Against Corporate Oversight

Tabrez Y. Ebrahim *

Corporate oversight is trending. Developed by courts during a predigital era, the duty of oversight is meant to protect shareholders against corporate malfeasance, while still giving directors enough leeway to take marketplace risks. Just as the law imposes a special fiduciary duty on those who are given trust, corporate law imposes a special fiduciary duty on directors in confronting risks to corporations. Over the years, this principle has garnered remarkably broad support among advocates for greater corporate accountability.

This Article seeks to disrupt the consensus for the standard of assessment of the duty of oversight by identifying lurking tensions, as well as reasons to doubt a uniform conception of risk in oversight liability. Although some harms to corporations could have been minimized if directors had taken more seriously their responsibility to actively oversee corporate affairs, the emergence of cybersecurity as a central corporate concern suggests that directors are overly cautious with cyber risks and are motivated by the fear of liability. This Article questions whether the current duty of oversight is adequate for the problem of assessing corporate decision making in hindsight and questions whether the standard has been reinvigorated with directors' assessment of emerging cybersecurity risks as claimed by some scholars. In so doing, this Article calls attention to the costs of reinvigorating the duty of oversight in U.S. corporate governance—a trend that effectively abrogates the business judgment rule, which would not be consistent with the scale and scope of modern cybersecurity or practical for implementation towards other disruption risks.

The evolution of the duty of oversight invites an enervating complacency towards assigning personal liability to directors for business performance and risk taking and points to a premature abandonment of more robust visions of the business judgment rule. Current

---

* Associate Professor of Law, Lewis & Clark Law School; Visiting Scholar, University of Texas at Austin School of Law & McCombs School of Business; Visiting Professor, Jordan University of Science & Technology; Scholar, Intellectual Property Policy Institute; Faculty Affiliate, Data Science Program, Lewis & Clark College; Research Affiliate, Bates Center for Entrepreneurship & Leadership, Lewis & Clark College; Research Affiliate, Fariborz Maseeh Department of Mathematics & Statistics, Portland State University; Research Affiliate, Portland Institute for Computational Science; Outreach & Advisory Group, Oregon Regional Computing Accelerator; Registered United States patent attorney; J.D., Northwestern University Pritzker School of Law; M.B.A., Northwestern University Kellogg School of Management; LL.M., University of Houston Law Center; Graduate Entrepreneurship Certificate, Stanford Graduate School of Business; M.S. Mechanical Engineering, Stanford University; B.S. Mechanical Engineering, University of Texas at Austin.

I am grateful for helpful comments from Eric Chaffee, Keith Cunningham-Parmeter, Michael H. Dessent, Lisa Fairfax, George Foster, Alexander I. Platt, Charlotte Tschider, Jeffrey Vagle, Amy Westbrook, Rebecca Wexler, and Josephine Wolff.

Thanks to the following forums for presenting this Article and their participants for helpful comments: AALS Annual Meeting: Business Associations Works-in-Progress Roundtable, Academy of Legal Studies in Business (ALSB) Annual Meeting, Cybersecurity Law and Policy Scholars Conference (CLPSC), Junior Faculty Forum on Law and STEM at the University of Pennsylvania Carey Law School, National Business Law Scholars Conference (NBLSC).

iterations of the oversight duty create risk aversion among directors, while failing to incentivize effective corporate protections in an era of cybersecurity. The business judgment rule better strikes the balance between technological risk-taking, corporate safety, and director liability. This Article takes a skeptical view of the current conception of the duty of oversight and argues for a reinvigoration of the business judgment rule as a better theory of liability to balance risk taking and decision making made with good faith and in the best interests of the corporation.

"It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so."

- *attributed to Mark Twain*[1]

"There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked."

- *John Chambers (former CEO of Cisco Systems)*[2]

1. *See* Rodger Dean Duncan, *What If What You Think You Know Just Ain't So?*, FORBES (May 31, 2019), [https://perma.cc/59PJ-RDLD].

2. John Chambers, *What Does the Internet of Everything Mean for Security?*, WORLD ECON. F. (Jan. 21, 2015), [https://perma.cc/U6QH-BFLT].

INTRODUCTION

The story of Uber's former Chief Security Officer being found guilty for failing to report a cyber breach illustrates the complex ways in which corporate leaders are justifiably concerned about liability arising from cyber breaches.[3] More recently, the Federal Trade Commission ordered Drizly (an online drinks marketplace business) and its CEO to take action towards restricting the collection and retention of consumers' data or face liability consequences.[4] Notably, the Securities and Exchange Commission charged SolarWinds and its Chief Information Officer for its lax cybersecurity practices and its ability to protect against cyberattacks.[5] The message from courts and regulators in the United States is clear—corporate leaders must protect data and take the right steps where cyber breaches occur, or else face liability.[6] These events are newsworthy not only because of the enormous stakes involved for these U.S. corporations, but also because of the potential for liability of their board of directors—specifically concerning their duty of oversight. These issues inform the subject of this Article, which argues against corporate oversight and argues for a reinvigoration of the business judgment rule as a better theory of director liability in the modern digital era.

The question of the standard of assessment of the duty of oversight is an important one, for cybersecurity possesses enormous new risk for corporations in the modern digital era. How should director oversight be assessed? This is a critical question given the crucial role of directors to act in the best interest of the company.[7] This question is particularly urgent for modern corporations which rely substantially on data and depend on information and communication technologies. Director liability is a central element of the debate since developing and maintaining robust cybersecurity entails costs and sufficient incentives created through legal liability, but corporations have argued against the notorious feasibility of developing secure systems.[8] Such considerations give rise to significant corporate gov-

3. Press Release, U.S. Att'y's Off., N. Dist. of Cal., Former Chief Security Officer of Uber Convicted of Federal Charges for Covering Up Data Breaches Involving Millions of Uber User Records (Oct. 5, 2022), [https://perma.cc/NH7E-DDGL].

4. Press Release, FTC, FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers (Oct. 24, 2022), [https://perma.cc/5YMQ-TTY9]; Press Release, FTC, FTC Finalizes Order with Online Alcohol Marketplace for Security Failures that Exposed Personal Data of 2.5 million People (Jan. 10, 2023), [https://perma.cc/T4Y4-9JD5].

5. Press Release, SEC, SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures (Oct. 30, 2023), [https://perma.cc/B67J-ETJE].

6. U.S. Att'y's Off., N. Dist. of Cal, *supra* note 3 ("The message in today's guilty verdict is clear: companies storing their customers' data have a responsibility to protect that data and do the right thing when breaches occur.").

7. Martin Gelter & Geneviève Helleringer, *Lift Not the Painted Veil! To Whom Are Directors' Duties Really Owed?*, 2015 U. ILL. L. REV. 1069, 1075 n.21.

8. *See, e.g.*, Evelyne Studer & Jacques De Werra, *Regulating Cybersecurity: What Civil Liability in Case of Cyber-Attacks?*, 2017 EXPERT FOCUS 511, 511 ("Businesses in various industries have generally resisted the imposition of legal cybersecurity responsibility . . . in view of the notorious unfeasibility of developing absolutely secure code."); *see also* Chris Florackis et al., *Cybersecurity Risk*, 36 REV. FIN. STUD. 1 (2023).

ernance policy questions regarding how directors should be assessed for the decision making.[9] One of the most striking and undertheorized aspects of corporate governance is the dynamic interplay of the duty of oversight and cybersecurity law and policy. Cybersecurity is a growing concern in corporate law, and recent international legal trends indicate a shift towards holding directors personally liable for cybersecurity failures.[10] It is of great concern whether directors' duty of oversight should include cybersecurity risk.

Thanks to a plentiful supply of scholarly debate, news reports, administrative agency guidance, and the extensive number of cases concerning bad outcomes and losses to corporations, corporate law has struggled with assessing directors' duty to prevent harm to the corporation.[11] Is the absence of adequate oversight by directors to blame for catastrophic

9. *See generally* Mariana Pargendler, *The Corporate Governance Obsession*, 42 J. CORP. L. 359 (2016) (describing the rise in attention on corporate governance as a control on corporate behavior in lieu of external regulation).

10. *See, e.g.*, Scott J. Shackelford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Comparative Case Study*, 67 S.C. L. REV. 609, 610, 614–18, 621–22 (2016) (asking "what exactly nations' due diligence obligations are to the public and private sectors"); Kayleen Manwaring & Pamela F. Hanrahan, *BEARing Responsibility of Cyber Security in Australian Financial Institutions: The Rising Tide of Directors' Personal Liability*, 30 J. BANKING & FIN. L. & PRAC. 20, 20–23 (2019) (describing Australian laws creating "potential consequences for individual directors if a cyber attack occurs" against a financial institution); Media Release, Australian Sec. & Inv. Comm'n, Court Finds RI Advice Failed to Adequately Manage Cybersecurity Risks (May 5, 2022), [https://perma.cc/PK4F-QEXF].

