Yale Journal of Law & Technology
Volume 28, Symposium Issue

Governing Toxic Data

Diane Lourdes Dick*, Joseph W. Yockey**

Companies increasingly boast to the public markets about their massive digital transformations and the value of their extraordinary customer insights. In this way, data is emerging as a crown jewel asset with unique corporate-governance implications under state and federal laws. For those firms touting data and other digital resources as among their most valuable assets, compliance with evolving cybersecurity and privacy laws, regulations, customer expectations, digital norms, and best practices will be the key to unlocking this value. By the same token, when compliance and policy gaps become pronounced, data and other digital assets can become toxic; not only will they fail to serve as drivers of corporate value, but they may generate significant liabilities. This category of "toxic" data can cause firms to incur massive litigation costs and regulatory fines and penalties, as well as major reputational damage that can destroy brand equity and erode market share. In light of recent signals by the U.S. Securities and Exchange Commission that it intends to focus on these risks, companies and their advisors must now anticipate that well-funded teams of regulators will aggressively monitor corporate disclosures and investigate compliance in an effort to carry out their mission to protect investors and maintain fair, orderly, and efficient markets. In response to this evolutionary enforcement moment, this Article provides the first comprehensive review of the corporate governance of data and other digital assets under state business-entities laws and the federal securities laws, paying special attention to evolving fiduciary responsibilities to monitor, oversee, and report on the risks associated with what we call toxic data.

Article Contents

Introduction

On October 30, 2023, the U.S. Securities and Exchange Commission (SEC) filed a civil action against SolarWinds, a publicly traded information-technology company, and its Chief Information Security Officer (CISO) Timothy Brown.[1] The complaint alleged that SolarWinds and Brown defrauded investors by making misleading public statements about the effectiveness of the company's cybersecurity controls,[2] particularly with respect to the "Orion software platform, a flagship product that the Company considered to be a 'crown jewel' asset and which accounted for 45% of its revenue in 2020."[3]

The SEC complained that in numerous public statements, SolarWinds and Brown "touted the company's supposedly strong cybersecurity practices" and "concealed from the public the Company's known poor cybersecurity practices."[4] Meanwhile, internal messages and documents reflected Brown's and other senior managers' awareness of material vulnerabilities in the company's cybersecurity systems and controls, such as inappropriate access to critical systems, "which could lead to 'major reputation and financial loss' for SolarWinds."[5] Notwithstanding these concerns, the company's SEC filings contained only "general, high-level risk disclosures" that grouped cyberattacks alongside other "generic and hypothetical" risks, such as fire and natural disasters.[6]

Eventually, the material gaps in SolarWinds' cybersecurity systems compromised the Orion product and caused the

---

* Charles E. Floete Distinguished Professor of Law, University of Iowa College of Law.
** F. Arnold Daum Chair in Corporate Law, University of Iowa College of Law.

[1] Complaint at 1, SEC v. SolarWinds Corp., No. 23-cv-9518 (S.D.N.Y. Oct. 30, 2023).
[2] *Id.*
[3] *Id.* at 2.
[4] *Id.*
[5] *Id.* at 5.
[6] *Id.* at 3.

company to experience "one of the worst cybersecurity incidents in history."[7] But while the breach highlighted the company's massive vulnerabilities, the SEC clarified that "SolarWinds' poor controls, Defendants' false and misleading statements and omissions, and the other misconduct described in this Complaint, would have violated the federal securities laws even if SolarWinds had not experienced a major, targeted cybersecurity attack."[8] In other words, the focus of the lawsuit was the defendants' ongoing misstatements, omissions, and schemes that called into question the firm's underlying value thesis—*not* the trigger event that eventually caused investors to realize massive losses (and that likely attracted SEC scrutiny in the first place).

The SEC's lawsuit sent shockwaves through the cybersecurity industry, as it signaled a major expansion of the SEC's regulatory footprint.[9] It also sent a clear message to CISOs that the agency will hold them accountable if they make—or allow their companies to make—misleading public statements about cybersecurity risks.[10] The lawsuit thus strongly incentivizes CISOs to take more deliberate steps to prevent cybersecurity breaches. Strong CISOs have always urged their companies to prioritize and address gaps in compliance with data protection laws, policies, and best practices.[11] But in the wake of the SEC's action against SolarWinds, it further appears that CISOs must monitor compliance gaps for materiality and escalate these risks to the very highest levels of corporate management—presumably even if this means going against the wishes of other senior leaders, or even engaging in whistleblower activity.

---

[7] *Id*. at 7.
[8] *Id*.
[9] *See* James Rundle, *SolarWinds Denies SEC Charges over Cyber Disclosures*, WALL ST. J. (Nov. 8, 2023, 6:25 PM ET), https://www.wsj.com/articles/solarwinds-denies-sec-charges-over-cyber-disclosures-31dcad0c [https://perma.cc/Y72Z-G78B].
[10] *See, e.g.*, Brian Walker, *The SEC To CISOs: Welcome to the Big Leagues*, FORBES (Nov. 9, 2023, 9:30 AM EST), https://www.forbes.com/councils/forbestechcouncil/2023/11/09/the-sec-to-cisos-welcome-to-the-big-leagues/ [https://perma.cc/LGV7-HHLE].
[11] *See What's Important to the CISO in 2025*, PRICEWATERHOUSECOOPERS, https://www.pwc.com/us/en/executive-leadership-hub/ciso.html [https://perma.cc/KP6U-38T8].

This Article argues that the SEC's prosecution of SolarWinds and its CISO marks a watershed moment in corporate governance in the evolving data economy. As companies increasingly tout digital transformations and the value of their data assets to the public markets, the SEC is likely to scrutinize such claims to fulfill its mandate of protecting investors and ensuring fair, orderly, and efficient markets. The lessons from the SolarWinds case extend far beyond CISOs and cybersecurity. For example, the SEC could plausibly bring a similar enforcement action against a company—and its Chief Privacy Officer (CPO)—for misleading public statements about data-privacy risks.

Beyond federal securities law, the SolarWinds case also underscores deeper governance challenges around data as a corporate asset. For firms that portray data as a critical driver of value, effective compliance with evolving cybersecurity and privacy obligations is essential. When compliance or governance gaps become pronounced, digital assets can grow toxic—no longer serving as sources of value but emerging instead as drivers of liability.

