Psaros Center for Financial Markets and Policy

GEORGETOWN UNIVERSITY McDonough School of Business

Cyber Risk and SEC Regulations: Navigating Boardroom Responsibilities

Marshall Lux
Visiting Fellow

Rohan Mistry
Research Assistant

Georgetown University's Psaros Center for Financial Markets and Policy

McDonough School of Business

May 2024

Introduction

In an era defined by complex data relations interconnecting all that we do, the proliferation of cyber threats poses significant challenges to stakeholders across sectors. The global cost of cybercrime is estimated to total $10.5 trillion by 2025.[1] As long-term developments such as generative AI, machine learning, and the Internet of Things continue to materialize, businesses across all industries must seriously consider cyber risk as a top priority for their management and Board of Directors.

As these advancements continue to unfold, so do the tactics of cybercriminals, who exploit vulnerabilities in systems with ever-increasing sophistication. The consequences of cybercrime are not just financial; they can also erode trust, damage reputation, and disrupt operations on a global scale. Amid this turbulent landscape, the role of the company board emerges as pivotal. In the aftermath of high-profile breaches like the SolarWinds incident, the importance for members of corporate Boards of Directors to be well-versed in cybersecurity matters has never been clearer. The responsibility is further enhanced in July 2023 through new regulations adopted by the U.S. Securities and Exchange Commission (SEC) that address how public companies must handle material cybersecurity attacks. Board members must not only stay abreast of the idiosyncratic risk within the cybersecurity realm but also actively foster collaboration and communication between key stakeholders, notably the Chief Information Security Officer (CISO) and other frontline defenders.

Breaking down silos between departments is paramount as effective cybersecurity defense requires a holistic approach that transcends organizational boundaries. By promoting a culture of vigilance and resilience, board members can empower their organizations to navigate the complex cyber threat landscape with confidence and agility. Furthermore, in response to evolving regulatory landscapes shaped by the SEC, board members must remain agile in adapting governance frameworks to ensure compliance and mitigate legal risks and be prepared to engage in immediate reporting plans in the situation that an 8-K must be published. As governments enact new laws and regulations to bolster cybersecurity measures, board members must proactively engage with regulatory bodies and stay ahead of compliance requirements to safeguard their organizations from potential liabilities.

The Evolution of the CISO

The role of the CISO has considerably transformed and continues to evolve in step with today's challenges and demands. According to one survey by Cisco, 86% of CISOs say that the role has changed so drastically that it has almost become a different job, particularly due to the role's ballooning responsibilities and relevance to the board.[2]

---

[1]Muggah, R. & Margolis M. (2023, January 2). Why we need global rules to crack down on cybercrime. *World Economic Forum*. https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/

[2] Splunk. (2023). The CISO report. *Cisco*. https://www.splunk.com/en_us/pdfs/gated/ebooks/the-ciso-report.pdf

Steve Katz became the world's first CISO when he was hired at Citicorp in 1995. At that time, the CISO role was viewed as a technical, niche occupation within the business's risk management and compliance operations.[3] Historically, boards of directors have often viewed cybersecurity as a technical issue rather than a strategic business concern. CISOs were originally in charge of cybersecurity working under the direction of the Chief Information Officer (CIO). In time, the increasing prevalence and high-profile nature of cyber attacks such as those against Target (2013)[4], Equifax (2017)[5], and SolarWinds (2019)[6] have ballooned the importance of the CISO relative to other board positions.

Instead of focusing on IT compliance and regulation, today's CISOs now focus on helping organization leaders understand the importance of cybersecurity and drive cybersecurity strategy.[7] This often involves issues beyond the organization, such as building partnerships, working with suppliers, and ensuring the safety of vendors. The role requires a unique combination of business and technical acumen; CISOs bridge the gap between the technical lingo of the IT department and the strategy discussions of business leadership. This is reshaping organizational structure; 47% of CISOs now report directly to their CEO.[8]

The Significance of SolarWinds and Corresponding Action by the SEC

SolarWinds is a Texas-based network management company that provides IT solutions to both businesses and the federal government. Beginning in September 2019, a series of attacks breached SolarWinds' networks. Rather than attacking the business itself, the hackers utilized a method known as a supply chain attack, which targets a third party to the business. In this case,

---

[3]Townsend, K. (2021, December 1). CISO conversations: Steve Katz, the world's first CISO. *SecurityWeek.* https://www.securityweek.com/ciso-conversations-steve-katz-worlds-first-ciso/

[4]In 2013, cyber thieves gained access to Target's internal records by installing malware through one of Target's third party vendors. The financial and personal information of as many as 110 million Target customers were removed and downloaded to a server in Eastern Europe.