11. *See, e.g.*, Eric J. Pan, *Rethinking the Board's Duty to Monitor: A Critical Assessment of the Delaware Doctrine*, 38 FLA. ST. U. L. REV. 209, 209–10 (2011) [hereinafter *Assessment*] (describing the duty to monitor under Delaware law and criticizing Delaware law for designing the scope of the duty "too narrowly . . . for plaintiffs to bring forward duty to monitor claims" and for "incentiviz[ing] directors to avoid asking questions or otherwise making efforts to uncover possible red flags"); Eric J. Pan, *A Board's Duty to Monitor*, 54 N.Y.L. SCH. L. REV. 717, 720 (2009–2010) [hereinafter *Duty*] (describing the duty to monitor under Delaware law and how the duty is limited because it has the potential to "cause a board to become risk averse"); Roy Shapira, *A New* Caremark *Era: Causes and Consequences*, 98 WASH. U. L. REV. 1857, 1863–66 (2021) (describing derivative suits on breaches of oversight duties as increasingly successful, as Delaware is defining more business activities as "mission critical," which creates a more rigorous duty to monitor); Lisa M. Fairfax, *Managing Expectations: Does the Directors' Duty to Monitor Promise More Than It Can Deliver?*, 10 U. ST. THOMAS L.J. 416, 418 (2012) (questioning whether the 21st century "efforts at enhancing oversight" are practicable and reasonable); Robert T. Miller, *The Board's Duty to Monitor Risk After* Citigroup, 12 U. PA. J. BUS. L. 1153, 1154–56 (2010) (describing SEC rule changes and political and academic proposals for more oversight in the wake of the 2008 financial crisis); Stephen M. Bainbridge, Star Lopez & Benjamin Oklan, *The Convergence of Good Faith and Oversight*, 55 UCLA L. REV. 559, 560–62 (2008) (criticizing good faith and oversight duties as "unnecessarily complicat[ing]" Delaware law); H. Justin Pace & Lawrence J. Trautman, *Mission Critical:* Caremark*,* Blue Bell*, and Director Responsibility for Cybersecurity Governance*, 2022 WIS. L. REV. 887, 888–89, 894, 896, 938 (describing how oversight claims gained significance in 2019 when the "Delaware courts . . . allowed five *Caremark* claims to survive" and, in the cybersecurity context, explaining that "[b]oards . . . suffer from a lack of cybersecurity subject matter expertise" and that while "[c]yber incidents have not traditionally resulted in liability for directors on the basis that they failed to provide proper oversight," any board should prepare for the possibility that "that may soon change" by creating a committee either devoted entirely to cybersecurity or with "cybersecurity as a significant part of its portfolio"); Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, 13 HASTINGS BUS. L.J. 275, 275–76, 280–82 (2017) (arguing that enterprises need to prepare for and respond to crises such as the Deepwater Horizon oil spill and the World Trade Center terror attacks); Jennifer Arlen, *The Story of* Allis-Chalmers*,* Caremark*, and* Stone*: Directors' Evolving Duty to Monitor* 23 (Law & Econ. Rsch. Paper Series, Working Paper No. 08-57, 2008), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1304272 ("To ensure that their firms abide by the laws, directors must assume direct responsibility—and active oversight—over corporate compliance. This includes intervention to adopt an effective compliance program as well as a willingness to assume direct authority over investigations of potential wrongdoing."); Regina F. Burch, *Director*

losses? How should corporate law look to the duty of oversight for holding directors responsible for harmful outcomes that do not involve wrongful or illegal acts? There is a tendency to search for answers in the easiest of places that leads to convincing results that are far from the truth.[12] There are varying scholarly views on the duty of oversight, and some scholars consider the doctrine to be "immature and incoherent,"[13] others consider its scope to be too narrow and argue it should be expanded,[14] while others still consider it to represent a "dated approach."[15] Scholars such as Professor Lisa Fairfax[16] and Professor Eric Pan[17] have described the oversight doctrine in analogies that reflect a need for more clarity. The metaphors provided by Professors Fairfax and Pan are highly salient for the

---

Oversight and Monitoring: The Standard of Care and the Standard of Liability Post-Enron, 6 WYO. L. REV. 481, 485–89 (2006); Wulf A. Kaal, *A Comparative Perspective on the Limitations of the Duty of Oversight—A Comment on Lisa Fairfax* (Univ. of St. Thomas Sch. of L., Legal Stud. Rsch. Paper No. 13-04, 2013); Barak Orbach, *The Duty to Monitor Disruption Risks*, NEB. GOVERNANCE. & TECH. CTR., March 2021, at 2–3; Commission Statement and Guidance in Public Company Cybersecurity Disclosures, Securities Act Release No. 33-10459, Exchange Act Release No. 34-82746 (Feb. 26, 2018); Cybersecurity Risk Management, Strategy, Government, and Incident Disclosure, 87 Fed. Reg. 16590 (proposed March 23, 2022); Press Release, SEC, SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (Mar. 9, 2022), [https://perma.cc/E95J-MA8N]; Press Release, SEC, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (July 26, 2023), [https://perma.cc/4755-55G9].

12. The "streetlight effect" (also known as the drunkard's search principle), is a type of observational bias that occurs when people only search for something where it is easiest to look. This streetlight inference phenomena suggests that people very often look for things where it seems convenient and comfortable and not where it is dark. *See* David E. Bernstein, *The Abuse of Executive Power: Getting Beyond the Streetlight Effect*, 11 FIU L. REV. 289, 304–05 n.82 (2016) (defining the streetlight effect); *see generally* Suryapratim Roy, *The 'Streetlight Effect' in Commentary on Citizenship by Investment*, *in* CITIZENSHIP AND RESIDENCE SALES: RETHINKING THE BOUNDARIES OF BELONGING 309 (Dimitry Kochenov and Kristin Surak eds., 2023) (discussing the negative impact of the streetlight effect on sale of citizenship); *see also* ABRAHAM KAPLAN, THE CONDUCT OF INQUIRY: METHODOLOGY FOR BEHAVIORAL SCIENCES 11, 17–18 (1980) (discussing the drunkard's search principle in behavioral science); CENGIZ DEMIR, TALES FROM NASREDDIN HODJA (2015) (describing an anecdote concerning the "streetlight effect" attributed to Nasreddin Hodja, who is credited with a tale about people who seek exotic sources for enlightenment).

A man was walking home late one night when he saw Mullah Nasreddin on his knees, searching under a street light for something on the ground.
"Mullah, what have you lost?" he asked.
"The key to my house," Nasreddin said.
"I'll help you look," the man said.
Soon, both men were down on their knees, looking for the key.
After some time, the man asked: "Where exactly did you drop it?"
Nasreddin waved his arm back towards the darkness. "Over there, in my house."
The man jumped up. "Then why are you looking for it here?"
"Because there is more light here than inside my house."
Looking for the Key, *in* CENGIZ DEMIR, TALES FROM NASREDDIN HODJA

13. *See* Fairfax, *supra* note 11, at 418.

14. *See Assessment*, *supra* note 11, at 210–11.

15. Faith Stevelman & Sarah C. Haan, *Boards in Information Governance*, 23 U. PA. J. BUS. L. 179, 271 (2020).

16. *See* Fairfax, *supra* note 11, at 417 (describing the oversight doctrine as being akin to evaluating whether directors had been "asleep at the switch").

17. *See Assessment*, *supra* note 11, at 211 (suggesting that the oversight doctrine is "like the drunk who only looks for his lost keys under the street lamp because that is where the light is").

need for greater clarification of directors' duty of oversight, which continues to unfold, even as it has seemed to be reinvigorated recently.[18]

In the context of the fiduciary duty of oversight, Delaware courts have not articulated its nature and contours.[19] While no U.S. court has defined the scope for attribution of corporate losses that give rise to oversight liability,[20] in practice, the material losses and surrounding circumstances shape the expectations of the duty of oversight.[21] To mitigate the impact of this effect in corporate governance for assessing liability with harm to the corporation, this Article takes the view that there should be a skeptical view of the duty of oversight. It argues against an overly strict expectation of corporate oversight and argues for a reinvigoration of the business judgment rule as a better theory of director liability to balance risk taking and decision making made with good faith and in the best interests of the corporation.[22] The business judgment rule, which allows courts to refrain from second-guessing directors' decisions so long as a rational basis can be found, is a better assessment of the liability of a director's decision making rather than discerning whether directors' conduct demonstrated proper oversight to prevent corporate losses.[23] The duty of oversight has been applied too expansively and inconsistently.[24]

Key issues explored in this Article are whether directors did their job, why courts excuse or do not excuse directors, and how courts should define and assess the duty of

18. *See* Pace & Trautman, *supra* note 11, at 891, 912–15 (describing the duty of oversight as threatening, arguing that cybersecurity may soon count as mission critical, and providing an overview of *Caremark* claims); Gail Weinstein, Phillip Richter & Steve Epstein, *2024* Caremark *Developments: Has the Court's Approach Shifted?*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 20, 2024), [https://perma.cc/HJ9W-BK4H] (explaining that the Delaware Court of Chancery has seemingly expanded the circumstances where the duty of oversight applies, including by defining employment-related issues as "mission-critical risks," specifying cybersecurity as a "mission-critical risk" for every online company, and holding that oversight liability applies to "key compliance risks" even when they are not "mission-critical risks" and that it applies to officers in addition to directors).

19. Lyman Johnson, *The Three Fiduciaries of Delaware Corporate Law—and Eisenberg's Error*, *in* FIDUCIARY OBLIGATIONS IN BUSINESS 57, 64 (A. Laby & J. Russell eds., 2021) (describing the confusion in Delaware fiduciary duty law arising out of the influence of legal scholar Melvin Eisenberg).

20. This Article discusses Delaware law. As mentioned later in the Article, an aim is to provide proposals that would give guidance to states as they evaluate their potential adoption. *Infra* Part III.

21. Orbach, *supra* note 11, at 15.

22. *See* discussion *infra* Part III.B.1.

23. Renee M. Jones & Michelle Welsh, *Toward a Public Enforcement Model for Directors' Duty of Oversight*, 45 VAND. J. TRANSNAT'L L. 343, 354 (2012) (explaining the business judgment rule).

24. This Article argues that duty of oversight (also known as oversight liability, *Caremark* liability, or the duty of monitoring) is a standard that is being applied too expansively or inconsistently. This Article is not arguing that the duty of oversight be displaced entirely by the business judgment rule. An argument that the business judgment rule be applied to the alleged failures of oversight would represent a significant departure from existing doctrine and would effectively insulate directors from liability even in cases of total inattention. The business judgment rule is an extremely deferential standard, which if it applies, directors are rarely held liable—they only need to show that their decision had a "rational basis." *Id.* Courts applying the business judgment rule almost always uphold the challenged conduct in practice. *See* James An, *Substance and Process in Corporate Law*, 20 N.Y.U. J.L. & BUS. 187, 225 (2024) ("In the day-to-day context, the business judgment rule looms large and generally shields unconflicted management decisions . . . ."). It should be noted that under Delaware law, the business judgment rule is usually outcome determinative unless there is some basis for overcoming it, such as when there is evidence of bad faith, conflicts of interest, or failure to inform. It is also inapplicable where there is a plausible claim of oversight failure rising to the level of conscious disregard of duty (as is explained later in this Article)—the standard set forth in *Caremark* and reaffirmed in *Stone v. Ritter*. *See* discussion *infra* Part I.B. That framework, while also deferential, reflects a distinct doctrinal approach grounded in the duty of loyalty.

oversight.[25] This Article argues that directors have remained responsible for anything that goes on under their watch based on the duty of oversight, which refers to directors' obligation to prevent harm to the corporation.[26] The corporate governance issue of the duty of oversight, which is considered one of the most difficult questions in corporate law, has gained national attention when there have been well-publicized corporate crises and ensuing scholarly corporate governance debate.[27] Notable instances include the housing-price bubble and the ensuing catastrophic losses by major financial crises,[28] food safety,[29] public health,[30] transportation,[31] among other major catastrophic disruptions.[32] to corporations. But do corporate losses from these instances illustrate that harm could have been prevented had directors of the corporation taken action?