As we use the term here, "toxic data" refers to digital information assets that, despite their initial value or strategic importance, become liabilities due to inadequate management, insufficient security measures, or misalignment with regulatory standards and societal expectations. The concept is analogous to the treatment of hazardous materials in environmental law, wherein substances such as contaminated land or hazardous waste must be managed meticulously to prevent significant harm. Just as laws like the Comprehensive Environmental Response, Compensation, and Liability Act[12] underscore how regulatory oversight and rigorous compliance practices are essential to prevent toxic environmental conditions from undermining asset value, toxic data requires governance structures that can anticipate, identify, and mitigate the harms it may cause. More specifically, data becomes toxic when it is mishandled, improperly secured, outdated, retained beyond its useful lifecycle, or used in ways that pose ethical, regulatory, or reputational risks.

---

[12] 42 U.S.C. §§ 9601-9675 (2024). This law, also known as the "Superfund" law, addresses hazardous waste sites across the nation.

This Article offers the first comprehensive analysis of corporate governance obligations surrounding data and digital assets, drawing on both state fiduciary duties and federal securities law. A key question animates our inquiry: even in the absence of a breach, can compliance failures themselves suggest that a company's data-driven value proposition is flawed? We argue yes. Data is among the most valuable corporate assets, central to strategic operations and market identity. But its value is inextricable from the risks it carries. Poor management of these assets erodes corporate value, exposes firms to liability, and undermines public trust. These realities demand a reexamination of how corporate officers and directors govern data—even when no headline-grabbing incident has occurred.

Although the SolarWinds saga centers on cybersecurity, its governance implications apply with equal force to privacy risks, AI governance failures, and other manifestations of toxic data. A firm that misleads investors about its privacy compliance or AI governance systems may invite the same regulatory scrutiny and derivative litigation risk. The principle is the same: when a company's value proposition hinges on data, its duties of oversight and disclosure extend across the entire data lifecycle—from acquisition to use to deletion. Accordingly, our analysis proceeds with an expansive conception of toxic data, encompassing cybersecurity, data-privacy, and algorithmic risk alike.

I. Corporate Cybersecurity and Privacy Programs

The growing prominence of digital transformation has elevated cybersecurity and privacy from a back-office compliance function to a critical governance and risk-management priority. Firms that once viewed cybersecurity as a cost center are now forced to reckon with the reality that weak cyber and privacy governance can directly erode corporate value, investor confidence, and regulatory standing. Recent SEC enforcement actions, such as those involving SolarWinds, reinforce that corporate leaders must actively oversee cybersecurity programs and ensure transparency in

risk disclosures.[13] This Section examines the corporate-compliance landscape, enforcement trends, and evolving expectations for firms navigating cybersecurity and privacy obligations.

While this Article primarily focuses on U.S. frameworks, the global nature of digital operations also demands awareness of international developments. For instance, the European Union's General Data Protection Regulation (GDPR) enforcement actions underscore similar governance challenges, highlighting the importance of cross-border compliance strategies.[14] Further comparative research into international corporate-governance practices, especially from jurisdictions actively enforcing data-privacy regulations like the EU and Canada, could provide multinational firms deeper insights into managing cross-border cybersecurity and privacy risks.

A. Traditional Compliance Function of Cybersecurity and Privacy

Corporate cybersecurity and privacy programs have historically been framed as compliance functions, ensuring adherence to regulatory requirements and industry standards.[15] These compliance programs operate within the context of federal, state, and international regulations, such as the Federal Trade Commission (FTC) Act[16] and major privacy statutes

---

[13] *See* Press Release, U.S. Securities and Exchange Commission, SEC Charges Four Companies with Misleading Cyber Disclosures (Oct. 22, 2024), https://www.sec.gov/newsroom/press-releases/2024-174 [https://perma.cc/KM8B-7XPR].

[14] *See, e.g.*, *EU Privacy Regulator Fines LinkedIn 310 Mln Euro*, REUTERS (Oct. 24, 2024, 5:05 AM EDT), https://www.reuters.com/technology/eu-privacy-regulator-fines-linkedin-310-mln-euro-2024-10-24 [https://perma.cc/NX3Q-LEJ5]; *Uber Fined in Netherlands for Sending Drivers' Data to the US*, REUTERS (Aug. 26, 2024, 4:48 AM EDT), https://www.reuters.com/technology/cybersecurity/dutch-privacy-watchdog-fines-uber-sending-drivers-data-us-2024-08-26 [https://perma.cc/XB9D-F437].

[15] *See The Importance of an Integrated Approach to Data Privacy Regulations in Cybersecurity*, KPMG, https://kpmg.com/us/en/articles/2025/integrated-approach-data-privacy-regulations-cybersecurity.html [https://perma.cc/LN4L-7X34].

[16] Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2024).

including the GDPR[17] and the California Consumer Privacy Act (CCPA).[18] Organizations must ensure they have the proper internal policies, governance frameworks, and reporting structures in place to comply with these laws.

A key aspect of traditional compliance has been establishing the roles of CISOs and CPOs. The CISO typically bears responsibility for developing, implementing, and overseeing a company's information-security strategy and protocols. This includes managing cybersecurity defenses, responding to security incidents, ensuring that the company's security architecture aligns with business objectives, and regularly assessing vulnerabilities and threats to corporate data assets. The CISO also serves as a crucial communicator, regularly updating executives and the board about the company's security posture and risk assessments.[19]

The CPO, on the other hand, is chiefly responsible for overseeing compliance with data-privacy laws and regulations, as well as advocating for consumer-privacy rights within the organization. This officer is tasked with creating and maintaining comprehensive data-governance policies, managing privacy impact assessments, and ensuring that all data collection, processing, and disposal practices comply with evolving laws such as the GDPR, CCPA, and other jurisdiction-specific regulations. Additionally, CPOs frequently coordinate with legal, compliance, and IT teams to address data-privacy concerns proactively and transparently.[20]

Despite these clearly defined responsibilities, organizations continue to face significant data-management challenges, including rapid regulatory changes, increasingly sophisticated cyber threats, and the inherent tension between data monetization and strict regulatory adherence. Both CISOs and CPOs must therefore navigate complex, shifting landscapes,

---

[17] Regulation (EU) 2016/679, of the European Parliament and of the Council, 2016 O.J. (L 119).

[18] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100.

[19] For an overview of the evolving regulatory landscape for CISOs, see Mark Lanterman, *CISO Beware Cyber Accountability Is Changing*, BENCH & B. MINN., Aug. 2023, at 10.

