ALM | LAW.COM

New York Law Journal

Protecting CISOs from the Growing Risk of Personal Liability

By Aravind Swaminathan, Joseph C. Santiesteban, Bradley A. Marcus and Benjamin Hutten
May 3, 2024

As cybersecurity attacks increase in sophistication, the financial and reputational impact for companies has never been more pronounced. For chief information security officers (CISOs) and other executives responsible for navigating a company through a data breach, the stakes are even higher.

CISOs confront significant personal civil and criminal liability in connection with their handling of breaches and associated disclosures. This raises serious concerns not only for CISOs and C-suite executives, but also for companies' abilities to secure expert personnel to safeguard their data and systems.

To protect executives on the front lines of cybersecurity incidents, companies should be alert to the issues discussed below and consider implementing best practices aimed at reducing the potential liability of key stakeholders.

SEC and DOJ Target CISOs in Their Individual Capacity

The liability landscape for CISOs shifted dramatically recently when the U.S. Securities and Exchange Commission (SEC) charged software company SolarWinds Corporation and its CISO, Timothy G. Brown, with fraud and internal control failures relating to cybersecurity risks and vulnerabilities. The charges followed a federal guilty verdict against another company's chief security officer arising from a separate and unrelated cybersecurity incident.

Photo: ljeab via Adobe Stock

The SEC action marked the first time the Commission has charged a CISO. In bringing both substantive and aiding-and-abetting violations of securities laws, the SEC alleged Brown made false statements regarding the company's security practices and a 2020 security incident. The agency filed a more detailed amended complaint in February 2024, depicting Brown as the leader of a "scheme to convince the public and actual or potential customers that the company was following industry-standard cybersecurity practices when—in

fact—it did not follow many of them[.]" *SEC v. SolarWinds et al.*, SDNY Case No. 23-cv-9518, Am. Compl. ¶ 57.

The SEC seeks significant monetary penalties and a permanent ban on Brown's ability to serve as an officer or director in any public company. The matter is pending a ruling on the defendants' motions to dismiss.

New Rules and Regulations Regarding Cybersecurity

Recent cybersecurity rules by the SEC and regulations by New York Department of Financial Services (NYDFS) suggest that CISOs are at risk for further breach-related enforcement actions.

SEC Cybersecurity Disclosure Rules

In December 2023, the SEC's cybersecurity disclosure rules became effective, obligating regulated companies and their CISOs to make timely disclosures related to material cybersecurity incidents and cybersecurity risk-management programs, strategy, and management's role in assessing and managing material cybersecurity risks.

A CISO is critical to a company's ability to comply with these rules, and CISOs are now actively involved in disclosure decisions. However, despite a CISO's well-intentioned actions, the SEC could seek to hold a CISO liable based on its own after-the-fact assessment regarding what should or should not have been disclosed, detected, and/or prevented.

At the time it charged Brown and SolarWinds, the SEC had not issued these new rules. Rather, the SEC relied upon a traditional methodology to claim that Brown misled investors about the company's cybersecurity practices and known risks. The new regulations allow the SEC to rely on specific cyber-related requirements aimed at holding individuals accountable for breach-related incidents.

NYDFS Cybersecurity Regulations

The NYDFS also appears to be targeting CISOs in their personal capacity for company-wide cybersecurity failures. Although the NYDFS has yet to file an enforcement action charging a CISO, its 2023 amendments to its Cybersecurity Regulations suggest it is not a question of *if* but *when* NYDFS files such an action. Indeed, one key and recently effective provision requires the CISO of a covered entity to submit an annual certification of compliance regarding the Cybersecurity Regulations (23 NYCRR §500.17), thus putting the CISO's conduct under scrutiny.

To the extent hindsight reveals these certifications are inaccurate, and depending on the circumstances, the NYDFS may follow the SEC's enforcement action against Brown and seek to hold CISOs liable based upon its certification requirements. *See SEC v. SolarWinds et al.*, SDNY Case No. 23-cv-9518, Am. Compl. ¶ 22 (alleging inadequacies of "sub-certifications attesting" to cybersecurity internal controls).

Companies Can Protect Their CISOs by Implementing Certain Practices

The SEC has not published formal guidance identifying the factors it will consider when charging a CISO or related cybersecurity executive. However, public statements by SEC officials are instructive.

SEC Enforcement Director Gurbir S. Grewal recently compared potential individual liability of CISOs to chief compliance officers (CCOs), stating that CISOs and CCOs "who operate in good faith and take reasonable steps are unlikely to hear from us." *See* Grewal, Remarks at Program on Corporate Compliance and Enforcement Spring Conference 2024, April 15, 2024. Grewal has also suggested that the SEC

will only bring enforcement actions against a compliance officer in "rare" instances where the officer:

• "Affirmatively participated in misconduct unrelated to the compliance function."

• "Misled regulators."