One of the most important issues in corporate governance is the way directors oversee the corporation's operations and make informed decisions based on "risks . . . requiring their attention."[33] The standards set forth for holding directors liable for corporate harm provide an incentive for directors to satisfy their duties or else face liability as an escalatory ladder ranging from a flexible duty of care analysis to a more strict oversight liability analysis.[34] Originally raised as a breach of fiduciary duty against directors who failed to properly put in place mechanisms to ferret out red flags, the duty of oversight has been much debated by scholars and rarely successful in practice by plaintiffs.[35] The scholarly literature has more or less agreed that the duty of oversight includes directors' obligation

25. *See* discussion *infra* Part I.B.

26. The duty of oversight, which is synonymous with the duty of monitoring, refers to the obligation by the board of directors to prevent possible harm to the corporation, wherein the scope of the duty refers to care that must be taken by the board to detect such possible harm that is of the type that requires board intervention. *See Duty*, *supra* note 11, at 720–21 (describing the duty to monitor and using it interchangeably with what others call a fiduciary duty of "oversight").

27. *See supra* note 11 and accompanying text.

28. *Duty*, *supra* note 11, at 718 (discussing the duty of oversight in the context of "catastrophic losses suffered by Bear Stearns, Lehman Brothers, AIG, and Citigroup"); Christine Hurt, *The Duty to Manage Risk*, 39 J. CORP. L. 253, 253–57 (2014).

29. *See, e.g.*, Marchand v. Barnhill, 212 A.3d 805 (Del. 2019) (discussing poor food safety controls with an ice-cream manufacturer that led to a listeria outbreak).

30. *See, e.g.*, *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222, 2019 WL 4850188 (Del. Ch. Oct. 1, 2019) (applying the duty of oversight to the misrepresentation of clinical trial success of a pharmaceutical company's drug).

31. *See, e.g.*, *In re* Boeing Co. Derivative Litig., No. 2019-0907, 2021 WL 4059934 (Del. Ch. Sept. 7, 2021) (applying the duty of oversight to safety issues with an airplane manufacturer).

32. *See, e.g.*, *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996) (analyzing an oversight duty claim arising from a healthcare company's failure to uncover an illegal kickback scheme); Stone v. Ritter, 911 A.2d 362 (Del. 2006) (showing the duty of oversight applied to a massive financial regulation compliance failure).

33. *Stone*, 911 A.2d at 370 (explaining that a conscious failure to oversee the company's oversight system counts as a violation of the duty of oversight because the fiduciaries are "disabling themselves from being informed of risks or problems requiring their attention").

34. *See* Stephen M. Bainbridge, Caremark *and Enterprise Risk Management*, 34 J. CORP. L. 967, 973 (2009) (describing the distinction made in *Caremark* between duty of care and duty of oversight violations); Cheryl L. Wade, *Corporate Governance Failures and the Managerial Duty of Care*, 76 ST. JOHN'S L. REV. 767, 770 (2002) ("[T]he potential for *any* duty of care litigation should serve as an incentive to boards to satisfy their duties."); Studer & De Werra, *supra* note 8, at 515 (considering cybersecurity in the duty of care context).

35. *See generally* Pace & Trautman, *supra* note 11 (discussing trends in duty of oversight cases); *Caremark*, 698 A.2d at 971–72 (illustrating how directors are typically not liable if they acted in good faith).

to oversee corporate activities that ultimately result in corporate harm which could have been prevented.[36] Courts have more or less dismissed lawsuits with a duty of oversight claim, until recently, a few claims survived in cases dealing with directors' failure with what were deemed "mission critical risks."[37] Did the directors do their job? The answer depends on whether one believes directors had breached the duty to oversee the corporation's actions, and if so, what is the standard for assessing liability.

While the question of what directors are supposed to do in governing corporate affairs is fairly well understood, what is less clear is whether they are liable when things go wrong and there is corporate harm. Directors have a fiduciary responsibility to protect shareholders' interests and to comply with regulations, and they can face liability if they fail to do so with bad faith or a conscious disregard.[38] The possibility of facing personal liability for harmful corporate outcomes (that do not involve wrongful or illegal acts) is one potential factor that motivates directors to act in shareholders' interests and to oversee corporate affairs diligently without excessive risk-taking.[39] Yet, measuring the extent to which the potential of being penalized for conscious disregard of known risks—that directors acted with actual or constructive knowledge that their omissions would harm the corporation—is a difficult standard for assessment.[40] The same liability applies to directors who breach the duty of oversight, so that even in different circumstances where directors' responsibility to prevent acts that lead to harmful results, one cannot know if this failure with oversight was caused by the director or the risk associated with the act or some other reason.

Scholars have long debated what efforts directors must take to detect possible corporate harm, such as the business' exposure to risk, and what types of possible corporate harm require directors' action.[41] On the one hand, scholars have argued that directors should be

36. The duty of oversight refers to the board of directors' function as an overseer (a fiduciary responsibility that stems from state statutes and obligations in the corporate governance structure), such that the directors are imposed liability for inattention or inaction that leads to harm to the corporation. *See Assessment*, *supra* note 11, at 212–16 (explaining the duty to monitor); Burch, *supra* note 11, at 489 ("The duty to monitor and oversee the corporation may arise in . . . factual situations involving directors' attention to the operation and management of the corporation."); *see* discussion *infra* Part I.B.

37. For surviving cases, see generally Marchand v. Barnhill, 212 A.3d 805 (Del. 2019); *In re* Boeing Co. Derivative Litig., No. 2019-0907, 2021 WL 4059934 (Del. Ch. Sept. 7, 2021); Teamsters Loc. 443 Health Serv. & Ins. Plan v. Chou, No. 2019-0816, 2020 WL 5028065 (Del. Ch. Aug. 24, 2020); Hughes v. Hu, No. 2019-0112, 2020 WL 1987029 (Del. Ch. April 27, 2020); *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222, 2019 WL 4850188 (Del. Ch. Oct. 1, 2019).

38. HOLGER SPAMANN, SCOTT HIRST & GABRIEL RAUTERBERG, CORPORATIONS IN 100 PAGES 35 (2020); Deborah A. DeMott, *Directors' Duty of Care and the Business Judgement Rule: American Precedents and Australian Choices*, 4 BOND L. REV. 133, 133 (1992); Johnson, *supra* note 19, at 67–69 (explaining fiduciary duties under Delaware law).

39. Louis J. Bevilacqua, *Monitoring the Duty to Monitor*, N.Y. L.J.: CORP. GOVERNANCE, Nov. 28, 2011, at 1 (describing personal liability for actions taken in bad faith) [https://perma.cc/SNZ7-6ND4]; George W. Dent, Jr., *The Revolution in Corporate Governance, the Monitoring Board, and the Director's Duty of Care*, 61 B.U. L. REV. 623, 626–30 (1981) (describing the board's role in monitoring).

40. *See* Elaine E. Bucklo, *The Supreme Court Attempts to Define Scienter Under Rule 10b-5:* Ernst & Ernst v. Hochfelder, 29 STAN. L. REV. 213, 215 (1977) (describing the difficulty of understanding scienter in the securities law context); Justin Jennewine, *What's Mine is Yours: The Circuit Split Over Collective Corporate Knowledge in Securities Fraud Litigation*, 84 U. CIN. L. REV. 847, 848–49 (2018) (describing the same); Hurt, *supra* note 28, at 270–71, 285; Studer & De Werra, *supra* note 8, at 516.

41. *See, e.g.*, Fairfax, *supra* note 11, at 418 (arguing that oversight is complicated and that Delaware law cannot expect more from directors); *Assessment*, *supra* note 11, at 212 (describing efforts and harms relevant to

informed about what is occurring within the corporation and be prepared to respond to occurrences that can cause large scale disruption to the business based on directors' omissions.[42] On the other hand, "directors are outsiders working part-time," and as such, the "increasing complexities" of understanding internal corporate affairs make it "unreasonable" for directors to oversee risks to the corporation.[43] Another more recent perspective has argued that while no court has defined the attributes of corporate losses that may give rise to directors' liability for failure of oversight, the duty to oversee material disruption risks already exists within contemporary governance norms and is part of the duty of oversight for directors.[44]

The normative debate about the duty of oversight has struggled to describe and theorize what exactly is being overseen and failed to prescribe the standard for how directors should oversee risks, corporate harm, and crises.[45] In many ways, as this Article argues, the duty of oversight in corporate governance scholarship is especially more challenging in the digital age and needs greater evaluation in general.[46]

In addition to raising skepticism about the duty of oversight doctrine and its standard for assessment, this Article examines potential problems and challenges with cybersecurity, which is a central concern for corporations.[47] In order to explore the duty of oversight's standard, this Article examines modern concerns with cybersecurity in corporations.[48] Cybersecurity risk is a risk that changes the landscape for potential director liability because of the uniqueness with continual monitoring, evidentiary problems, and technological complexity that presents concerns for the modern corporation.[49] The facts of the

---

the duty to monitor); Miller, *supra* note 11, at 1154–56 (discussing scholarly and political calls for greater oversight expectations); Bainbridge, Lopez & Oklan, *supra* note 11, at 561 ("Delaware law requires a director to have a rudimentary understanding of the firm's business and how it works, keep informed about the firm's activities, engage in a general monitoring of corporate affairs, attend board meetings regularly, and routinely review financial statements."); Arlen, *supra* note 11, at 1–2, 22–23; Pace & Trautman, *supra* note 11, at 891–92; Orbach supra note 11, at 2–4.