[20] For an overview of the CPO's primary roles and responsibilities, see *The Chief Privacy Officer: The New "Must Have,"* ASS'N OF CORP. COUNS., https://www.acc.com/sites/default/files/resources/20190314/1493964_1.pdf [https://perma.cc/4WL9-64CT].

ensuring that their compliance efforts remain effective, adaptable, and aligned with broader business objectives.

While navigating these complexities has traditionally been viewed as a cost of doing business, a more sophisticated understanding is emerging. Rather than seeing compliance as a purely defensive measure, leading firms are beginning to recognize that robust cybersecurity and privacy programs can be powerful drivers of corporate value and competitive advantage. This shift in perspective transforms cybersecurity and privacy from a reactive necessity into a proactive strategic asset.

1. Evolving Value-Building Function of Cybersecurity and Privacy

As companies increasingly navigate the complexities of evolving cybersecurity and privacy regulations, compliance has begun to shift from being perceived merely as a regulatory obligation to an essential driver of competitive advantage. Strong cybersecurity and privacy programs not only help mitigate legal and operational risks but also actively build investor confidence, enhance brand reputation, and solidify regulatory standing. Forward-thinking companies now recognize robust cybersecurity and privacy programs as fundamental to their overall value proposition. They increasingly integrate sophisticated cybersecurity practices directly into their business strategies, leveraging advanced security protocols and privacy protections as distinguishing factors that signal trustworthiness and reliability to customers, investors, and regulators alike.

Companies known for strong cybersecurity and privacy frameworks often benefit from increased consumer loyalty, as transparency and accountability in data handling become critical considerations for customers deciding which businesses to trust with their personal information.[21] Furthermore, organizations demonstrating proactive compliance can

[21] *See* Chris McKie, *Cybersecurity as a Brand Differentiator: Building Consumer Trust*, FORBES (Feb. 24, 2025, 7:30 AM ET), https://www.forbes.com/councils/forbescommunicationscouncil/2025/02/24/cybersecurity-as-a-brand-differentiator-building-consumer-trust [https://perma.cc/N99E-HJ6R].

leverage their cybersecurity posture in marketing and investor communications, differentiating themselves positively in crowded and competitive marketplaces.[22] This strategic emphasis on data protection and privacy not only helps in preventing costly incidents but also positions companies favorably in the eyes of regulators, potentially reducing scrutiny and fostering positive engagement with oversight bodies.

Investor expectations around transparency have notably increased, especially given high-profile data breaches and regulatory actions such as those involving SolarWinds and Equifax.[23] Regulatory scrutiny underscores the necessity for businesses to provide thorough, accurate, and timely disclosures regarding their cybersecurity and data privacy practices and risks.[24] In turn, organizations that successfully demonstrate robust cybersecurity and privacy-management capabilities through clear disclosures gain an additional competitive edge, reassuring investors of their commitment to long-term risk mitigation and governance excellence.

2. Toxic Data: When Data Becomes a Liability

As we noted above, the concept of "toxic data" refers to information assets characterized by regulatory, reputational, or operational risks tied to inadequate governance or controls. High-profile breaches underscore how improperly managed data becomes a critical vulnerability.

For instance, in 2017, Equifax, one of the largest credit reporting agencies in the United States, suffered a massive data breach, compromising the sensitive personal information of nearly 150 million consumers.[25] Attackers exploited a known

---

[22] *See id.*; *see also* Anupma Narula, Frank Milano & Raj Singhal, *Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry*, DELOITTE (Nov. 14, 2024), https://www2.deloitte.com/us/en/insights/topics/risk-management/consumer-data-privacy-strategies.html [https://perma.cc/3DW6-B3YC].

[23] *See infra* text accompany notes 25–27; 45–46.

[24] For a thoughtful examination of data-related corporate disclosures, see Megan Wischmeier Shaner, *Growing Tensions: Consumer Privacy and Corporate Disclosures*, 77 SMU L. REV. 477 (2024).

[25] *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1308 (N.D. Ga. 2019).

vulnerability in a software used by Equifax and gained unauthorized access to these consumers' names, Social Security numbers, birth dates, addresses, and driver's license numbers.[26] Equifax faced intense criticism for its slow response, delayed public disclosure, inadequate cybersecurity measures, and the problematic sale of company stock by executives before publicly announcing the breach. The incident led to numerous lawsuits, regulatory fines (including a settlement of up to $700 million with U.S. regulators), and widespread reputational damage, highlighting the company's critical gaps in corporate governance, cybersecurity preparedness, and data-privacy compliance.[27]

Recent scholarship and industry analysis have highlighted these and other data-related risks as an emerging challenge within corporate data-governance and cybersecurity frameworks.[28] Organizations frequently accumulate vast quantities of redundant, obsolete, or sensitive data without implementing clear retention or disposal policies, significantly elevating their security and regulatory risk profiles. Proactive data-lifecycle management—including periodic audits, structured data-disposal policies, and enhanced encryption measures—is essential to mitigating these risks. Advanced AI-driven classification tools can further assist firms in identifying, categorizing, and managing high-risk data effectively.

While cybersecurity and privacy breaches represent obvious examples of toxic data, emerging uses of artificial intelligence introduce subtler but equally serious risks. For instance, firms deploying AI models trained on biased or outdated datasets may inadvertently cause harm to consumers or investors that triggers liability under discrimination laws or enforcement by the FTC or Consumer Financial Protection

---

[26] *Id*. at 1308–09.

[27] *See* Avie Schneider & Chris Arnold, *Equifax to Pay Up to $700 Million in Data Breach Settlement*, NPR (July 22, 2019, 9:25 AM ET), https://www.npr.org/2019/07/22/744050565/equifax-to-pay-up-to-700-million-in-data-breach-settlement [https://perma.cc/82SB-63F6]/

[28] *See, e.g.*, Michael R. Siebecker, *Reconceiving Corporate Rights and Regulation in the AI Era*, 89 MO. L. REV. 941 (2024). For an early look at these important issues, see Mark F. Foley, *Board Oversight of Information Technology, Data Privacy, and Data Security: Preserving Critical Business Assets*, WIS. LAW., Aug. 2007, at 17.

Bureau (CFPB). Moreover, public companies that exaggerate the effectiveness or safety of their AI systems—such as promising explainability or auditability that does not exist—could face SEC scrutiny for misstatements or material omissions. These risks underscore the need for governance frameworks that treat AI governance as part of the broader toxic-data landscape.