• "Where there was a wholesale failure… to carry out their compliance responsibilities." *See* Grewal, Remarks at New York City Bar Association Compliance Institute, Oct. 24, 2023.

The first two instances are straightforward, but the third gives the SEC wide discretion in deciding when a CISO has engaged in "wholesale failure[s.]" Without clear guidance on what constitutes "wholesale failures[,]" companies should proactively take steps to protect their CISOs and other cybersecurity executives. To that end, companies should consider adopting and implementing some or all of the following "best practices," several of which are drawn from cybersecurity governance requirements issued by the NYDFS and Federal Trade Commission.

• **Establish clear reporting lines and decision-making protocols.** Companies should document and regularly update protocols that outline how a CISO reports to the board of directors and management. This includes processes for promptly reporting and escalating cybersecurity risks and incidents with clear documentation of the information provided and the decisions made.

The NYDFS has codified this requirement in its recent Cybersecurity Regulation (23 NYCRR §500.4). When effective in November 2024, the regulation will require enhanced reporting by the CISO to the board. It also will require board oversight of cybersecurity risk management for NYDFS-covered entities.

For FTC-regulated financial institutions, CISOs must report in writing, regularly and at least annually, to their boards or equivalent governing body. 16 C.F.R. §314.4(i). It should also be clear who the decision-maker is for risk acceptance and key incident response functions.

• **Maintain a robust cybersecurity framework.** Companies should implement a cybersecurity framework that aligns with recognized standards (*g.*, NIST, ISO/IEC 27001) and is tailored to the specific risks an organization faces. This includes conducting regular risk assessments and updating the cybersecurity framework accordingly. *See, e.g.*, 23 NYCRR §500.9, which requires at least annual updates to cyber risk assessments, and whenever a change in the business or technology causes a material change to the business' cyber risk.

• **Develop and test an incident response plan (IRP).** Companies should create a business-wide IRP that aligns to NIST 800-61 and includes legal considerations, such as notification timelines and regulatory compliance. The plan should include means for assessing severity based on factors that include operational impact, data impact, reputational impact, and financial impact. The IRP should direct escalation to legal departments, management and the board depending on the incident's severity. The company should test the plan regularly with critical staff through tabletop exercises and revise it based on lessons learned. *See* 23 NYCRR §500.16.

• **Stay on top of legal and regulatory obligations.** Keep apprised of evolving cybersecurity laws and regulations that affect an organization, both domestically and internationally, and establish policies and procedures for compliance. Making specialized resources and training available to the CISO and key personnel can support this endeavor.

• **Implement a detailed record-keeping protocol.** Companies should develop and implement a detailed record-retention protocol related to cybersecurity management, including policies and procedures, training and incident response.

• **Promote a strong CISO/legal counsel culture and relationship.** The lawyer-CISO relationship should start early by building a framework for counsel and the CISO to work together so the company can make effective, informed decisions. Legal counsel should be involved in reviewing and drafting policies and procedures, IRPs and vendor contracts, and in investigating incidents.

• **Foster a culture of ethical conduct and transparency.** Companies should promote a culture of transparency regarding cybersecurity risks and incidents with the relevant stakeholders.

• **Secure adequate cybersecurity insurance.** Companies should negotiate director and officer insurance policies to include comprehensive coverage for CISOs. They also should scrutinize these policies because not all of them cover the types of claims commonly brought in cybersecurity enforcement or litigation, *g.*, consumer protection claims.

• **Provide sufficient resources, including continuing education.** Companies should make appropriate resources available to the CISO so the CISO can implement effective cybersecurity measures and appropriately respond to incidents.

Conclusion

Although the above frameworks are not legal standards, and aligning to them is not a silver bullet, they can demonstrate management's commitment to cybersecurity and contribute to an effective cybersecurity program. Following these practices will demonstrate good faith efforts by CISOs to fulfill their responsibilities and can significantly reduce the potential for their personal liability.

Aravind Swaminathan (*Partner, Orrick, Cyber, Privacy and Data Innovation)* helps clients, including chief information security officers, navigate a new world of regulatory risk, from cybersecurity incidents to online trust and safety to defending executives in high-stakes litigation and enforcement actions.

Joseph C. Santiesteban (*Partner, Orrick, Cyber, Privacy and Data Innovation)* is a trusted cybersecurity lawyer and strategic advisor, who regularly steers clients through data breaches as a partner in crisis management.

Bradley A. Marcus *(Partner, Orrick, White Collar, Investigations and Compliance)* is a white collar and complex civil litigator with over 15 years of experience representing corporate and individual clients in their most high-stakes civil and criminal enforcement actions, investigations and litigation.

Benjamin Hutten *(Partner, Orrick, International Trade and Investment)* provides global compliance, investigation and defense services to a wide range of foreign and domestic financial institutions, fintechs, corporations, and individuals.

Aravind, Joe, Brad and Ben are members of Orrick's Technology Enabled Crimes team, which provides advice to companies and senior executives on risk and incident response arising from cybersecurity threats.