42. Fairfax, *supra* note 11, at 418 (noting that "there appears to be a growing desire to make the oversight role more robust to ensure that directors pay greater attention to their monitoring responsibilities so that they can be more informed regarding what is occurring within the corporation, better prepared to respond to those occurrences, and better equipped to prevent inappropriate conduct."); Burch, *supra* note 11, at 489; Orbach, *supra* note 11, at 2–3.

43. Kaal, *supra* note 11, at 9.

44. Orbach *supra* note 11, at 1, 15–16, 18.

45. Jonathan Bundy et al., *Crisis and Crisis Management: Integration, Interpretation, and Research Development*, 43 J. MGMT. 1661, 1663 (2017).

46. *See* Stevelman & Haan, *supra* note 15, at 197 ("[T]he internet had had a revolutionary impact on corporate affairs.").

47. Cybersecurity risk is a critical and highly publicized legal issue facing businesses. The problem stems from the fact that nearly all of a business' records and transactions are created, communicated, stored, and transmitted in digital form using networked computers and interconnected devices. Unauthorized access, alteration, disclosure, use, and accidental loss of data and personal information stems from cyberattacks and data breaches, which can range from unexpected and unintentional disruptions to intentional and sophisticated planned cyberattacks. A patchwork of laws increasingly imposes on businesses a duty to provide security of data and to protect against cybersecurity risk. As security of data evolves into a legal obligation, monitoring of the cybersecurity risk has become a corporate governance concern for the board of directors.

48. *See* discussion *infra* Part II.A.2.

49. *See* Pace & Trautman, *supra* note 11, at 896–97; *see also* Studer & De Werra, *supra* note 8, at 512 ("Companies currently face a great deal of uncertainty when assessing the risk of legal liability that may arise from or following a cyber-attack.").

recent and regular flurry of corporate cyberattacks and data breaches to corporations continue to unfold.[50] One consideration that has seemed apparent almost immediately was that directors were not adequately informed about the corporation's affairs with cybersecurity-related reporting or information systems or controls. This is especially true in light of the fact that "[v]irtually every facet" of corporate affairs has become connected with cybersecurity in modern-day corporations.[51] It will become more difficult to detect and evaluate whether directors consciously disregarded implementing adequate reporting information systems or controls.[52] That duty, however, can be clarified to guide courts, corporations, and directors with conduct that will help restore shareholder confidence.[53] While there has been scant discussion in legal scholarship, legislation, and case law of the duty of oversight risks, such as cybersecurity risk, as this Article assesses and reveals, it would be inconsistent with existing corporate fiduciary law and inherently unmanageable.

This Article proceeds in three Parts. Part I describes directors' fiduciary duties and their evolution towards the unfolding of the duty of oversight. This history, which delves into associated cases, highlights the recent shift in reinvigorating the duty of oversight and reveals the incoherence of the doctrine, while prompting new interpretations of the duty of oversight. Part II explores the undertheorized phenomenon of risk and its impact on the duty of oversight. It describes the emergence of cybersecurity as a central corporate governance concern, which after introducing its technological foundations characterizes its implications for corporate governance, the duty of oversight, and cyber risk management. Part II draws on these accounts to explore several policy considerations of these findings. Part III builds a foundation for a more holistic law and policy framework for the duty of oversight with theoretical insights and normative analysis, prescriptions, and future directions. It also offers prescriptions for pragmatically reforming the duty of oversight by shifting it in different ways and explores their effects on corporations. Part IV concludes.

I. DUTY OF OVERSIGHT AMONG FIDUCIARY DUTIES IN CORPORATE LAW

Fiduciary law has long roots in law.[54] An important foundation of fiduciary law is the "concern with relationships in which one person is empowered to exercise decision-making authority on behalf of another."[55] There are many dimensions to fiduciary law, but one of most relevant for the purposes of corporate law is the relationship between the director of

50. Phyllis Sumner, Jonathan Day & Michael Mahoney, *Cybersecurity: An Evolving Governance Challenge*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Mar. 15, 2020), [https://perma.cc/SB62-DT87] (discussing directors' challenges with cybersecurity and breaches); SEC, PUBLIC COMPANY CYBERSECURITY DISCLOSURES; FINAL RULES 1 (2023), [https://perma.cc/69X2-TA27] (explaining that "cybersecurity threats and incidents pose an ongoing and escalating risk to public companies").

51. Stevelman & Haan, *supra* note 15, at 197.

52. *See generally In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996) (clarifying the duty of oversight); *see also* Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006) (describing a board's failure to act by either "utterly fail[ing] to implement" or "consciously fail[ing] to monitor" reporting systems or controls as violations of the duty of oversight for "demonstrating a conscious disregard for their responsibilities").

53. *See* discussion *infra* Part II.C.

54. Paul B. Miller, *The Fiduciary Relationship, in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW 64–67 (Andrew S. Gold & Paul B. Miller eds., 2014).

55. Lionel Smith, *Fiduciary Relationships: Ensuring the Loyal Exercise of Judgment on Behalf of Another*, 130 L.Q. REV. 608, 608 (2014).

the corporation and its shareholders.[56] As such, fiduciary duties are central to corporate governance,[57] which requires that the business affairs of a corporation be managed by or under the control of its directors.[58] Fiduciary duties are "meant to reduce agency costs between shareholders and directors" and are meant "to impose liability for director wrongdoing."[59]

The existence and exercise of this power with fiduciary duties, however, frequently clashes with assessment of the standard of liability in light of observational biases and hindsight biases.[60] This tension is evident in the duty of oversight (also called the duty of monitoring), which like all fiduciary duties, is associated with prohibiting directors from acting against the interests of the corporation's shareholders.[61] The rise of disruptive risks, which this Part assess cases that discuss mission critical risks, has challenged fundamentally yearnings for a safety valve to prevent opportunist directors who might abuse the structure of their duties.[62] This tension between risk and the duty of oversight is especially acute in cybersecurity, which is distinctive because of uniqueness with continual monitoring, evidentiary problems, and technological complexity that present central corporation concerns for the modern corporation.[63] To explore this tension, it is helpful to first examine the context of fiduciary duties, including the advent of the duty of oversight, which are topics that the Article turns to next.

---

56. Harvey R. Miller, *Corporate Governance in Chapter 11: The Fiduciary Relationship Between Directors and Stockholders of Solvent and Insolvent Corporations*, 23 SETON HALL L. REV. 1467, 1470 (1993) (describing a director's duties of care and loyalty owed to "the corporation and its stockholders").

57. Bryce C. Tingle & Eldon Spackman, *Do Corporate Fiduciary Duties Matter?*, 4 ANNALS CORP. GOVERNANCE 272, 274 (2019).

58. Miller, *supra* note 56, at 1469–70.

59. Darian M. Ibrahim, *Individual or Collective Liability for Corporate Directors*, 93 IOWA L. REV. 929, 931 (2008).

60. Niek Strohmaier et al., *Hindsight Bias and Outcome Bias in Judging Directors' Liability and the Role of Free Will Beliefs*, 51 J. APPLIED SOC. PSYCH. 141, 142 (2021) (defining "hindsight bias" as "perceiving past events as more foreseeable and/or inevitable than was realistically the case prior to the event's unfolding" and warning that "decisions made by a director that seemed reasonable at the time, might in case of a bad outcome (e.g., company going bankrupt) be perceived as negligent").

61. Paul D. Weitzel, *The Case Against Officer Fiduciary Duties*, 102 NEB. L. REV. 344, 352–55 (2023) (explaining that fiduciary duties are expected to "prohibit[] directors and officers from acting against the interests of the corporation's shareholders").

62. Henry E. Smith, *Why Fiduciary Law is Equitable, in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW (Andrew S. Gold & Paul Miller eds., 2014).

63. Martin Lipton, Sabastian V. Niles & Marhsall L. Miller, *Risk Management and the Board of Directors*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Mar. 20, 2018), [https://perma.cc/M4FL-YW8C] (describing oversight difficulties with cybersecurity); JOSEP DOMINGO-FERRER ET AL., WHITE PAPER 4: TECHNOLOGICAL CHALLENGES IN CYBERSECURITY 13 (2017) (describing evidentiarily difficult cybersecurity threats such as "Memory-Resident Malware"); Shaivesh Kamra, *Impact of Data Breaches to Organizations and Individuals*, 3 (Feb 24, 2020), https//ssrn.com/abstract=3510590 (describing unique risks in cybersecurity, including artificial intelligence and the reality that "[i]nternet of things are often not built with security"); Raghvendra Kune et al., *The Anatomy of Big Data Computing*, 46 SOFTWARE: PRAC. & EXPERIENCE 79, 79–81 (2016) (showing the complexity of modern cloud-based methods of gathering, storing, and monitoring data); *see also* Herbert Zech, *Information as Property*, 6 J. INTELL. PROP., INFO. TECH. & ELEC. COM. L. 192, 193 (2015) (describing how cloud computing has complicated the relationship between data and the hardware that stores it).