To comprehensively address these challenges, companies must establish robust, proactive data-governance strategies. Foundational elements of those strategies include implementing comprehensive data retention and disposal policies, conducting routine security and compliance audits, and maintaining transparency by communicating data-management practices to stakeholders. Incorporating privacy-by-design principles is also critical, as it ensures that organizations anticipate and proactively manage data-related risks rather than merely responding to crises.

A successful governance framework also depends on organizational alignment and culture. Firms should pursue cross-functional collaboration among their legal, compliance, and information-technology teams to foster an integrated approach that aligns with regulatory expectations and industry best practices. Furthermore, consistent training programs are essential to enhance employee awareness of cybersecurity best practices and compliance obligations.

By adopting a risk-based approach to data security, firms can prioritize their resources effectively and ensure that the most sensitive and critical data receives heightened protection. Ultimately, embedding these governance strategies into broader corporate practices not only reduces legal and regulatory exposure but also strengthens market positioning by bolstering trust among consumers and investors. With these governance strategies in place, it becomes essential to clearly define and understand the specific responsibilities of corporate directors and officers for overseeing cybersecurity and privacy risks, as detailed in the following section.

II. Corporate Risk Oversight and Reporting Requirements

Corporate directors and officers face increasingly complex obligations to oversee risks associated with cybersecurity and privacy. Recent case law, coupled with enhanced reporting requirements issued by the SEC and other regulatory bodies, underscores the importance of robust governance structures for managing toxic data. This section provides a detailed overview of these developments as well as the practical considerations that corporate leaders tasked with overseeing cybersecurity and privacy risks should engage with.

A. Fiduciary Duties Under Delaware Law and Beyond

Pursuant to the landmark standard first articulated in *In re Caremark International Inc. Derivative Litigation*, Delaware courts recognize that directors have an affirmative duty to implement and monitor corporate compliance programs and reporting systems.[29] Failure to "attempt to assure a reasonable information and reporting system exists" can expose directors to personal liability for breaching their fiduciary obligations.[30] This doctrine was further clarified in *Stone v. Ritter*, where the Delaware Supreme Court held that oversight responsibility is grounded in the duty of loyalty and good faith.[31] *Stone* explained that to establish a breach of fiduciary duty for lack of oversight, shareholders must show that (1) the directors "utterly failed to implement any reporting or information system or controls," or (2) having implemented such a system or controls, the directors "consciously failed to monitor or oversee its operations."[32] Under this framework, directors are held liable only if they knowingly ignored their responsibility to act in the face of a duty to do so, reflecting a conscious disregard of their oversight role.

Thirteen years after *Stone*, the Delaware Supreme Court signaled its evolving understanding of oversight by stressing that boards must pay special attention to risks integral to a

---

[29] 698 A.2d 959 (Del. Ch. 1996).
[30] *Id*. at 971.
[31] 911 A.2d 362, 369-70 (Del. 2006).
[32] *Id*. at 370.

corporation's "mission critical" operations.[33] In *Marchand v. Barnhill*, the Court reversed the dismissal of a *Caremark* claim where the board allegedly failed to implement any meaningful system to monitor "mission critical" food-safety risks in a company whose core business involved the production of ice cream.[34] Writing for the Court, Chief Judge Strine observed that one of the most critical issues facing Blue Bell Creameries, the company at issue, is to ensure that "the only product it makes—ice cream—is safe to eat."[35] Yet the Blue Bell board had "no committee overseeing food safety, no full board-level process to address food safety issues, and no protocol by which the board was expected to be advised of food safety reports and developments."[36] Notably, when "yellow and red flags about food safety were presented to management, there was no equivalent reporting to the board," leading the Court to conclude that "the complaint alleges specific facts that create a reasonable inference that the directors consciously failed 'to attempt to assure a reasonable information and reporting system exist[ed].'"[37]

By underscoring the importance of formalized compliance structures and robust reporting mechanisms for critical operational risks, *Marchand* confirmed that directors must take affirmative steps to ensure ongoing awareness of, and responsiveness to, potential issues that strike at the heart of a company's business model. For example, boards should create or empower committees specifically tasked with monitoring and reporting on mission-critical risks, ensure that management provides regular and substantive reports on compliance issues, and establish formal protocols for escalating red flags to the board's attention. Under the specific facts of *Marchand*, two factors central to the Court's decision were the absence of any board-level committee dedicated to food safety and the lack of a systematic process for the board to receive and evaluate critical information regarding that "mission critical" risk.[38]

---

[33] 212 A.3d 805, 824 (Del. 2019).
[34] *Id.* at 809.
[35] *Id.* at 822.
[36] *Id.* at 809.
[37] *Id.*
[38] *Id.* at 824.

From the perspective of toxic data, cybersecurity and data-privacy risks can rise to the heightened zone of oversight responsibility outlined in *Marchand* when a firm's core value proposition depends on secure and compliant data handling.[39] As a result, directors and officers of today's data-driven companies must do more than merely adopt surface-level controls; they must stay informed about data flows, evaluate the efficacy of protective technologies, and ensure that adequate reporting structures are in place to detect potential incidents.

It is crucial, however, to clarify that enhanced fiduciary obligations around cybersecurity and data privacy do not equate to requiring directors to manage day-to-day cybersecurity operations or become technical experts themselves. Rather, consistent with established Delaware jurisprudence, boards should maintain an informed, vigilant oversight role, ensuring the implementation of adequate information and reporting systems and responding diligently to significant compliance issues and risks as they arise. Defining reasonable boundaries for oversight ensures that directors can effectively perform their fiduciary duties without becoming overly enmeshed in operational specifics beyond their expertise or role.

These fiduciary standards do not operate in isolation. Rather, they interact in meaningful ways with federal securities law, particularly the SEC's disclosure regime. On one level, strong board-level oversight as required under *Caremark* and

---

[39] A growing body of scholarship has proposed updating the *Caremark* framework to address cybersecurity oversight failures. Most notably, Professor Jennifer Arlen argues that directors should face liability when they knowingly fail to oversee the accuracy of corporate statements made to business or government customers about cybersecurity practices. *See* Jennifer Arlen, *Directors' Caremark Liability for Fraudulent Disclosures to Customers About the Company's Cybersecurity: SolarWinds Reconsidered,* 50 J. CORP. L. 1141 (2025). While our analysis similarly views cybersecurity disclosure as a governance priority, we situate these oversight failures within a more general framework of "toxic data"—a concept that encompasses privacy, AI-governance, and other risks that stem from digital-asset mismanagement—and we argue that effective governance of toxic data requires not only fiduciary vigilance but also enhanced federal disclosure obligations and institutional reform.