Committee on Commerce, Science, and Transportation. (2014, March 26). A "kill chain" analysis of the 2013 Target data breach. *United States Senate*. https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

[5]In 2017, Equifax, one of the world's largest consumer reporting agencies (CRA), reported a massive data breach impacting 148 million consumers. Hackers had access to incredibly sensitive data, such as names, Social Security numbers, dates of birth, addresses, credit card numbers, etc. Equifax was ordered to pay $575 million as part of a settlement with the FTC, CFB and US States. The FBI indicted four Chinese military-backed hackers in connection with the data breach.

Committee on Oversight and Government Reform. (2018, December). The Equifax data breach. *United States House of Representatives.* https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf
https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

[6]See "The Significance of SolarWinds and Corresponding Action by the SEC"

[7]Gregory, J. (2024, April 2). The evolution of a CISO: How the role has changed. *SecurityIntelligence.* https://securityintelligence.com/articles/ciso-role-evolution/

[8]Splunk. (2023). The CISO report. *Cisco*. https://www.splunk.com/en_us/pdfs/gated/ebooks/the-ciso-report.pdf

that would be Orion, SolarWinds' line of products. Over 30,000 public and private organizations, including local, state, and federal agencies, use the Orion network management system. In February 2020, the hackers uploaded the malicious code known as SUNBURST into Orion. The malicious code allowed the intruder to have remote access to an infected computer. Beginning in March, SolarWinds unknowingly spread SUNBURST during its rollout of updates to the Orion system and its users.

It was not until November 2020 that FireEye, a security professional services firm, detected an intrusion into its system. In coordination, Microsoft had also reported that several of its services and cloud platforms were compromised, many of which are used by several federal agencies. Most notable of those impacted include Homeland Security, the Department of State, the Department of Commerce, and the Department of the Treasury. While the purpose of the attack is still unknown, it is suspected that the deep and broad reach of the data would have been used for ransom or espionage.

On October 30th, 2023, the SEC announced it had filed charges against both SolarWinds and its CISO Timothy Brown in connection to the cyber attack. This notable lawsuit was the first time an individual was directly charged with cybersecurity enforcement claims by the SEC.[9] A key trend throughout the complaint is that management was aware of the cybersecurity deficiencies but rather lied to its customers and investors by painting a misleading image of the strength of SolarWinds' risk management practices. Specifically, the complaint alleges:

- SolarWinds' public statements about its cybersecurity were misleading when in fact it "had no program/practice in place for the majority of the controls."[10]
- SolarWinds failed to make any specific disclosures after it had learned of a series of security breaches experienced by the U.S. government and cybersecurity companies in 2020.
- SolarWinds failed to devise and maintain internal controls to protect its critical assets.

As the SolarWinds case continues to shape board responsibility in cyber, the SEC issued new requirements for cybersecurity disclosures in July of 2023. The new rules have two main components[11]:

1. Material cybersecurity incidents would need to be disclosed to investors within four business days by filing an 8-K. An 8-K, also known as a "current report" is an unscheduled document publicly traded companies file with the US SEC. This would

[9]Pittman, P. et al. (2023, November 14). The SEC's charges against SolarWinds and its Chief Information Security Officer provide important cybersecurity lessons for public companies. *White&Case*. https://www.whitecase.com/insight-alert/secs-charges-against-solarwinds-and-its-chief-information-security-officer-provide

[10]United States Securities and Exchange Commission. (Filed 2023, October 30). US SEC v. SolarWinds Corp. and Timothy G. Brown, Complaint. *US SEC.* https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf

[11]United States Securities and Exchange Commission. (2023, July 26). Cybersecurity risk management strategy, governance, and incident disclosure. *US SEC.*https://www.sec.gov/corpfin/secg-cybersecurity

include the incident's nature, scope, timing, and estimated impact on the registrant. This is an all-encompassing rule: there is no exemption or safe harbor for events occurring to third-party vendors. Registrants may still need to report events impacting these vendors if they are part of the "regular channels of communication" of the business.[12] The filing serves as a timely notification to investors of significant changes within the company, such as material acquisitions, major financial/operational changes, or bankruptcy. An exception by the U.S. Attorney General could be made if publishing the material risk in an 8-K poses a national security threat.

2. Annual disclosure of cybersecurity risk management, strategy, and governance will need to be made in the 10-K, as part of Item 106. This will include the process of how a firm specifically assesses, identifies, and manages cybersecurity threats. Additionally, *Item 106 will require companies to describe the board of directors' oversight of cybersecurity risk and management's role and expertise in dealing with such dangers.*

Overall, the final rule aims to address concerns over investor access to timely information related to cybersecurity as a result of the widespread use of technology, artificial intelligence, and the increasing relevance of profits from ransomware.[13] This rule, in addition to the SolarWinds case, makes it clear the SEC will be examining all records of the company, not just SEC filings. Documentation will be integral. While the SEC claims that the new regulation provides more transparency and accountability, there still exists pushback by CISOs and uncertainty around discerning what is considered "material."