A. Directors' Fiduciary Duties

In general, the principle of directors' fiduciary duties refers to pursuing the good of the corporation not their own, or else being subject to legal claims by the corporation or by shareholders.[64] As a general matter, fiduciary duties entail that a director owes duties to corporations—to act loyally and to act carefully.[65] Delaware courts speak in terms of the duty of loyalty and the duty of care.[66] Under corporate fiduciary doctrines, the duty of care requires directors "to exercise power competently," and the duty of loyalty requires directors "to advance the [corporation's] interests and bars . . . self-dealing."[67] The duty of care, which is defined by reference to reasonable prudence, is qualified by the business judgment rule that insulates decisions aimed at a corporation's best interests from after-the-fact judicial scrutiny.[68] However, director exculpation by the Delaware General Corporation Law presents a wrinkle since it "authorizes a corporate charter to eliminate the personal liability of directors for monetary damages for breach of the fiduciary duty of care."[69]

Extrapolating and abstracting from these fiduciary duties, suggests that one party is "trusted with power over the interests of another," a beneficiary that is "vulnerable as a result."[70] To facilitate such trust, the law imposes a special obligation that varies under the circumstances including with conduct, such as with directors monitoring the conduct of the agents of a corporation by exercising oversight of a reasonable information and reporting system.[71]

The duty of oversight has been anchored in the duty of loyalty, with the reasoning that a truly loyal fiduciary would properly oversee responsibility and a refusal to do so would be disloyal.[72] Said another way, liability for breaches of the duty of care are of limited concern to directors, since they can be protected by the business judgment rule, corporate indemnification, and exculpatory provisions; however, directors can face liability under the duty of loyalty for failure to properly oversee corporate affairs (or have in place the adequate reporting or information systems or controls).[73] The duty of oversight encom-

64. SPAMANN, HIRST & RAUTERBERG, *supra* note 38, at 35.

65. DeMott, *supra* note 38, at 133; Johnson, *supra* note 19, at 57–60.

66. Other duties—such as the duty of good faith, duty of oversight, and the duty to avoid knowingly unlawful actions—are typically treated as components or manifestations of the duty of loyalty and duty of care. *Stone v. Ritter* clarifies that there are only two corporate fiduciary duties, the duty of loyalty and the duty of care. Stone v. Ritter, 911 A.2d 362, 369–70 (Del. 2006).

67. SPAMANN, HIRST & RAUTERBERG, *supra* note 38, at 36.

68. Christopher M. Bruner, *Is the Corporate Director's Duty of Care A 'Fiduciary' Duty? Does it Matter?*, 48 WAKE FOREST L. REV. 1027, 1029–30 (2013).

69. Julian Velasco, *How Many Fiduciary Duties Are There in Corporate Law?*, 83 S. CAL. L. REV. 1231, 1256 (2010).

70. Julian Velasco, *A Defense of the Corporate Law Duty of Care*, 40 J. CORP. L. 647, 694–95 (2015) (quoting Julian Velasco, *Fiduciary Duties and Fiduciary Outs*, 21 GEO. MASON L REV. 157, 159 (2013)).

71. Julian Velasco, *Fiduciary Principles in Corporate Law*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW 61, 61–63 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019) (describing fiduciary duties of directors in the context of the freedom provided to them by the business judgment rule).

72. Weitzel, *supra* note 61, at 354 ("[A] truly loyal fiduciary would give proper oversight, and a bad faith refusal to do so would be disloyal. If the lack of oversight is such that it constitutes bad faith, then this breach of the duty of oversight is a breach of the duty of loyalty.").

73. Pace & Trautman, *supra* note 11, at 887.

passes a good faith effort to try "to put in place a reasonable board-level system of monitoring and reporting" of operations.[74] Under the traditional ambit of the duty to oversee, compliance, or monitoring for legal violations, is required; but it does not enforce bad decision-making or excessive risk-taking.[75] However, recently, the duty of oversight has been held to require not only legal compliance but also operational viability and financial performance.[76] More specifically, for example, the Delaware Supreme Court has established that the predicate for liability for the fiduciary duty of oversight has been set by sustained failure and continued neglect (but not brief distraction or temporary interruption).[77] Yet there are still interpretative challenges for the duty of oversight which can benefit from new elucidations.[78] Before turning to what new interpretations the duty of oversight encompasses, such as disruption risks that cause a chain reaction of high-impact corporate traumas, the next Part begins with a description of the advent of the duty of oversight and delves in the interpretative challenges with overseeing of disruption risk.

B. Advent of the Duty of Oversight

To ensure that corporations abide by the laws, directors are required to have an active oversight role. The duty of oversight has historically included appointing corporate officers and exercising informed business judgment with corporate performance, but has also come to include ensuring legal compliance.[79] The duty of oversight cases in Delaware, the dominant state in the United States for corporate law, have set a high bar for director liability, but the courts have offered little guidance on specific facts and have developed a largely incoherent doctrine.[80] Five Delaware cases demonstrate the evolution of the duty of oversight for corporate directors: *Allis-Chalmers*, *Caremark*, *Stone*, *Citigroup*, and *Marchand*.[81] The normative debate in these cases concern how to use fiduciary-duty liability to induce attention to compliance without overbearing court interference with business decisions. The underlying wrong in these cases concern triggering director liability from *inaction and inattention*, which is unlike the business judgement rule's focus on director's *actions being on an informed basis* in good faith and honest belief that the action was for the best interests of the corporation.[82]

---

74. SPAMANN, HIRST & RAUTERBERG, *supra* note 38, at 45 (quoting Marchand v. Barnhill, 212 A.3d 805, 821 (Del. 2019)).

75. *See supra* note 39 and accompanying text.

76. SPAMANN, HIRST & RAUTERBERG, *supra* note 38, at 45–46.

77. Stone v. Ritter, 911 A.2d 362, 372 (Del. 2006) (quoting *Caremark* as requiring "sustained or systematic failure" to find liability for a *Caremark* claim); MODEL BUS. CORP. ACT § 8.31(a)(2)(iv) (AM. BAR ASS'N. 1998) (describing "sustained failure" or failure to respond "timely" to what a reasonable director would have "significant concern" over as some of the conditions under which personal liability should apply to directors).

78. *See* discussion *infra* Part I.C.

79. Arlen, *supra* note 11, at 1 (explaining that "[h]istorically, Delaware permitted directors to exercise oversight indirectly through their power to hire and fire corporate officers" and that "[l]egal compliance is a natural candidate for director oversight").

80. Jones & Welsh, *supra* note 23, at 346 (criticizing the courts for "hav[ing] yet to develop a coherent doctrine governing director liability for the breach of oversight duties" and for "offer[ing] little guidance about the kinds of facts that would satisfy this arduous standard").

81. Orbach, *supra* note 11, at 11.

82. *See generally* Jeremy S. Piccini, *Director Liability, the Duty of Oversight, and the Need to Investigate*, BUS. L. TODAY, Mar. 2011 (explaining the historical impetus of the duty of oversight, what it is, and how it's

Beginning in 1963 with *Graham v. Allis-Chalmers Manufacturing Company*, the Delaware Supreme Court primarily considered whether directors should be required to oversee legal compliance, and determined that directors are not liable for losses from corporate illegality unless they ignored clear signs of wrongdoing.[83] However, this stance began to change in 1996 in a far-reaching Delaware Chancery Court opinion with *In re Caremark International Inc. Derivative Litigation*, which expanded directors' oversight duties and adopted a standard of review that constrained courts' authority to hold directors liable for poor compliance decisions.[84] In effect, *Caremark* established that the reasonableness of directors' decision-making process required a good faith effort to implement and rely on monitoring systems.[85] The *Caremark* court emphasized that timely information about potential red flags was essential for directors to perform their role, and held that directors must "exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner,"[86] but that such a duty applied to "only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system [exists]."[87] While *Caremark* expanded directors' oversight duties beyond *Allis-Chalmers* by requiring "all directors . . . [to follow] a fiduciary duty to adopt an information and reporting system" in compliance with the law, it established a narrow standard of review to govern director liability for failure to monitor compliance.[88] In rejecting gross negligence, a high hurdle was placed on showing bad faith, such that neglect resulting from a bad motive and a grossly unreasonable failure to act would not be not enough.[89]

Then in 2006, the Delaware Supreme Court in *Stone v. Ritter* affirmed *Caremark*'s statement that directors owe a duty of good faith to ensure the existence of a compliance program.[90] The *Stone* court clarified that monitoring liability can only be imposed on directors who deliberately ignored red flag issues, and in effect, made it virtually impossible to prove that directors breached their oversight duty.[91] The *Stone* court set that director oversight liability requires one of the following: (1) "directors utterly fail[ing] to implement any reporting or information system or controls;" or (2) "having implemented such a system or controls, consciously failed to monitor . . . its operations thus disabling themselves from being informed of risks or problems requiring their attention."[92]

---

investigated); *see also* Bevilacqua, *supra* note 39, at 2 (describing *Caremark* claims as being based on director "inaction").

83. Graham v. Allis-Chalmers Mfg. Co., 188 A.2d 125, 130 (Del. 1963) (providing an example of a breach: "If [a director] has recklessly reposed confidence in an obviously untrustworthy employee, has refused or neglected cavalierly to perform his duty as a director, or has ignored either willfully or through inattention obvious danger signs of employee wrongdoing, the law will cast the burden of liability upon him").

84. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch.1996) (reasoning that "a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists").

85. Orbach, *supra* note 11, at 12.

86. Caremark, 698 A.2d at 970.

87. *Id.* at 971.

88. Arlen, *supra* note 11, at 19.

89. *Caremark*, 698 A.2d at 970–71.

90. Stone v. Ritter, 911 A.2d 362, 369–70 (Del. 2006).

91. Bevilacqua, *supra* note 39, at 2.

92. *Stone*, 911 A.2d at 370.