Marchand improves the accuracy of public disclosures, reducing the risk of omissions or misstatements that might trigger SEC enforcement. On another level, the existence of SEC actions or investigations may bolster the plausibility of state-law fiduciary-duty claims, particularly by providing plaintiffs with credible evidence of red flags that were ignored by directors. In this way, federal disclosure obligations and state fiduciary duties operate as interlocking enforcement regimes: the former informs investors and regulators, while the latter ensures that directors are actively interrogating the validity of what their companies are saying to the market.

B. SEC Obligations Around Risk Reporting

On July 26, 2023, the SEC adopted new rules requiring public companies and foreign private issuers to disclose material cybersecurity incidents and provide annual disclosures regarding cybersecurity risk management, strategy, and governance.[40]

First, under Item 1.05 of Form 8-K, companies must report material cybersecurity incidents within four business days of determining their materiality, including details on the incident's nature, scope, timing, and impact.[41] The rule contains a national-security exception, enabling the U.S. Attorney General to delay disclosure if it poses a substantial risk to public safety or national security.[42]

The new rules also introduce Item 106 of Regulation S-K, requiring public companies to annually disclose their cybersecurity-risk-management processes, board oversight, and management's role in addressing cybersecurity threats.[43] Notably, the SEC removed a proposed requirement for companies to disclose board-level cybersecurity expertise,

---

[40] Press Release, U.S. Sec. and Exchange Comm'n, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (July 26, 2023), https://www.sec.gov/newsroom/press-releases/2023-139 [https://perma.cc/WMF3-L9BV].

[41] *Id.*

[42] Foreign private issuers (FPIs) must report similar incidents on Form 6-K and include cybersecurity risk disclosures in Form 20-F. *See id.*

[43] *Id.*

recognizing that cybersecurity oversight does not necessarily require specialized technical knowledge.[44]

These requirements mark a significant shift in cybersecurity-reporting obligations, appearing to promote greater transparency and uniformity in disclosure practices. Companies should assess their cybersecurity-risk-management programs, incident-response procedures, and board-oversight structures to ensure compliance with the new reporting obligations. Given the potential regulatory and reputational risks, they should also review their internal-disclosure controls, coordinating with the audit committee and cybersecurity and legal teams, and prepare for structured real-time incident reporting to meet these requirements effectively.

As noted above, recent SEC enforcement actions underscore the prospect of heightened regulatory scrutiny surrounding cybersecurity disclosures and risk management. In October 2023, the SEC charged SolarWinds and its CISO for allegedly misleading investors about the company's cybersecurity posture prior to the 2020 SolarWinds Orion software breach.[45] The SEC claimed SolarWinds misrepresented its cybersecurity controls and risks, violating antifraud provisions of federal securities laws. However, in July 2024, a federal court dismissed most of the SEC's claims, ruling that internal accounting controls do not extend to cybersecurity controls, though allegations related to misleading public cybersecurity statements were allowed to proceed.[46]

In October 2024, the SEC fined four technology companies—Unisys Corp., Avaya Holdings, Check Point

---

[44] *Understand SEC Requirements for Cybersecurity Disclosures*, DELOITTE (July 2024), https://www.acc.com/sites/default/files/2024-08/ACC-Az-Chapter---Understanding-SEC-Requirements-for-Cyber-Disclosures-Program-Matrials---Deloitte---8.20.24_0.pdf [https://perma.cc/BQR6-JA7D].

[45] Press Release, U.S. Securities and Exchange Commission, SEC Charges SolarWinds and Chief Information Officer with Fraud, Internal Control Failures (Oct. 30, 2023), https://www.sec.gov/newsroom/press-releases/2023-227 [https://perma.cc/XCE2-DYUN].

[46] *Judge Rejects SEC's Aggressive Approach to Cybersecurity Enforcement*, WHITE & CASE (July 29, 2024), https://www.whitecase.com/insight-alert/judge-rejects-secs-aggressive-approach-cybersecurity-enforcement [https://perma.cc/9GP4-9BTZ].

Software Technologies, and Mimecast Limited—for misleading disclosures about their exposure to the SolarWinds hack.[47] Then, in December 2024, the SEC reached a $3.55 million settlement with Flagstar Bancorp over allegations that the company misrepresented the extent of a 2021 cyberattack and lacked adequate cybersecurity disclosure controls.[48] The same month, the SEC settled recordkeeping charges with ICBC Financial Services, a U.S. subsidiary of the Industrial and Commercial Bank of China, following a November 2023 ransomware attack that disrupted the firm's operations.[49] The SEC noted that the attack led to deficiencies in maintaining accurate books and records, as well as failures in providing required notifications for securities-related transactions to customers. However, due to ICBC's prompt remedial actions and full cooperation during the investigation, the SEC opted not to impose a civil fine.[50] Finally, in January 2025, Ashford Inc. settled SEC charges that it failed to disclose the full scope of a 2023 cyberattack affecting sensitive personal information of 46,000 individuals, agreeing to pay a $115,231 penalty.[51]

These actions highlight the SEC's aggressive enforcement posture and reinforce the need for accurate, timely, and complete cybersecurity disclosures to mitigate the risk of regulatory scrutiny. Of course, whether these regulatory trends continue during the new Trump administration remains

---

[47] Press Release, U.S. Securities and Exchange Commission, SEC Charges Four Companies with Misleading Cyber Disclosures (Oct. 22, 2024), https://www.sec.gov/newsroom/press-releases/2024-174 [https://perma.cc/KM8B-7XPR].

[48] Press Release, U.S. Securities and Exchange Commission, SEC Charges Flagstar for Misleading Investors about Cyber Breach (Dec. 16, 2024), https://www.sec.gov/enforcement-litigation/administrative-proceedings/33-11343-s [https://perma.cc/C4QS-MGVA].

[49] Press Release, U.S. Securities and Exchange Commission, SEC Settles Recordkeeping Charges with ICBC Financial Services Cybersecurity Incident (Dec. 2, 2024), https://www.sec.gov/enforcement-litigation/administrative-proceedings/34-101794-s [https://perma.cc/8MMC-AZLA].

