protiviti®
Global Business Consulting

Are SEC Charges Against SolarWinds and Its CISO Signalling a New Era of Personal Accountability?

November 3,
2023

On October 30, the U.S. Securities and Exchange Commission (SEC) announced charges against SolarWinds, a software company, and its chief information security officer (CISO) for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. The company previously reported in June that certain current and former executive officers, including the CISO, had received Wells notices[1] in connection with an SEC investigation. Because the company's disclosures at that time were lacking in specifics, there was much speculation in the press and among law firms as to why the Wells notices were issued and, more importantly, the takeaways for issuers, CISOs and other executives going forward.

Historically, the SEC has focused on the CEO and CFO, or equivalent roles, insofar as executive officer accountability is concerned. They sign the quarterly executive certifications and the annual internal control assertions, as required by the Sarbanes-Oxley Act of 2002. The speculation around the Wells notices to a SolarWinds non-certifying executive is whether it is an indication of the SEC adopting an expanded view of executive accountability in public reporting companies. While a new move on the board for the SEC, this is not the first regulatory accountability extension of its kind. Other regulators, particularly in the financial services industry, have been extending enforcement actions further into the C-suite by, for example, holding chief compliance officers to account for regulatory failures.

The Commission's Allegations

The complaint alleges that, from at least SolarWinds' October 2018 IPO through at least its December 2020 announcement that it was the target of a massive, nearly two-year long cyberattack, the company and its CISO defrauded investors by overstating its cybersecurity practices and understating or failing to disclose known risks. Specifically, it is alleged that:

[1] A Wells notice is a communication that the SEC staff is considering bringing an enforcement action against the recipient alleging violations of U.S. securities laws.

- In its filings with the SEC during this period, SolarWinds allegedly misled investors by disclosing only generic and hypothetical risks at a time when the company and CISO knew of specific deficiencies in cybersecurity practices as well as increasingly elevated risks the company faced.
- The company's public statements about its cybersecurity practices and risks were at odds with the CISO's internal assessments, presentations and statements.
- There were multiple communications among company employees, including the CISO, throughout 2019 and 2020 questioning the company's ability to protect its critical assets from cyberattacks.
- The CISO ignored repeated red flags about the company's cyber risks which were well known throughout the company and was aware of cybersecurity vulnerabilities but failed to either resolve the issues timely or, at times, sufficiently escalate them within the company.

As a result, the SEC alleges that the company was not in a position to provide reasonable assurance that its most valuable assets, including its flagship Orion product, were adequately protected. The commission further asserts that the company and CISO engaged in a campaign to paint a false picture of the company's cybersecurity control environment, thereby depriving investors of accurate material information.

A New Era of Personal Accountability in Public Reporting?

The SEC stated in its October 30 release[2] that its enforcement action not only charges the company and the CISO "*for misleading the investing public and failing to protect the company's 'crown jewel' assets, but also underscores [its] message to issuers: implement strong controls calibrated to your risk environments and level with investors about known concerns*." This statement conveys zero tolerance for neglect and indifference to properly informing investors of material information. The charges against the CISO also imply that, in any situation involving an egregious omission of material facts in reports to the investing public, the SEC staff would seek to track down culpable executives.

CISOs and other functional leaders in public companies should take note of the potential for increased oversight of their operations by the SEC to the extent that they are involved with activities, decisions, information and risks affecting financial reporting and other public disclosures. They should be mindful of potential exposure to violations of the federal

[2] "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures," U.S. Securities and Exchange Commission, October 30, 2023: www.sec.gov/news/press-release/2023-227.

securities laws, as all may be required to provide data that are directly or indirectly incorporated into SEC filings. In effect, the SolarWinds case may be much more than a wake-up call for CISOs. As an indicator of a potential expansion in personal accountability emerging in public reporting, it is a matter of interest to all C-level executives to consider what they can do to avoid personal liability.

Addressing this expansion of personal accountability requires companies to enable it and individual executives to perform to it. With that in mind, following is a summary of nine points for executives of SEC registrants and those functional leaders potentially impacted to consider:

- **Advocate for a culture of effective risk governance and compliance.** This is square one. Effective risk governance and balanced incentives set the tone for quality public reporting and disclosure and a strong control environment. In addition to focusing on protocols relating to financial and non-financial reporting compliance, SEC registrants should employ a robust risk governance culture as well as compliance and internal audit functions emphasising core values and monitoring and reporting on enterprise risk and adherence to applicable laws, regulations and internal policies. Everyone has a stake in an effectively functioning risk management and compliance culture.
- **Create awareness of the importance of public disclosure under the federal securities laws.** Responsibility for the adequacy of public disclosures ultimately falls to everyone possessing and contributing information either required by statute or regulation or deemed material to investors. This means:
    - Everyone should be aware of the disclosure implications of their respective activities.
    - Reporting needs to be an integral part of every manager's job.

  For some organisations, this will require a change in mindset – hence, the focus on personal accountability.
- **Ensure there is clarity on corporate roles and responsibilities.** Many organisations have a disclosure committee, charter, policies and procedures. But disclosure committees as well as the disclosure process need the right information reported through appropriate channels to function effectively. If there isn't timely access to the needed information, their effectiveness is diminished. That is why everyone engaged, either directly or indirectly, in the disclosure process has an

important role to play regardless of whether they serve on the disclosure committee. The roles and responsibilities of this committee, individual executives, financial and public reporting preparers, and other contributors to the disclosure process should be delineated and coordinated.