Most recently, Delaware courts tightened the standard upon which directors could be held liable for oversight claims, but business risks or market trends have never been found by a Delaware court to implicate a director's duty of oversight.[93] In more recent cases, the Delaware judiciary has limited the finding of oversight liability to the most extreme instances of bad faith, those involving violations of law, rather than business risk, for which there is protection by the business judgment rule.[94] The 2009 Delaware Court of Chancery case *In re Citigroup Shareholder Derivative Litigation* concluded that *Caremark* only applies to legal risks and ruled that directors cannot be held liable for risks associated with financial bubbles.[95] In the 2019 case *Marchand v. Barnhill*, the Delaware Supreme Court specified procedural standards for oversight matters are intrinsically critical to the company's business operations, and in so doing, blurred the distinction between legal and business risks.[96]

Additionally, in 2019, the Chancery Court of Delaware sustained *Caremark* claims in four cases, thereby recognizing the pertinence of the duty of oversight doctrine.[97] Most recently, the 2021 Delaware Court of Chancery case *In re Boeing Company Derivative Litigation* found it reasonable to infer that Boeing's directors breached their oversight duties by not doing enough to oversee, prevent, and react to 737 Max safety issues.[98] As a result of the *Boeing* case, courts will give more weight to culpable ignorance (what they should have known), proper documentation to oversee issues, and the sharing of information between officers and directors.[99]

C. Retheorizing the Duty of Oversight

The recent invigoration of the oversight doctrine raises the question: what among a corporation's risk management system and processes should directors be liable for overseeing? Even further, in what scenarios and ways should directors be liable for failing to make a good faith effort to establish and monitor systems for identifying and responding to risks, and if so, how should it be assessed? Of course, the most straightforward answer to these questions is that directors are already liable for overseeing risk and they should be evaluated with reasoning from current case law. In fact, one scholar, Professor Orbach, has assessed broadly the duty to oversee risks of a type considered disruptive, which he argues is inherent in directors' fiduciary duties and which he suggests directors should be liable

93. Arlen, *supra* note 11, at 4–5, 18 (describing Chancellor Allen's fear that, without the good faith requirement for a *Caremark* claim, oversight liability would make directors "excessively risk averse"); Roy Shapira, *Max Oversight Duties: How* Boeing *Signifies a Shift in Corporate Law*, 48 J. CORP. L. 119, 125, 142–43 (2022) (explaining that *Caremark* claims historically only proceeded for failure to monitor illegal conduct, but suggesting that, in the future, Delaware may allow claims in the context of failure to adhere to nonlegal ESG requirements).

94. Miller, *supra* note 11, at 1153–56 (describing and criticizing reform advocates who want to see oversight liability for failure to monitor business risk in the wake of the 2008 financial crisis).

95. Orbach, *supra* note 11, at 12–13.

96. Marchand v. Barnhill, 212 A.3d 805, 809, 821–22, 824 (Del. 2019) (focusing on the lack of oversight for an area of the business that was "essential and mission critical").

97. *See* Shapira, *supra* note 11, at 1860, 1863–66 (describing the "quadfecta" of *Caremark* claims succeeding beyond the motion to dismiss); *see also* Pace & Trautman, *supra* note 11, at 890–91, 922–25 (explaining *Teamsters Local v. Chou*).

98. *In re* Boeing Co. Derivative Litig., No. 2019-0907, 2021 WL 4059934, at *32 (Del. Ch. Sept. 7, 2021).

99. Shapira, *supra* note 93, at 138.

for its failure.[100] Professor Lisa Fairfax has noted that oversight liability is challenging to assess by stating that "the nearly insurmountable standard for imposing liability for oversight breaches at best may render the doctrine irrelevant for purposes of encouraging appropriate director behavior, and at worst may undermine the extent to which directors feel compelled to take their oversight [monitoring] role seriously."[101]

Much legal scholarship on the duty of oversight focuses on the important question of whether an attempt in good faith to establish a reasonable reporting system for risk monitoring and not ignoring resulting red flags if directors had taken their responsibility to oversee corporate affairs more seriously.[102] This is considered "possibly the most difficult theory in corporat[e] law" for a plaintiff to win a judgment.[103] The standards set forth in cases have not proved particularly helpful in holding directors accountable for breaching the duty of oversight, which reflects the view that breaches should be difficult for plaintiffs to litigate so as not to diminish the willingness of directors to take risks that might otherwise enhance shareholder value.[104]

Scholars have fruitfully attempted to assess the perceived tensions between obligations and breaches of oversight liability but have not attempted to reveal the direct mechanism of risks by which to connect to director liability. Courts have struggled to resolve the apparent conflicts between risk of a threat and oversight liability's accountability for corporate losses.[105] Also, courts and commentators have been suspicious of expansion of oversight liability. For example, Professor Robert Miller has noted that an expansive oversight liability would be "tantamount to repealing the business judgment rule" and would not make practical sense.[106] By considering a broad swath of risk in oversight liability, it would in effect require repealing or significantly abridging the exculpatory clauses in a corporation's charter.[107] Additionally, the court in *Stone v. Ritter* has criticized broad oversight by interpreting the duty to monitor such that oversight suits would be blocked by a burdensome scienter requirement.[108] An additional debate is whether risks are disruptive when

100. Orbach, *supra* note 11, at 16.

101. Fairfax, *supra* note 11, at 418.

102. The duty of oversight is also referred to as the duty to monitor, and the terms are used interchangeably. Delaware case law most often uses duty of oversight.

103. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996).

104. *See generally* Hurt, *supra* note 28.

105. Thomas Wuil Joo, *Theories and Models of Corporate Governance* 5–6 (Univ. of Cal., UC Davis Legal Stud. Rsch. Paper Series, Rsch. Paper No. 213, 2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1543397; Lyman P.Q. Johnson & David Millon, *Recalling Why Corporate Officers are Fiduciaries*, 46 WM. & MARY 1597, 1607–08 (2005); John Pound, *The Promise of the Governed Corporation*, HARV. BUS. REV., Mar.–Apr. 1995, at 90 ("Corporate failures occur because of subtle failures in the decision-making process—in how boards and managers make decisions and monitor corporate progress."); OECD, RISK MANAGEMENT AND CORPORATE GOVERNANCE 13 (2014) ("[E]ffective risk management is not about eliminating risk taking, which is indeed a fundamental driving force in business and entrepreneurship. At the same time, the need to strengthen risk management practices has been one of the main lessons from the financial crisis.").

106. Miller, *supra* note 11, at 1156 (describing proposals to expand oversight duties as "entirely impracticable").

107. DEL. CODE ANN. tit. 8, § 102(b)(7) (2025) (providing that a Delaware corporation's certificate of incorporation may contain "[a] provision eliminating or limiting the personal liability of a director or officer to the corporation or its stockholders for monetary damages for breach of fiduciary duty as a director or officer," but not including duty of loyalty breaches, acts "not in good faith," and not applicable to a director under Section 174).

108. Miller, *supra* note 11, at 1163.

they are realized and what those risks entail. These discussions motivate even greater discussion on new interpretations for the duty of oversight.[109]

The dominance in the duty of oversight of omissions by directors has left little space for other values or justifying interpretations. Mainstream duty of oversight perspectives still focuses on the necessary conditions of omissions. After all, a director who is inactive or inattentive to a risk that causes a harm to the business has arguably failed to oversee adequately. However, courts have traditionally limited this perspective to legal risks for which compliance is satisfactory.[110] Similarly, courts have traditionally not assessed the characteristics and nature of the risk that causes corporate losses because of direction omission.[111]

Tellingly, new interpretations of risks provide motivations and justifications for the duty of oversight and even for information flows within a business.[112] For example, the recent interpretation in the 2019 case *Marchand v. Barnhill* that the substantial blurring of business and legal risks is indeed significant for the duty to oversight.[113] Underappreciated but important shifts in interpretation of risk necessitate a methodological reassessment of directors' liability.[114] Seen in this light, the Delaware courts' oversight decision in *Marchand* reflects a sentiment that risk oversight is critical to a business's operation and towards assessment of the directors' good faith efforts.[115] Additionly, in parallel to Delaware courts' invigoration of the oversight duties under *Caremark* and encountering inseparable business and legal risks in *Marchand*, oversight liability is encountering external situations that are not caused by the business but may give rise to liability.[116] Whereas shareholder derivative lawsuits concerning breach of oversight obligations in Delaware are overwhelmingly dismissed or settled,[117] increased proliferation of and attention to risks compel examination of whether directors should be held accountable for corporate losses from failure to oversee disruptive vulnerabilities for businesses. This normative consideration forms the basis of the ensuing Parts of this Article and has significant implications for theoretical insights and normative analysis, prescriptions, and future studies in Part III.

---

109. *See* discussion *infra* Part II.A.

110. Arlen, *supra* note 11, at 1–2 (specifying Delaware's historical understanding of oversight as "a duty to oversee their firm's compliance with criminal laws").

111. *See* discussion *infra* Part II.A.1.

112. Shapira, *supra* note 93, at 121 (describing the Delaware's trend in defining risks as "mission critical" and, thus, subject to *Caremark* claims).

113. Marchand v. Barnhill, 212 A.3d 805, 809 (Del. 2019) ("[D]irectors have a duty 'to exercise oversight' and to monitor the corporation's operational viability, legal compliance, and financial performance.").

114. Shapira, *supra* note 93, at 139–41 (identifying ambiguous areas for *Caremark* claims in the wake of *Boeing*).

115. *Marchand*, 212 A.3d at 824 (finding the failure to monitor a listeria outbreak as sufficient to claim an oversight violation because, upon analyzing the operations of the corporation, the court found that the listeria outbreak affected operations that were "essential and mission critical").

116. *See generally In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch.1996); *Marchand*, 212 A.3d at 809, 823–24; *see also* Pace & Trautman, *supra* note 11, at 891 (describing the "reinvigorated" duty to monitor after *Marchand*).

117. Shapira, *supra* note 11, at 1859 (explaining that, historically, "derivative actions over directors' failure of oversight were routinely dismissed at the pleading stage"); Orbach, *supra* note 11, at 2, 14.

1. Monitoring of Oversight Risks

While the substantial blurring of business and legal risks is indeed significant, this Part highlights an underappreciated but important shift in risk that necessitates a methodological reassessment of directors liability.[118] In parallel with Delaware courts line of cases concerning the duty of oversight starting with *Caremark* and turning to *Marchand* (that emphasized the inseparable nature of business and legal risks), oversight liability is encountering new situations that may give rise to liability.[119] Whereas shareholder derivative lawsuits concerning breaches of oversight obligations in Delaware are overwhelmingly dismissed or settled, new types of exogenous oversight risks compel examination of whether directors should be held accountable for corporate harm and losses.[120] In these situations, external events and occurrences, which appears to be unrelated to directors' decision making or appear to be indirect effects of directors' decision making, raise the issue of whether corporate harm occurred from the failure to oversee disruptive vulnerabilities for corporations.[121]

In contradistinction to the duty of oversight liability's focus on internal corporate procedures that reduce the likelihood of corporate traumas, corporations have vulnerabilities to external disruptions that may differ based on the degree of risks. Although this Part distinguishes between these internal corporate procedures and external disruption trends for analytical purposes, they may be related. This Part does not contend that Delaware courts have embraced a particular assessment of corporate losses that implicate oversight liability in a way that is a means into itself. Rather, courts' assessments arise as a byproduct of failing to distinguish what risks trigger director liability under the duty of oversight. In the case of corporate crisis and disruption, evaluation of risk should necessitate reformulating whether directors took sufficient steps to enact reasonable measures.[122] Seen in this light, the Delaware courts' oversight decision in *Marchand* reflects a sentiment that risk oversight is critical to a business' operation and towards assessment of the directors' good faith efforts.[123] As such, risk assessment should go hand-in-hand with requiring courts to engage more fully with the duty of oversight. This normative insight has significant implications for the prescriptions for the duty of oversight, and of course, any move towards emphasizing *ex ante* identification of risks will likely increase directors' involvement with internal controls.[124]

---

118. *See supra* note 114 and accompanying text.