[50] *Id.*

[51] James Rundle, *Asset Manager Ashford Settles SEC Allegations it Failed to Disclose Extent of Hack*, WALL ST. J. (Jan. 14, 2025, 4:11 PM ET), https://www.wsj.com/articles/asset-manager-ashford-settles-sec-allegations-it-failed-to-disclose-extent-of-hack-dafec329 [https://perma.cc/9JPT-E6K8].

unclear. Leading cybersecurity and data-privacy experts believe that the "SEC might have a lighter touch during the second Trump administration" with companies perhaps given greater "leeway such as more time to disclose hacks."[52]

Given this regulatory uncertainty, firms should adopt proactive compliance strategies to manage cybersecurity and privacy risks effectively, independent of the prevailing political climate. Companies might achieve this by establishing governance frameworks that exceed current minimum regulatory standards, fostering internal compliance cultures oriented toward continuous improvement and flexibility. Proactive governance strategies not only ensure preparedness for shifting regulatory expectations, but also provide a robust defense against reputational harm, litigation risk, and potential financial liabilities.

C. Certifications by CISOs and CPOs

The evolving regulatory landscape has increasingly emphasized the accountability of corporate executives, particularly CISOs and CPOs, in ensuring the adequacy of their organizations' cybersecurity and privacy programs. While there is no universal mandate requiring CISOs and CPOs to personally certify these programs, several regulations and standards implicitly necessitate their active involvement and oversight.

For instance, the European Union's GDPR mandates that organizations appoint a Data Protection Officer (DPO) under specific conditions, such as when an organization engages in large-scale processing of sensitive personal data.[53] The DPO's role closely aligns with that of a CPO, focusing on monitoring compliance, advising on data-protection obligations, and acting

---

[52] *Id*. The news article cites Michael Bahar, co-lead of global cybersecurity and data privacy at the law firm of Eversheds Sutherland, for this proposition. *See id*; *Michael Bahar*, EVERSHEDS SUTHERLAND, https://www.eversheds-sutherland.com/en/united-states/people/bahar-michael [https://perma.cc/3XAQ-F8P8].

[53] *Data Protection under GDPR*, YOUR EUR. (Mar. 3, 2025), https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm [https://perma.cc/5MTD-73GZ].

as a liaison with supervisory authorities.[54] Although the GDPR does not explicitly require DPOs to certify the adequacy of privacy programs, their responsibilities inherently involve ensuring that these programs meet regulatory standards.

In the realm of information security, standards like ISO/IEC 27701, and the broader ISO/IEC 27000 family of standards, provide frameworks for managing and certifying information-security and privacy controls.[55] Organizations often seek certifications such as ISO/IEC 27001 to demonstrate their commitment to information-security management.[56] While these certifications do not require CISOs to personally attest to the adequacy of cybersecurity programs, achieving and maintaining the certifications typically involves significant leadership and oversight from CISOs to ensure compliance with the prescribed standards.

Thus, while there may not be explicit regulatory requirements compelling CISOs and CPOs to certify the adequacy of their organizations' cybersecurity and privacy programs, their roles are integral to ensuring compliance with relevant laws and standards. Their expertise and leadership are crucial in developing, implementing, and maintaining programs that meet regulatory expectations and protect organizational assets.

* * *

In sum, Delaware's *Caremark* and *Marchand* line obliges directors to *build and monitor* "mission-critical" compliance systems; the SEC's 2023 cybersecurity rules oblige issuers to *describe and demonstrate* those systems in real time. In effect, the SEC tells investors *what* boards must reveal, while *Caremark* dictates *how* boards must assure themselves that the revelation is accurate. Each framework fills a gap in the other.

---

[54] *See The Role of a Data Protection Officer (DPO) in GDPR Compliance*, GDPR ADVISOR, https://www.gdpr-advisor.com/gdpr-dpo-role [https://perma.cc/6ED5-W7YB].

[55] *ISO/IEC 27000 Family*, INT'L STANDARDIZATION ORG., https://www.iso.org/standard/iso-iec-27000-family [https://perma.cc/S8CT-3J6D].

[56] *ISO 27001*, INT'L ACCREDITATION COUNCIL, https://iacouncil.org/iso-27001 [https://perma.cc/5UXD-QXS2].

Caremark gives the SEC's disclosure mandates practical teeth inside the boardroom, and the SEC gives plaintiffs an objectively verifiable yardstick against which to test directors' good-faith oversight processes. Indeed, boards are now urged to thoroughly document their cybersecurity oversight precisely because plaintiffs and regulators will most likely scrutinize those records as a prelude to derivative litigation or investigations into cyber-related disclosures.[57]

Framing toxic-data oversight as a joint product of state fiduciary law and federal disclosure mandates thus clarifies why boards cannot treat cybersecurity as a garden-variety operational risk. Together, these areas of law create a two-stage enforcement dynamic. Federal regulatory scrutiny lays the groundwork for shareholder derivative suits regarding cyber-related governance or disclosures, and the prospect of those suits is what in turn provides boards with strong incentives to integrate their approach to disclosure with their fiduciary approach to toxic data.

III. Discussion

The ongoing massive digital transformation has fundamentally altered many companies' core mission by shifting their strategic focuses from traditional revenue-generation models to data-driven strategies built around digital assets and customer insights. As firms increasingly tout these digital transformations to investors and stakeholders, there arises an implicit assumption that robust privacy and cybersecurity compliance frameworks are integral to the underlying value thesis. However, this assumption often diverges from reality. When organizations fail to adequately secure their digital infrastructure or overlook critical compliance obligations, their data assets can swiftly become liabilities—toxic data—which present profound risks to investors, customers, regulators, and the broader marketplace.

---

[57] Jenness E. Parker, William E. Ridgway & David A. Simon, *What Companies Can Do to Protect against Cyberattacks*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Dec. 7, 2024), https://corpgov.law.harvard.edu/2024/12/07/what-companies-can-do-to-protect-against-cyberattacks [https://perma.cc/8PZU-S3LT].

The concept of toxic data is analogous to the treatment of hazardous materials in environmental law, wherein substances such as contaminated land or hazardous waste must be managed meticulously to prevent significant harm. Laws like the Comprehensive Environmental Response, Compensation, and Liability Act underscore how regulatory oversight and rigorous compliance practices are essential to preventing toxic environmental conditions from undermining asset value. Similarly, mishandled, inadequately secured, or obsolete data can transform from an asset into a source of corporate vulnerability, leading to diminished investor confidence, increased regulatory scrutiny, litigation risks, and potentially severe reputational damage.