Initial Responses and a Potential CISO Chilling Effect

The U.S. government, particularly the SEC, is making it clear that cybersecurity is a serious boardroom concern and no longer just a matter of statutory compliance. As cyber breaches become increasingly prevalent and impactful, board members are faced with the challenging task of discerning what constitutes a material risk to the organization. This determination is no longer straightforward, as the potential ramifications of cyber incidents extend far beyond financial losses to encompass reputational damage, regulatory scrutiny, and even existential threats to the business.

There has been pushback from the CISO community in response to the SEC complaint and new rules. The SEC's move to link security incidents with personal liability for CISOs through the SolarWinds case has triggered concerns and resistance among security professionals. This newfound accountability places CISOs in a defensive posture, as they grapple with the implications of shouldering legal responsibility for cybersecurity failures. While CISOs may acknowledge the need for improved transparency regarding cybersecurity risks to shareholders, many harbor reservations about the SEC's tactics. The imposition of personal liability raises the

[12]Mazor, C. et al. (2023, July 30). SEC issues new requirements for cybersecurity disclosures. *Deloitte.* https://dart.deloitte.com/USDART/home/publications/deloitte/heads-up/2023/sec-rule-cyber-disclosures
[13]Ibid.

stakes significantly, prompting some CISOs to reassess their career trajectories, particularly within publicly traded companies where the scrutiny is most intense.

Moreover, the SEC's regulatory approach introduces a less obvious but equally significant risk for CISOs and executives: the potential dilemma between facing legal action or blowing the whistle on organizational wrongdoing. In instances where internal governance mechanisms fail to address cybersecurity vulnerabilities adequately, CISOs may find themselves caught between loyalty to their employers and ethical obligations to disclose breaches or systemic deficiencies.[14]

How Boardrooms Can Prepare

Boardrooms must increasingly be able to tie together business guidance and key performance indicators with cyberstrategy going forward, rather than viewing cybersecurity as a function of risk and compliance separate from firm growth. From a governance perspective, one of the board's most important tasks is to verify that management has a clear perspective of how the business could be impacted and that the appropriate skills and resources are in place to mitigate potential wrongdoing. These are critical aspects that must be detailed in the 10-K as part of Item 106. Furthermore, the board will be responsible for aligning the cyber risk program to a detailed risk profile.[15] To help aid in a framework, the National Association of Corporate Directors has published a handbook on cyber-risk oversight, citing six key principles[16]:

1. Directors need to understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Board of Directors should have adequate access to cybersecurity expertise and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
4. Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework and reporting structure with adequate staffing and budget.
5. Board-management discussions about cyber risk should include the identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or

---

[14]Rudawski, A. et al. (224, February 26). Chief Information Security Officers and cyber whistleblowing: considerations for boards and breach response teams. *Allen&Overy.* https://www.allenovery.com/en-gb/global/news-and-insights/publications/chief-information-security-officers-cyber-whistleblowing-considerations-boards-breach-response-teams

[15] Enterprise Risk Services. (2016, June). Cybersecurity: The changing role of the Board and the Audit Committee. *Deloitte.* https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf

[16]National Association of Corporate Directors & Internet Security Alliance (2023). Director's handbook on cyber-risk oversight. *NACD.* https://www.nacdonline.org/contentassets/4931ac5b05a84111953919eaa03a38e9/cyber-risk-oversight-handbook_webcompressed.pdf

transfer, such as through insurance, as well as specific plans associated with each approach.

6. Board of Directors should encourage systemic resilience through collaboration with their industry and government peers and encourage the same from their management teams.

CISOs in particular make up a key part of the direction going forward. Executives should recognize CISOs as key members of their boardrooms. By including the CISOs and properly recognizing cyber risk as a strategic risk, a top-down approach that emphasizes preparation and accountability can be established, avoiding silos between CISOs and the rest of the company. According to new SEC disclosure requirements, while boardrooms must take the necessary measures to avoid a cyberattack, it is equally important that board members have a plan when a cyberattack occurs. Response plans and communication protocols specifically designed to deal with breaches should be made with the input of all necessary parties, including IT, Risk, Legal, etc. In other words, board members must ensure the firm knows what to do *when* a breach occurs in addition to installing prevention measures. Board of Directors may also want to think about purchasing cyber insurance and/or Directors and Officers (D&O) insurance as a method of risk management.[17] Doing so can help prevent personal liability and cybersecurity litigation from becoming intertwined, particularly for the CISO, avoiding SolarWinds-like legal aftermath.