119. *Marchand*, 212 A.3d at 824 (connecting oversight liability to business risk, at least insofar as the business risk is "mission critical").

120. *See, e.g.*, Orbach, *supra* note 11, at 4–6.

121. *Id.*

122. Bundy et al., *supra* note 45, at 1664 (describing the "*internal perspective*" on crisis management as "involve[ing] the coordination of complex technical and relational systems and the design of organizational structures to prevent the occurrence, reduce the impact, and learn from a crisis").

123. *Marchand*, 212 A.3d at 809, 823–24.

124. In this sense, risk assessment implicates a tradeoff between agency cost theory of board governance and information stewardship. However, difficulties of application of information governance, where active mobilization of data reporting and analysis under the board's stewardship is likely to be exacerbated in oversight liability, where fragmentation arises since data and information can easily cross state boundaries, but states may adopt different laws.

2. Extending Oversight Liability into an Indirect Liability

As pointed out earlier, risk conceptualization and assessment offer a compelling model to reorient liability with the duty of oversight, such as to a narrower conception.[125] In sum, the limiting principles of risk assessment would shield corporate directors from the threat of a broad range of unexpected liabilities and mitigate the burden of overseeing a myriad of far-flung risks.[126] Realizing the full potential of risk should require a mechanism to impose some accountability. With a more predictable assessment of risk, the corporation should internalize that expectedness and characteristics of liability to the supply chain context as well. In this way, corporations would be held accountable for foreseeable liability that arises from such characteristic risks. Internalization of such risks would provide a powerful incentive to mitigate suspect suppliers and vendors altogether.

As such, risk conceptualization and assessment should support enterprise liability for risk that would hold directors liable for suppliers' and vendors' misconduct through an enterprise oversight liability. Unique among disruption risks, a novel theory of enterprise oversight liability would hold directors as indirectly liable for their suppliers' and vendors' judgment. Ensuring that directors are indirectly liable for their suppliers' and vendors' actions would force directors to internalize social costs. Imposing indirect liability on directors would encourage them to develop and propagate reforms through their vendors and suppliers. Attempts to hold directors secondarily liable for their suppliers' and vendors' actions may present challenges, since directors may carefully engineer legal separation with suppliers and vendors. Furthermore, enforcement of an enterprise oversight liability may present substantive, procedural, and practical barriers.

II. OVERSIGHT IN WHAT SENSE?

Scholars and courts have never squarely addressed the issue of what oversight refers to or should mean in corporate law. Nor has any other advocate of the duty of oversight been able to specifically state what oversight could be when a new circumstance applies. Part of the challenge of analyzing the duty of oversight entails defining what the term "oversight" means. Various definitions abound, and the interpretation of "oversight" can be so capacious as to encompass diverse functions in the corporate law context. However, in the *Caremark* claim context, "oversight" is synonymous with "monitoring."[127] The dictionary definition of "monitor" means "to watch, keep track of, or check usually for a special purpose"[128] or "the act of observing something (and sometimes keeping a record of it)."[129]

This Article questions whether a crisp definition exists in corporate law, and rather than offer a categorical definition, it contends that the "oversight" or "monitoring" nature of the duty of oversight is a question of degree, dependent on several factors. It is possible

125. *See* discussion *supra* Part I.C.1.

126. Instead, the duty of oversight should focus on risks that are more likely to be considered expected and predictable and correspondingly trigger a need for liability. While risk itself is premised on uncertainty and unpredictability, there are gradations and imposing a narrower view of risk assessment ensures that directors do not hale into court for minor offenses or predictable and endemic wrongs.

127. *See supra* note 26 and accompanying text.

128. Monitor, MERRIAM-WEBSTER, [https://perma.cc/C8CS-9RR6].

129. *Monitor*, VOCABULARY.COM DICTIONARY, [https://perma.cc/GT64-T6S7].

to imagine ways corporate law might be able to reconcile how to define "oversight" before considering moving the duty elsewhere or moving the duty away from directors or eliminating the duty entirely, as this Article prescribes. However, in general, the history and evolution of fiduciary duties in corporate governance demonstrates a lack of fit.[130] It may seem naïve to argue that the duty of oversight does not fit into the legal theories of fiduciary duties for corporate law, but as this Part shows, obstacles keep the duty of oversight from meetings its intended goal. Furthermore, this Part explores a specific context—cybersecurity—in which analysis and reformation of the duty of oversight is helpful.[131]

In particular, this Part argues that the emergence of cybersecurity as a central corporate law issue provides valuable insights for assessing and attributing liability when the duty of oversight does not provide sufficient deterrence to prevent the risk of corporate harm.[132] Working within the existing duty of oversight framework, this Part proposes that courts apply cybersecurity as a case study to deny director liability in cases in which disruption risk substantially causes corporate harm.[133] Drawing on concepts from risk management, this Article argues that when disruptive risk—whether cybersecurity, economic, environmental, natural disaster, pandemic, political, tort, weather, or wildfire—causes substantial corporate harm, courts should not attribute liability to directors for failure of a duty to monitor risk. In offering this proposal, this Article draws on, and in many ways challenges, previous scholarly application of a corporate fiduciary duty to oversee risk.[134] While commentators have emphasized the conceptual and technical difficulties of duty to oversee risk, this Article finds new support for applying insights from cybersecurity in recent scholarship and case law. Furthermore, it draws on theoretical accounts to show that overseeing risk may be highly conducive to other parts of the corporation or corporate law, thus mitigating significant objections to modifying or reforming the existing duty of oversight. Rather than let the duty of oversight remain doctrinally murky and not fit well into current theories of corporate governance, this Part sets the foundations for theoretical implications and normative analysis to draw prescriptions and motivate future directions.[135]

A. Corporate Law's Treatment of "Oversight"

Corporate governance seeks to provide sufficient deterrence to stop directors' behavior that could harm shareholders.[136] Fiduciary theory in corporate law provides a mechanism to protect the reified corporation.[137] A particular fiduciary duty, the duty of oversight,

130. *See* discussion *infra* Parts III.B.1–2.

131. *See* discussion *infra* Parts II.A.2, II.B.

132. *See* discussion *infra* Parts II.A.2, II.B.

133. *See* discussion *infra* Parts II.A.2, II.B.

134. Hurt, *supra* note 28; Orbach, *supra* note 11, at 15 (stating that "the oversight duty applies to only legal risks" and that "directors cannot be held accountable for corporate losses arising from failures to monitor climate change risks, wildfire risks, and cybersecurity threats").

135. *See* discussion *infra* Part II.

136. Weitzel, *supra* note 61, at 352–56 (explaining the "prohibit[ive]" function of fiduciary duties).

137. *See, e.g.*, RESTATEMENT (THIRD) OF AGENCY § 1.01 cmt. f(2) (AM. L. INST. 2006) (describing the corporate person's right to control its agents).

seeks to promote deterrence of directors' actions that could harm the corporation by conferring personal liability on the director for its breach.[138] The interpretation of "oversight" in the duty of oversight can be quite broad, which both enhances deterrence of directors' harmful actions and behaviors and provides shareholders with significant reason to file suit against directors for not properly overseeing responsibilities.[139] In the historical development of the duty of oversight, however, corporate governance cases have significantly complicated its interpretation.[140] Paradoxically, by reinvigorating the duty of oversight, courts may have chilled the momentum to question its interpretation.[141]

To understand the breadth of the duty of oversight and how it confers director liability for either a failure to implement reporting, information systems, or failure to implement controls (thus disabling directors from being informed of risks), one must understand the nature of risks.[142] All of the recent cases where a duty of oversight claim survived a motion to dismiss, which previously was a difficult threshold for plaintiffs, warrants evaluation of how risk was assessed or interpreted, so as to understand the scope of potential liability. To use an example, a shareholder could plausibly claim that corporate harm from a risk for which there was not sufficient control, information gathering, or reporting, could have been prevented had a director taken preventative action. Even if the director had simply overseen implementation of an information technology system designed to thwart cyberattacks, but one resulted, then under the recent reinvigorated duty of oversight, the director could potentially be liable.[143] However, a breach of the duty of oversight cannot be inferred from a bad outcome.[144] Of course, the requirements of duty of oversight, particularly that a claim be assessed with the risk and likelihood of the corporate harm together with a director's actions resulting in the corporate harm, constrains the scope of the liability.[145] In this fashion, risk assessment is integral to the interpretation of the duty of oversight, and this Article turns to analyzing risk and its role in corporate governance before delving into the emergence of cybersecurity as a central corporate law issue for providing valuable insights.

138. *Assessment*, *supra* note 11, at 225 (arguing that deterrence via personal liability is an important function of fiduciary duties and that the duty to monitor should be strengthened if the personal liability risk is not serious enough to deter); *Duty*, *supra* note 11, at 731–32 (describing Delaware's move towards defining oversight claims as part of the duty of loyalty, from which directors' personal liability cannot be excluded).

139. Weitzel, *supra* note 61, at 354–55 (describing the expansion of the breadth of oversight duties).

140. *See* discussion *supra* Part I.B.

