

Redefining the Cybersecurity Paradigm: CISOs and Boards in the Wake of Regulatory Shakeups

Article By:

Avery Simmons

In an age where cyber threats loom large over the financial sector's horizon, recent regulatory actions signal a paradigm shift in the regulatory framework governing cybersecurity for publicly traded companies. The amplified role of the chief information security officer (CISO) and heightened duties given to boards of directors herald a new era of cyber vigilance and accountability. As regulators increasingly focus on individual accountability for CISOs and may commence enforcement actions on this front, CISOs and boards should reassess how to handle their cyber strategy going forward.

Expanding the Role of the CISO

Traditionally viewed as the technical guardians of an organization's digital fortresses, CISOs are finding themselves front and center in the regulatory and governance spotlight. On Oct. 30, the SEC announced fraud charges against SolarWinds and its CISO following recently implemented disclosure requirements relating to cyber risk, the outcome of which could set the precedent to hold CISOs individually accountable for their organization's cyber resilience. Despite the original disclosure requirements not singling out CISOs for personal liability, the agency justified its action by alleging in its complaint that the company's public statements on its cybersecurity risks contradicted its internal assessments, thus misleading investors. New amendments to cybersecurity regulations for financial institutions under the New York Department of Financial Services (NYDFS) appear to have a similar aim in holding CISOs personally accountable for organization cybersecurity vulnerabilities – one provision mandates that the CISO, along with the organization's highest-ranking executive, annually certify compliance with the state's Cybersecurity Regulations.

These regulatory developments have the potential to redefine the role of the CISO, bridging the gap between the technicality of cybersecurity and the strategic imperatives of executive leadership. CISOs are obligated to personally certify compliance under the NYDFS amendments, increasing the incentives to be more hands on throughout the process should they risk incurring personal liability. For compliance, CISOs will not only keep abreast of the kaleidoscope of cyber threats but also possess a firm grasp of the regulatory terrain that shapes their strategic response. The NYDFS amendments stipulate that CISOs must articulate a clear, actionable narrative of cybersecurity postures to their boards, encapsulating the subtleties of risk and the nuances of tactical response. While these regulations are specific to New York, should regulators in other states follow suit, CISOs of firms across the country could see the risk of personal liability in organizational cybersecurity

matters on the horizon. Yet, this prospect could in turn further professionalize the CISO role, as it would encompass a panoramic view of the organization's cyber health, flag material cybersecurity issues, and chart a course through the maelstrom of potential cyber events, all while ensuring alignment with overarching business goals.

A New Doctrine for Directors

Should NYDFS be adopted in more jurisdictions, boards of directors, traditionally distanced from the granularities of cybersecurity, will need to take a more hands-on role. The NYDFS regulation's governance obligations for cybersecurity requires that the board of directors or equivalent governing body oversee the organization's cybersecurity risk management, possessing a sufficient understanding of cybersecurity-related matters, as well as providing sufficient resources for managing the cybersecurity program. Additionally, the SEC's enforcement posture, punctuated by the landmark SolarWinds litigation, could underscore the board's duty to exercise rigorous oversight over cybersecurity disclosures and to engage deeply with the material impacts of cyber risks. Given that the board has a fiduciary duty to shareholders to oversee the risk management practices of the company, cyber risks are likely to increasingly become a part of the calculus in board members' decision-making. Oversight would become more critical as regulatory bodies heighten their scrutiny of how companies manage and report cyber risks.

The implication is that boards would need to possess or more directly access cybersecurity expertise, not merely to satisfy regulatory edicts but to foster a culture of cyber resilience through close coordination and collaboration with CISOs on cybersecurity strategies. It would be the board's ultimate responsibility to hold the company's executives, including the CISO, accountable for the effectiveness of their cybersecurity program and their actions in the event of a breach. The board's responsibility in this case extends to a more active role beyond fiduciary oversight, entailing active engagement in strategic cyber risk management and ensuring that cybersecurity measures are interwoven with business continuity and growth strategies.

Personal Liability at the Forefront

With the SEC's enforcement of its most recent cybersecurity disclosure requirements and legislation like the NYDFS amendments taking place, with the potential for regulations in more jurisdictions to follow suit, the specter of personal liability looms large for CISOs and potentially, other board members. No longer insulated by the collective shield of corporate personhood, individuals could face the prospect of being held personally accountable for lapses in cyber governance. The SolarWinds case serves as a stark reminder that misrepresentation or inadequate disclosure of cybersecurity vulnerabilities may lead to severe legal repercussions.

For CISOs, the risks, whether financial, legal, or reputational, present potential pitfalls where each step – from response to a cyber incident to the communication strategy surrounding it – could lead to fallout if not carefully navigated. The quest for personal legal safeguards, such as robust directors and officers (D&O) insurance coverage and indemnification provisions, is a potential strategy in mitigating this newfound risk. Yet, the devil can be in the details. Depending upon the corporate structure, D&O coverage may not spread to the CISO's position or have broad cyber exclusions.

For boards, the threat of personal liability remains, as the door is open for regulators to expand enforcement mechanisms. Cases like SolarWinds may propel boards to take a more proactive stance on cybersecurity, recognizing how the way cyber risks are managed and communicated can have substantial legal, financial, and reputational consequences. Boards will face the responsibility of

ensuring that senior management, including the CISO, is equipped to address cybersecurity challenges effectively. One potential pitfall is the prospect that new regulations solely targeting CISOs for personal liability may reduce trust between the CISO and the board, hindering the compatibility of cybersecurity strategy with business goals should CISOs seek to protect their individual interests over those of their company. This makes proper planning and collective accountability between CISOs and boards even more important in strengthening organizational resilience amid future regulatory waves.

Conclusion

The recalibration of roles and liabilities for CISOs and boards is emblematic of a broader recognition of cybersecurity as a critical pillar of organizational integrity and shareholder value. New regulatory frameworks and rules in the making create an environment where cyber governance is not an IT concern but a central tenet of corporate stewardship. Potential downsides remain, such as the risk of publicly shared information on organizational cybersecurity vulnerabilities becoming exploited by hackers. In addition, the present gap in training for CISOs, who tend to be more technical-focused, and board members, who may be more business-minded, could serve as a hurdle in presenting a solid action plan for the responsibilities being demanded of these roles. Yet, while the legal, financial, and reputational risks for CISOs and boards are evident, a silver lining remains for the paradigm shift to further professionalize the roles to be more accountable to modern-day cybersecurity challenges. When communicating the cyber vulnerabilities that an organization faces to investors, transparency is of utmost importance; making misleading or false claims to investors necessitates the SEC to act.

Expectations of cyber governance are changing, requiring organizational leadership to face increased accountability in managing related risks. As regulators redefine the responsibilities of roles and potential liabilities, CISOs and boards will have strong incentives to adapt and evolve, fortifying their cyber defenses and governance practices in lockstep with the shifting sands of the regulatory landscape. The challenges are formidable, but so too are the opportunities to redefine leadership in the digital age.

William Samir Simpson contributed to this article.

© 2025 Bradley Arant Boult Cummings LLP

National Law Review, Volume XIV, Number 18

Source URL: <https://natlawreview.com/article/redefining-cybersecurity-paradigm-cisos-and-boards-wake-regulatory-shakeups>