When it comes to investing in cyber technology, boardrooms must adopt a multifaceted approach to prepare for cyber risks effectively. While enhancing ROI is undoubtedly crucial, board members must recognize that investing solely in cyber technology is not a silver bullet solution. Instead, discussions within the boardroom should pivot towards cultivating resilience rather than solely emphasizing prevention measures.[18] Resilience encompasses a broader spectrum of strategies, including robust incident response plans, comprehensive employee training, and fostering a culture of cyber awareness throughout the organization. By shifting the conversation towards resilience, board members can acknowledge the inevitability of cyber threats and focus on how the organization can effectively mitigate, respond to, and recover from potential breaches. Furthermore, boardrooms must consider the interconnected nature of cyber risks with other aspects of business operations. This includes evaluating supply chain vulnerabilities, assessing third-party risks, and understanding the potential impact of cyber incidents on regulatory compliance and reputational damage. As new SEC regulations detail, there will be no exemption or safe harbor for registrants if a critical cyber attack targets one of their third-party vendors.

---

[17]IANS Faculty. (2023, September 21). Why CISOs need D&O Liability Insurance Coverage Now. *IANS.* https://www.iansresearch.com/resources/all-blogs/post/security-blog/2023/09/21/why-cisos-need-d-o-liability-insurance-coverage-now

[18] Milica, L. & Pearlson, K. (2023, May 2). Boards are having the wrong conversations about cybersecurity. *Harvard Business School.* https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity

Ransomware is another (potentially very expensive[19]) area that boardrooms must be prepared to engage with. As with other aspects, resilience is just as important as prevention. Companies that can navigate ransom attacks successfully are those with a Board of Directors that have adequately prepared themselves for the attack lifecycle. This requires good data-keeping habits before such an attack, such as backed-up data, separated files, and levels of redundancy. In addition to pressure testing such systems, all details that should be detailed in the 10-K in Item 106. During an attack, documentation will be vital to remain in compliance with new SEC regulations. Publishing an 8-K following a ransomware attack, or any cybersecurity attack, demands that companies be able to describe the nature, timing, scope, and estimated impact of the attack.

As board members develop a plan of action around ransom attacks, several key questions and risks ought to be addressed. Most importantly, there is no guarantee that data will be accessed even after paying a ransom. Board of Directors engaging with bad actors may encourage further action, such as double extortion and additional attacks. Second, board members need to consider the legal and regulatory implications of paying the ransom. Could payment constitute supporting criminal groups, terrorism, rogue states, etc.? Finally, while potentially costly, cyber insurance can play a critical role in further ensuring the safety of company assets or potentially covering the costs of ransomware. Board members ought to consider all of these aspects when it comes to thinking about ransomware.

When it comes to the new SEC regulations more broadly, board members must be incredibly vigilant in reviewing all public disclosures, not just SEC filings. The Board of Directors carries the burden to ensure all material is accurate. This may include a company's security policy, online representations, and even corporate discussions. Board members must recognize that boilerplate language in disclosures is no longer sufficient and may even be detrimental. Generic, one-size-fits-all statements can fail to adequately convey the unique risks and strategies of a particular organization, leaving stakeholders nescient and potentially eroding trust. Instead, board members should prioritize clear, concise, and tailored communication that accurately reflects the company's cybersecurity posture and risk management approach. This may involve collaborating closely with legal and cybersecurity experts to craft disclosures that strike the right balance between transparency and confidentiality. Moreover, board members should be proactive in assessing the effectiveness of existing disclosure practices and continuously refine them in response to evolving regulatory requirements and emerging cyber threats. Regular reviews and updates to public disclosures demonstrate a commitment to accountability and risk awareness, instilling confidence among investors, customers, and other stakeholders in the face of this new SEC regulation.

---

[19] In one survey, 96% of CISOs reported a ransom attack, and of that, 83% stated that their company decided to pay the ransom. More than half of respondents paid more than $100,000, with 9% of respondents paying more than $1 million in ransom.

Splunk. (2023). The CISO report. *Cisco*. https://www.splunk.com/en_us/pdfs/gated/ebooks/the-ciso-report.pdf

Final Remarks

The evolving landscape of cybersecurity demands a proactive and holistic approach from boardrooms. With the global cost of cybercrime projected to soar, businesses must recognize that cyber risk is intertwined with overall business risk. The role of the CISO has evolved significantly, with a growing emphasis on strategic leadership and collaboration across departments. The SolarWinds incident and subsequent SEC actions underscore the imperative for transparent and accurate public disclosures, requiring the Board of Directors to move beyond boilerplate language and prioritize tailored communication. By fostering a culture of resilience, breaking down silos between departments, and staying vigilant in regulatory compliance, boardrooms can navigate the complex cyber threat landscape with confidence and safeguard their organizations' interests, reputation, and stakeholders' trust.