- **Engage appropriate internal stakeholders.** Engagement is a two-way street. Executives with overall responsibility for financial statements and other public reports should ensure that their peers in the C-suite and across business units, functions and geographies, as well as appropriate subject-matter experts in complex areas, are aware of significant matters under their auspices having disclosure implications. Likewise, if there are issues in a specific domain that have potential disclosure implications, it is the responsible executive's duty to ensure sufficient resources are brought to bear to obtain the necessary insights to satisfy disclosure requirements. For that reason, communications of changes in disclosure requirements should be timely.
- **Enable individual executives who are at risk.** Executives who own activities, decisions and information having significant public reporting implications and who must perform to expectations should be empowered with a clear mandate, have the authority to initiate positive change and, as noted above, be adequately resourced. The above focus on risk governance and compliance, creating awareness, delineation and coordination of roles, and effective engagement should enable a "speak up" culture with respect to fair and reliable reporting. To that end, escalation protocols should facilitate unfiltered communications to the audit committee on sensitive matters, particularly if the individual does not have direct board access privileges. Depending on the nature and significance of an executive's responsibilities, an actual or a consultative seat at the table of the disclosure committee (or its equivalent) may be appropriate.
- **Encourage everyone signing an internal certification to take a pause.** Many larger organisations support the Sarbanes-Oxley Section 302 quarterly executive certifications with an internal sub-certification process in which unit, functional and geographical leads and others charged with reporting and disclosure responsibilities represent that they provided appropriate information for external reporting and disclosure purposes and maintain appropriate internal controls. All at-risk executives should be satisfied they have discharged their respective reporting responsibilities before signing these "backup certifications."

- **Enhance the disclosure process with a chain of accountability.** Backup certifications supporting the quarterly executive certifications provide a "chain of certifications." They typically mirror the executive certification representations and do not necessarily provide assurance that reliable information is being furnished to management for timely disclosure. As an alternative, a "chain of accountability" arises from clearly linking required disclosures to the internal reporting processes that are designed to deliver the necessary information in a timely manner to those making disclosure decisions. For disclosure processes that pertain to critical issues, such as cyber breaches, the company should encourage the responsible executives to evaluate the related risk and control points, identify gaps and formulate action plans to close the gaps. A clear focus on data sources, reporting accuracy and clarity, and the controls around reporting and appropriate disclosure reinforces a culture of personal accountability, which also enhances awareness.

- **Periodically evaluate the effectiveness of the disclosure process.** An assessment of the disclosure controls and procedures infrastructure should consider the organisation's performance expectations, incentive compensation programs and other behaviour-influencing practices that may impact fair reporting. Identified control points provide the basis for developing appropriate metrics and for focusing process-owner monitoring. They also provide a business context for focusing internal audit plans. The results of process owner monitoring and internal audits should be reported to the responsible executives and to the disclosure committee for review. The disclosure committee should remain abreast of new and emerging disclosure risks and assume responsibility for determining whether there are any aspects of the company's culture that could frustrate the goal of fair reporting. Responsible executives should escalate any concerns regarding the efficacy of disclosure controls and procedures. For example, if a significant component of the CFO's and accounting management's compensation is linked to profits, that approach should be examined to ensure there is adequate balance given to quality reporting.

- **Recognise that sustainability (ESG) and other emerging non-financial reporting and disclosures are expanding the boundaries of personal accountability in public reporting.** Executives reporting ESG and other non-financial data which ultimately are incorporated in SEC filings and other venues should be satisfied that there is sufficient rigor in ensuring its completeness, accuracy and consistency. This responsibility entails having in place effective disclosure controls

and procedures.[3] It may be just a matter of time before the SEC staff makes an example of individuals responsible for misleading disclosures in this space.

Finally, as a certifying officer, the CFO should take the lead in reinforcing the importance of everyone's role in providing reasonable assurance of fair presentation of public disclosures. Equally important, the CEO should set the proper tone for fair and reliable reporting with respect to the organisation's functions residing outside of finance. Chief information officers have an increasingly important role to play in overall information technology audit governance, which impacts financial reporting systems. The audit committee should inquire about the rigor and approaches to reporting the expanding list of financial and non-financial data required in SEC filings, including the efficacy of the underlying disclosure controls and procedures and any planned *external* audit or assurance that will be needed. Similarly, *internal* audit functions should continually evolve, staying abreast of the shifting business and risk landscape and discussing resource constraints with the audit committee as well as any scope limitations that may be placed on their activities.

The Key Takeaway

All significant parties with a hand in public reporting, whether direct or indirect, should consider themselves an integral part of the personal accountability chain. The SolarWinds case underscores the need for any C-suite member or unit, functional or geographical leader who is a contributor to public reporting to take this responsibility seriously. If indeed the SEC is going to enforce personal accountability, companies should focus more on internal awareness, including formal training throughout the chain of accountability regarding compliance with applicable laws and regulations and a clear delineation of internal responsibilities. They also should ensure there are effective escalation and reporting channels as well as adequate resourcing, and that they inform the board and audit committee timely of significant issues. In addition, individual executives owning activities, decisions and information having significant public reporting implications should measure up to their respective responsibilities to support the company's compliance with the federal securities laws.

[3] "COSO Issues Supplemental Guidance on Internal Control Over Sustainability Reporting," Protiviti Flash Report, March 30, 2023: www.protiviti.com/us-en/flash-report/coso-issues-supplemental-guidance-internal-control-over-sustainability-reporting?utm_source=COSO+Infographic&utm_medium=referral&utm_campaign=COSO+Flash+Report.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 *Fortune* 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®