alleged to have engaged in "highly unreasonable or extreme misconduct."[53]

Many of the arguments raised by the defense and amici in this case did not fall on deaf ears; they found a ready audience in the court. The court had no problem dispatching the SEC's arguments regarding its internal controls claims or those premised on SolarWinds's pre-breach risk disclosure or post-breach 8-K as, alternately, "incorrect," a "non-starter," lacking "perspective and context," "unpersuasive," and unable to be "squared with the statutory text."[54] But the court was not swayed by the defense's arguments that Brown was "a cybersecurity professional who had no executive position at the time or any role in investor relations,"[55] or by arguments that the case would encourage fraud claims against CISOs "who enforce[] a company's policies by maintaining open lines of communication with their team about potential compliance gaps."[56] Instead, the court focused on Brown's knowledge, his awareness of SolarWinds's poor cybersecurity hygiene, and his role in creating and disseminating statements touting the company's cybersecurity to the public over a period of years. From this, cybersecurity professionals should understand that the court's decision — while in many ways a defense victory — cemented their potential liability for public representations regarding the cybersecurity programs they oversee.

What and Where: The only portion of the case to survive accuses SolarWinds and Brown of engaging in securities fraud based upon the company's Security Statement. What was the Security Statement? It was a document aimed at "provid[ing] SolarWinds' *customers* with more information about its security infrastructure and practices."[57] Where was it made available? It was posted on the company's website, located in the "Trust Center" section. Brown also shared it with customers, "representing that it recounted how SolarWinds mitigated the risk of cyberattacks." And the company provided it "as its official response to customer questionnaires about its cybersecurity practices."[58] It was a customer-facing document, intended to assure companies and governments interested in buying products from a company "whose products (software) had cybersecurity as a key attribute and whose key clients (government agencies and Fortune 500 companies) expected the software they purchased to be and remain uncompromised."[59] The nature of the representation, its intended audience, and its location — a public website, not a Form 10-K annual report filed with the SEC — did not deter the court from finding a security fraud claim based upon the Security Statement actionable. The court swiftly rejected defendants' argument that they could not be held liable because the Statement "was directed to *customers*, not investors," calling that argument flat "wrong" and noting that "false statements on public websites can sustain securities fraud liability."[60]

Interestingly, the court dismissed the SEC's claims relating to the company's SEC filings (both before and after the breach was disclosed) and more casual communications with the public, such as press releases, blog posts, and podcasts. As to the former, the court deemed the disclosures in the former to be more than fulsome; the pre-breach disclosures "enumerated in stark and dire terms the risks the company faced were its cybersecurity measures to fail," while the post-breach

[52] *Id.* at 54.

[53] *Id.* at 86.

[54] *Id.* at 90, 97, 100, 108.

[55] *Securities & Exchange Comm'n v. SolarWinds Corp.,* No. 1:23-cv-09518, 2024 WL 752645, at *41 (S.D.N.Y. Feb. 22, 2024).

[56] *Proposed Brief for Chief Information Security Officers & Cybersecurity Organizations as Amici Curiae in Support of Defendants' Motion to Dismiss, at 17.*

[57] SolarWinds, 741 F. Supp. 3d at 51 (emphasis added).

[58] *Id.*

[59] *Id.* at 83–84.

[60] *Id.* at 79 (emphasis in original).

disclosures, "made at a time when SolarWinds was at an early stage of its investigation, and when its understanding of the attack was evolving," sufficiently "captured the big picture: the severity of the SUNBURST attack."[61] As to the latter, the court found they were "non-actionable corporate puffery, too general to cause a reasonable investor to rely upon them."[62] The court noted in particular that none of these more casual statements purported to describe SolarWinds's cybersecurity practices "at the level of detail at which a reasonable investor would have relied on them in making investment decisions."[63]

The district court's parsing of the different kinds of statements at issue is instructive. Documents that SolarWinds filed with the SEC, including in the "fog of war" following discovery of the breach, were deemed nonactionable; these kinds of statements, which presumably received considerable scrutiny and were subject to careful review by a variety of advisors, including regulatory counsel, passed muster. Other more episodic or casual statements — blog posts, remarks on a podcast, press releases — made no specific promises regarding the company's practices and thus presented little risk of misleading investors. The Security Statement seems to have been situated somewhere in between these two categories. It stated that SolarWinds "complied with the [NIST] Cybersecurity Framework," "used a secure development lifecycle to create its software products," "employed network monitoring," "had strong password protection," and "maintained good access controls."[64] It purported to describe the company's cybersecurity practices at a level of sufficient technicality and specificity that allowed the court to find that it was an actionable promise to investors and more than mere puffery. As a customer- rather than investor-focused communication, it is not hard to imagine that it did not undergo the kind of review that more formal communications with the investing public might receive before being made widely available and broadly disseminated.