These parallels raise critical governance questions: Do corporate executives and board members fully recognize data-related risks? And do they proactively manage these risks before they escalate into crises? Addressing this question requires firms to move beyond superficial compliance measures and instead embed robust data-governance strategies deep within their operational and strategic frameworks. Boards must rigorously oversee data management practices, demand transparent reporting on data risks, and adopt proactive risk mitigation and response plans.

To strengthen corporate governance in response to these emerging challenges, we propose several critical reforms, including appointing board members with specialized cybersecurity and privacy expertise, adopting clearer and more rigorous reporting standards, introducing mandatory executive certifications of compliance, and establishing a dedicated Cybersecurity and Privacy Task Force within the SEC. These proposals are discussed in more detail in the following subsections.

A. Board Composition and Expertise

A pivotal step toward enhancing data governance in the digital era involves strengthening the composition and expertise of corporate boards regarding cybersecurity and data privacy. Given the rapid evolution and increasing complexity of cybersecurity threats and privacy regulations, board members must be well-equipped to oversee these emerging risks effectively. One potential reform is for regulatory bodies,

such as the SEC, to require publicly traded companies to include directors who possess specific, demonstrable expertise in cybersecurity and data privacy.[58] By ensuring specialized knowledge at the board level, companies would be better positioned to critically evaluate their cybersecurity strategies, anticipate emerging threats, and engage constructively with executive management regarding compliance and risk management.

To be sure, mandatory expertise requirements could face practical challenges, including difficulties in sourcing qualified candidates, particularly for smaller companies or those outside technology-driven industries. Additionally, such requirements risk narrowing the diversity of board perspectives by overly emphasizing technical credentials. Similar concerns arose in response to the audit committee financial expertise requirement introduced by the Sarbanes-Oxley Act of 2002,[59] yet firms effectively adapted through targeted director-training programs, director-compensation strategies, strategic use of external advisory committees, and leveraging professional networks.[60]

To address these current concerns, regulatory frameworks could similarly incorporate flexibility, such as allowing companies to fulfill expertise requirements through advisory boards or specialized committees dedicated explicitly to cybersecurity and privacy oversight. For instance, companies might proactively establish committees like Meta's dedicated

---

[58] For a thoughtful discussion of the risks and benefits of appointing directors in an effort to cover certain areas of substantive expertise on the board, see Yaron Nili & Roy Shapira, *Specialist Directors*, 41 YALE J. ON REGUL. 652 (2024).

[59] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 15, 18, 28 & 29 U.S.C. (2024)).

[60] *See, e.g.*, Jimmy Carmenate, Caroline C. Hartmann, Divesh S. Sharma & Vineeta D. Sharma, *Finding Financial Experts for Audit Committees: What Compensation Can CPAs Expect?*, CPA J. (March 2022), https://www.cpajournal.com/2022/03/21/finding-financial-experts-for-audit-committees [https://perma.cc/RW92-R8NF].

privacy committee, providing concentrated guidance without constraining overall board composition and diversity.[61]

Beyond structural adjustments, organizations must prioritize regular, structured training programs to continuously update directors on evolving cybersecurity threats, regulatory changes, and best practices. Regular training—encompassing scenario-based exercises, tabletop incident simulations, and interactive case studies—would enhance directors' preparedness to respond decisively during real-world cyber incidents. Moreover, these types of training programs would address the evolving nature of digital risks, thereby ensuring that board oversight remains informed, proactive, and effective.

Ultimately, the structural and educational reforms we suggest will create robust corporate-governance frameworks capable of addressing the complex challenges posed by cybersecurity and data privacy risks. By strategically embedding expertise, adopting flexible governance structures, and prioritizing continuous education, organizations can better protect their data assets, mitigate potential liabilities, and reinforce long-term stakeholder trust and corporate resilience. Importantly, while advocating for enhanced cybersecurity expertise at the board level, it is essential to emphasize that directors should fulfill an informed and vigilant oversight role—not become directly involved in daily cybersecurity operations or detailed technical management. Clearly delineating these boundaries will help directors effectively perform their fiduciary responsibilities without being overly drawn into operational specifics beyond their expertise or governance mandate.

To operationalize these reforms, companies should consider multiple pathways for satisfying board-level expertise requirements. One route could be the nomination of directors with formal certifications—such as Certified Information Privacy Professional/United States (CIPP/US) status for privacy or Certified Information Systems Security Professional (CISSP) status for security—who bring deep subject-matter

---

[61] For a critical discussion of Meta's attempts at self-regulation, see, Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 YALE L.J. 2418 (2020).

knowledge. Alternatively, directors might fulfill the requirement through documented experience overseeing cybersecurity or privacy compliance in another public company. Smaller firms and those in less tech-centric industries could rely on expert advisory panels or rotating external consultants who attend board meetings and contribute to risk assessments. Stock exchanges or proxy advisors could support these efforts by identifying best practices and standardizing credentials across sectors. Ultimately, implementation need not follow a one-size-fits-all model. What matters most is that companies develop credible, auditable mechanisms to ensure informed oversight of data-related risks at the board level.

B. Clearer Reporting Standards for Privacy and Cybersecurity

We recommend that regulators adopt a standardized disclosure checklist covering key elements of cybersecurity and privacy governance. This checklist would require public companies to disclose:

- The existence and scope of internal data maps identifying critical assets;
- Frequency and outcomes of data retention audits and disposal reviews;
- Use of automated processing tools, including AI systems, and related risk-mitigation procedures;
- Results of third-party penetration tests or security audits (in anonymized, high-level form);
- Processes for assessing the materiality of cybersecurity and privacy risks;
- Roles and training of CISOs, CPOs, and responsible subcommittees;
- Number and severity of past incidents, regardless of materiality threshold; and
- Ongoing investments in privacy-enhancing technologies and AI-explainability tools.