When and Why: The last two elements in this analysis are perhaps the most important. The Security Statement was posted on the company's website beginning in late 2017, after Brown's arrival at the company, and it remained available and "virtually unchanged" throughout the years leading up to the discovery of the SUNBURST breach."[65] It was made during a period before the SUNBURST breach — when Brown and others within the company were aware of its "weak security" and the "very vulnerable state" in which the "[c]urrent state of security . . . leaves . . . our critical assets."[66] The court recounted in extensive detail allegations regarding internal discussions among company personnel throughout this period as to SolarWinds's "deeply flawed" cybersecurity program, highlighting problems that were "identified as early as mid-2017 . . . *before the Security Statement was posted on SolarWinds' website*."[67] The court's decision repeatedly refers to Brown's knowledge and failure to fix, escalate, or disclose security issues throughout the pre-breach period.[68]

The court's conclusions regarding the Security Statement seem to have been driven by this confluence of facts: the Security Statement was publicly available during a period when SolarWinds had, and was aware that it had, gaping holes in its cybersecurity. The Security Statement was disseminated during the years leading up to the breach when something could have been done about these risks. Instead of addressing the risks or revising the Security Statement, the company permitted a severe disconnect to persist between what company personnel knew and what was being said to the public. In ruling that the SEC's case could proceed as to the Security Statement, the court seized upon this disconnect and did not mince words, concluding that the Statement: contained "bogus claims," "prevaricated," "portrayed a diametrically opposite representation [from what the company knew] for public consumption," included "sustained public misrepresentations, indeed many amounting to flat falsehoods," and was "misleading if not outright false."[69]

III. CONCLUSION

For companies, boards, and cybersecurity professionals seeking to minimize risks, refresh their thinking on cybersecurity governance, and enhance their cybersecurity programs, the challenges are legion. The regulatory landscape presents uncertainty and complication. And the court's early decision in *SolarWinds*, while narrowing some areas of legal risk,

[61] *Id.* at 89, 100, 102.

[62] *Id.* at 89.

[63] *Id.*

[64] *Id.* at 51–52.

[65] *Id.* at 52 n.6.

[66] *Id.* at 50.

[67] *Id.* at 54, 60 (emphasis added).

[68] *Id.* at 62–63.

[69] *Id.* at 81–83.

does leave open fairly wide avenues to individual and corporate liability. At this particular juncture, the following observations may prove useful in designing a cybersecurity governance structure sturdy enough to withstand unanticipated risks:

Consider the "who" and prioritize legal expertise. Given the fragmented and patchwork state of cybersecurity regulation at both the federal and state levels, and rapidly shifting regulatory priorities, companies should seek out expert counsel with deep experience who are prepared to master regulatory complexity and, where appropriate, balance competing demands among regulators, including in situations calling for cross-border expertise. Companies should also ensure that those who, like Brown, oversee cybersecurity programs have appropriate training, guidance, and support in determining whether and how to escalate cybersecurity issues.

Consider the "why" and focus on internal elevation and external consistency. Many critics of the SEC's case have argued that it would "chill internal discussions and self-assessments," discouraging CISOs and their staff from engaging in "candid" debate or disclosure of vulnerabilities.[70] That argument does not appear to have swayed the court in *SolarWinds*, nor should any company conclude that quelling internal discussions will reduce cybersecurity risks. One key lesson of *SolarWinds* is that effective cybersecurity programs should include means to rationally and appropriately filter day-to-day complaints and notifications of "one-off instances of noncompliance"[71] so that matters that are systemic and significant can be elevated, addressed, and, where needed, disclosed.[72] What the court found problematic and ultimately actionable was the dire contrast between the internal dialogue regarding SolarWinds's cybersecurity and its outward representations. The solution is not to quell that internal dialogue, but rather to scrutinize outward representations to avoid any such mismatch.

Consider the "what," "where," and "when" and focus on communications outside of the "box." The court's ruling in *SolarWinds* is a clarion call for companies to focus on public communications that, like the Security Statement, may be situated somewhere between blog post and 10-K, and disseminated through means other than SEC filings and investor relations. Annual disclosures regarding cybersecurity management and governance now required under the 2023 cyber rule should of course receive due care and attention,[73] and disclosures (whether pursuant to Item 1.05 or otherwise) made in the aftermath of a data compromise should as well. But the viability of the SEC's case as to the Security Statement highlights the importance of examining statements that may receive little or no scrutiny from disclosure counsel, that may be publicly available and directed to non-investor audiences, and that may be made available in a forum not on the radar of compliance or in-house counsel. Ensuring that the right people are looking in the right places *before* a breach occurs may be half the battle. ■

[70] *Proposed Brief for Chief Information Security Officers & Cybersecurity Organizations as Amici Curiae in Support of Defendants' Motion to Dismiss*, at 15.

[71] *Id.*

[72] SolarWinds, 741 F. Supp. 3d at 63 (noting "Brown did not elevate [the VPN security weakness] or alert senior executives to the VPN security issue").

[73] One commentator has observed that boards of directors face heightened liability under *Caremark* and thus have increased incentives to appropriately oversee cybersecurity governance and disclosures in the wake of *SolarWinds*. Jennifer Arlen, *Caremark Liability for Materially Misleading Cybersecurity Disclosures: SolarWinds Reconsidered*, Harv. L. Sch. F. on Corp. Governance, Mar. 18, 2025, https://corpgov.law.harvard.edu/2025/03/18/caremark-liability-for-materially-misleading-cybersecurity-disclosures-solar-winds-reconsidered/.