In contrast to the SEC's current cybersecurity-disclosure rules—focused primarily on incident reporting and board oversight—this checklist would shift the emphasis toward

governance practices, preventive safeguards, and programmatic maturity. The goal is to give investors a fuller picture of how seriously a company takes its obligations, not merely whether it discloses known problems after the fact.[62]

In addition, regulators could mandate formal certifications by corporate executives—similar to those required under Sarbanes-Oxley—to enhance accountability and rigor. Specifically, CISOs and CPOs could be required to certify, on an annual or quarterly basis, that their cybersecurity and privacy programs meet specified regulatory standards, are subject to regular review, and are free from known, undisclosed vulnerabilities. These certifications should also encompass AI-governance systems, including model-explainability protocols, fairness audits, and transparent reporting on AI use in data management and customer-facing systems. Requiring executive sign-off in these areas would not only reinforce accountability but also incentivize more meticulous and proactive governance practices.

Moreover, requiring timely disclosure of cybersecurity incidents—regardless of immediate materiality and in keeping with applicable national security exceptions—would promote market transparency and investor protection. Companies could be required to report such incidents within a defined period, providing clear information about the nature, scope, response actions, and implications of each event. Regular, standardized disclosures about compliance initiatives, risk-mitigation strategies, and improvements to cybersecurity frameworks would further bolster investor confidence and enable more accurate assessments of a company's digital resilience.

C. Formation of a Cybersecurity and Privacy Task Force

To enhance regulatory oversight and enforcement capabilities, the SEC should establish a dedicated Cybersecurity and Privacy Task Force within its Division of Enforcement. Modeled on the agency's ESG Task Force, which was launched in 2021 to proactively monitor corporate

---

[62] *See also* Mihails Diamantis & Rishab Nithyanand, *Information About Data*, 28 YALE J.L. & TECH. 238 (2026). (arguing for mandatory disclosures about corporate data practices as a means of forcing firms to learn more about their own data and its importance).

ESG disclosures and investigate potential misrepresentations,[63] this new unit would systematically evaluate public company disclosures related to cybersecurity and privacy practices.

The proposed Task Force would be charged with identifying material gaps, inconsistencies, and misstatements in corporate disclosures concerning data governance. Equipped with multidisciplinary expertise—brought by employing legal, cybersecurity, privacy, and forensic professionals—the unit would be positioned to detect risks that might otherwise go unnoticed. Its mandate would include proactive surveillance of disclosures, coordination with other regulatory bodies and industry experts, and targeted investigations where public statements appear inconsistent with underlying risk realities or internal assessments.

By enforcing disclosure obligations with consistency and rigor, the Task Force would deter underinvestment in cybersecurity and privacy programs, promote more accurate risk communication to investors, and reinforce the message that data governance is integral to market integrity. Beyond enforcement, the existence of a specialized unit would signal the SEC's institutional commitment to addressing the risks of toxic data—a commitment likely to influence how companies allocate resources, structure internal controls, and assess materiality.

Taken together, the three reforms proposed in this Part—board-level expertise, executive accountability and reporting, and enhanced regulatory enforcement—form an integrated

---

[63] For an engaging history of SEC's ESG initiatives, see Jena Martin & Rachel Chambers, *The Securities and Exchange Commission as Human Rights Enforcer?*, 18 VA. L. & BUS. REV. 93 (2023). On SEC's decision to disband its ESG Task force, *see* Andrew Ramonas, *SEC Abandons ESG Enforcement Group Amid Broader Backlash*, BLOOMBERG L. (Sept. 12, 2024, 3:17 PM EDT), https://news.bloomberglaw.com/esg/sec-quietly-dissolves-climate-and-esg-enforcement-task-force [https://perma.cc/9UAV-6V6G]; *See also* Jamie D. McGinnis, Amy D. Roy & George B. Raine, *Reading the Tea Leaves on SEC's Disbanding of its Enforcement ESG Task Force*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Oct. 3, 2024), https://corpgov.law.harvard.edu/2024/10/03/reading-the-tea-leaves-on-the-secs-disbanding-of-its-enforcement-esg-task-force [https://perma.cc/A8QY-5GFM] (observing that ESG-related issues remain a focus of SEC's agenda even absent the formal task force).

governance framework for toxic data. The first ensures informed oversight; the second promotes transparency and accountability; the third delivers institutional credibility and deterrence. These reforms operate not in isolation, but in concert, representing a broader cultural shift in how boards, executives, and regulators understand the responsibilities that come with treating data as a core corporate asset.

* * *

By implementing these comprehensive reforms, corporations can significantly strengthen their cybersecurity and privacy practices, fostering proactive risk-management cultures that embed digital compliance as core elements of strategic business operations. In doing so, they not only safeguard against the severe repercussions of toxic data, but also leverage robust data governance as pivotal drivers of sustained corporate value, investor trust, and market competitiveness.

Conclusion

In synthesizing the insights presented throughout this Article, it is clear that data has become one of the most valuable corporate assets, central to strategy, innovation, and market positioning. Yet data's value is inseparable from the risks it carries. When mismanaged, improperly secured, or misrepresented, digital assets can turn toxic: undermining trust, attracting regulatory scrutiny, and triggering material legal and financial consequences. As companies deepen their digital transformations, they must recognize the dual nature of data—not only as a source of strategic advantage, but as a latent source of liability that demands disciplined governance.

This Article has proposed a multi-faceted governance framework to meet the growing challenges of toxic data. The recommendations include requiring board-level expertise in cybersecurity and privacy, adopting clearer and more rigorous disclosure standards, mandating executive certifications of compliance, and creating a dedicated Cybersecurity and Privacy Task Force within the SEC. Collectively, these reforms aim to strengthen oversight, improve transparency, and align

corporate behavior with evolving expectations around data governance and accountability.

Implementing these reforms will not be without difficulty. Companies may struggle to identify qualified board candidates, balance transparency with confidentiality, or navigate shifting regulatory landscapes. But these challenges only underscore the urgency of reform. Firms should actively invest in board education, collaborate with industry partners and regulators, and pursue internal assessments of data governance practices to prepare for the heightened scrutiny and obligations ahead.

Future research should empirically assess how these reforms influence corporate performance and risk exposure. Studies might explore correlations between board cybersecurity expertise and incident frequency or examine investor reactions to enhanced disclosures. Practitioners, in turn, can contribute by piloting and publicizing best practices, helping to shape a more resilient, ethical, and accountable approach to managing digital risk.

Ultimately, when a company's core value proposition is driven by data, then effective governance of that data is inseparable from its long-term viability. Recognizing the potential for digital assets to become toxic, and embedding robust oversight mechanisms to manage that risk, will enable firms not only to prevent harm but to credibly position data as a sustainable source of value creation, regulatory legitimacy, and stakeholder trust.