141. Pace & Trautman, *supra* note 11, at 891, 896, 931 (describing oversight liability as "newly reinvigorated").

142. *See* discussion *infra* Part II.A.2.

143. Pace & Trautman, *supra* note 11, at 938 (explaining that a board must not delegate cybersecurity oversight to management but rather the board "must take an active hand" to avoid *Caremark* liability); Chirantan Chatterjee & D. Daniel Sokol, *Data Security, Data Breaches, and Compliance*, *in* THE CAMBRIDGE HANDBOOK OF COMPLIANCE (Benjamin van Rooji & D. Daniel Sokol eds., 2021); Brad Lunn, *Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine*, 4 J.L. CYBER WARFARE 109, 110, 124, 135 (2014); Martin Lipton, Daniel A. Neff & Andrew R. Brownstein, *Risk Management and the Board of Directors*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Nov. 20, 2019), [https://perma.cc/R254-FUYS].

144. Hurt, *supra* note 28, at 280.

145. *Id.*

1. Consideration of Risk

Much has been written about the incoherence of the duty of oversight, but much less has been written about the risk associated with directors' actions or inactions, including analyses that distinguish the liability standard applicable to varying levels of risk.[146] One issue to examine is why courts, commentators, and plaintiffs' lawyers fail to distinguish analyses of the duty of oversight breaches in a way that focuses on how the role of risk played in the directors' decision-making. This Part argues that courts should analyze the duty of oversight owed by directors by distinguishing the degree that the role of risk played in the directors' decision-making. Thus far, courts have not distinguished between the degree of risk and the directors' decision-making while overseeing reporting, information systems, or controls, leading to the conclusion that breaches of the duty of oversight could not be proven, even in instances where inattentiveness was blatant or egregious.[147] The nature of the risk inherent in action or inaction by a director underlies assessment of a directors' duty of oversight. Drawing upon risk theory and risk management literature can shed new light on both the concept of oversight itself and its relationship to directors' liability.[148]

Liability with the duty of oversight is understood as providing what could be called a "unitary" view that fails to consider the severity of risk and the nature of the risk. Within this view, the duty to oversee in corporate governance does not discriminate legal risk from other risks.[149] At least in a formal and traditional sense, courts have viewed the duty of oversight as applying to legal risks in narrow legalistic interpretations.[150] Risks may not only be legal risks, but can be strategic risk, compliance risk, and operational risk.[151] Risks may be graded differently based on a threat's characteristics.[152]

Scholars have assessed this unitary view of liability for the duty of oversight in different ways. Professor Barak Orbach, in 2021, suggested that the duty of oversight liability

146. Fairfax, *supra* note 11, at 418 (describing the duty to monitor as potentially "incoherent").

147. *See* discussion *infra* Part II.B.3.

148. For example, risk can be differentiated by the nature of a potential disruptive threat through classification by categories (such as nature of occurrence and time to impact, as well as by identification and certainty) to better appreciate critical risk assumptions at a more granular level to drive roles and responsibilities inherent in corporate governance.

149. Orbach, *supra* note 11, at 15 (stating that "the oversight duty applies to only legal risks" and that "directors cannot be held accountable for corporate losses arising from failures to monitor climate change risks, wildfire risks, and cybersecurity threats").

150. Holly J. Gregory, *Board Oversight of Compliance Risk*, 2020 THE GOVERNANCE COUNS. 38, 38.

151. OFF. OF THE COMPTROLLER OF THE CURRENCY, COMPTROLLER'S HANDBOOK: CORPORATE AND RISK GOVERNANCE 4–5 (2019).

152. The black swan metaphor represents a risk characterization that can apply to directors' liability. The color of swans has been used as a metaphor to describe the degree of improbable and significance of an event. The metaphor of the black swan has been utilized to refer to highly improbably events, which are not foreseeable by the usual statistics, and as a result, the inability to estimate the likelihood of such events precludes their application. *See generally* NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE (2007); *see also* Geary Sikich, *Black Swans, Grey Swans, White Swans*, ACCENDO RELIABILITY, [https://perma.cc/46D7-NZ6P]; Matthias Matthjis, *White, Grey, and Black (Euro) Swans: Dealing with Transatlantic Financial Risk in 2012*, AGI (April 3, 2012), [https://perma.cc/VMQ7-P3LG]; Annette Hofmann & Nicos A. Scordis, *Challenges in Applying Risk Management Concepts in Practice: A Perspective*, 21 RISK MGMT. & INS. REV. 309, 312 (2018) (discussing probabilistic approaches to uncertainty in pricing risks).

is broad by noting "that the dramatic changes in the attributes and understanding of disruption risks have broad ramifications on approaches towards oversight obligations of directors."[153] Professor Lisa Fairfax, in 2012, suggested that liability with the duty of oversight is challenging to assess by noting that "the nearly insurmountable standard for imposing liability for oversight breaches at best may render the doctrine irrelevant for purposes of encouraging appropriate director behavior, and at worst may undermine the extent to which directors feel compelled to take their oversight [monitoring] role seriously."[154] Scholars have fruitfully attempted to assess the perceived tensions between obligations and breaches of oversight liability, but have not attempted to reveal the direct mechanism of risks by which to connect to director liability. Courts have struggled to resolve the apparent conflicts between risk of a threat and oversight liability's accountability for corporate losses.[155]

In rethinking risk theory's relationship with corporate governance, there are direct mechanisms by which risk theory works in concert with oversight liability. First, by selectively considering risk classification into directors' liability evaluation, courts can help ensure risk that is germane to decision-making. In this manner, oversight liability is not a one-size-fits-all approach, and risk categorization affirmatively reduces the lack of clarity with the nature of the risk, such as the question of whether the duty of oversight applies to large-scale risks triggered outside of the corporations.[156] Second, consideration of principles of risk in evaluation of the duty of oversight would also encompass legal risks but also other types of non-legal risk. As noted, *Marchand* blurred the distinction between legal and business risks.[157] Furthermore, *Citigroup* noted that directors could not be held liable for oversight claims in the context of an external disruptive risk.[158] These cases prevent attributing corporate losses not caused or triggered by the corporation. Such interpretations, however, clash with the increasing overlap between legal and non-legal risks. The essential point is that legal and non-legal risks are difficult to differentiate in underappreciated ways. Risk theory's contribution to directors' oversight liability also sheds new light on directors and officers (D&O) insurance and for crisis management in corporations.[159]

Indeed, in proposing that consideration of risk is a worthwhile evaluation of directors' liability with the duty of oversight, there should be closer connections between risk evalu-

153. Orbach, *supra* note 11, at 18.

154. *See supra* note 101 and accompanying text.

155. *See* discussion *supra* Part I.C.

156. On the other hand, risk categorization operates in a manner that would create boundary setting challenges for courts based on the nature of the risk and would present additional board involvement into management.

157. *See supra* note 114 and accompanying text.

158. *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 130 (Del. Ch. 2009) (holding that directors could not be held liable for failing to foresee the business impact of subprime mortgages).

159. *See generally* Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1495 (2017) (arguing that "cyber incidents generally, and data breaches specifically, should be treated as strict liability offenses"); Asaf Lubin, *Insuring Evolving Technology*, 28 CONN. INS. L.J. 130 (2021) (discussing cyber insurance and comparing its regulatory value with New York's regulatory regime); *see also* Christopher C. French, *Insuring Against Cyber Risk: The Evolution of an Industry*, 122 PENN. ST. L. REV. 607, 609 (2018) (discussing the "rapidly evolving insurance market for cyber risks" where insurers "are flying blind to some extent because they do not have a track record to predict what the actual insured losses will be or how courts will interpret the policy language when disputes arise").

ation and oversight in corporate governance. Risk classification provides valuable pathways for corporate governance, and such considerations provide a normative constraint on the type of risk for which directors should have a duty of oversight. Accordingly, the duty of oversight should not be expansive.[160]

Courts and commentators have been suspicious of the expansion of liability with the duty of oversight. For example, Professor Robert Miller has noted that an expansive liability with the duty of oversight would be "tantamount to repealing the business judgment rule" and would not make practical sense.[161] Considering a broad swath of risk in liability with the duty of oversight would, in effect, require repealing or significantly abridging the exculpatory clauses in a corporation's charter.[162] Additionally, the court in *Stone* emphasized that duty of oversight claims are subject to exculpatory provisions,[163] and thus can only proceed if they allege a breach of the duty of loyalty, such as bad faith.[164] As such, courts should implement a narrower conception of risk than is presently considered for the duty of oversight.[165]

In effect, consideration of risk in assessment of the duty of oversight will shed new light on the scope of the duty of oversight. Furthermore, doing so will allow current vocabulary of corporate governance to be sharper about what it refers to a director's oversight duty—in particular, whether it's a standard of conduct or a standard of liability.

2. Emergence of Cybersecurity Risk as a Central Corporate Concern

While at first glance, focusing on a particular type of risk appears limited to corporate governance, recognizing the emergence of cybersecurity as a central corporate law issue provides valuable insights for assessing and attributing liability with the duty of oversight.[166] Some commentators have highlighted the importance of information technologies to corporate governance practices. As Professors Faith Stevelman and Sarah Haan have recognized, "[v]irtually every facet of [corporate] affairs became automated, monitored,

160. For example, the presence of crisis, disruption, and exogenous risks theories in the business and management literature—circumstances that cause sudden and far-reaching shocks to corporations—should cast doubt on scholars' arguments on the idea that directors should have a special duty to monitor such risk (such as cybersecurity, which would effectively entail a unique fiduciary responsibility over information technology).

161. Miller, *supra* note 11, at 1156.

162. DEL. CODE ANN. tit. 8, § 102(b)(7) (2025) (providing that a Delaware corporation's certificate of incorporation may contain "[a] provision eliminating or limiting the personal liability of a director . . . to the corporation or its stockholders for monetary damages for breach of fiduciary duty as a director . . . : (i) [F]or any breach of the director's . . . duty of loyalty to the corporation or its stockholders; (ii) [F]or acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law; (iii) [U]nder § 174 of [the Delaware General Corporation Law]; or (iv) [F]or any transaction from which the director . . . derived an improper personal benefit").

163. *See generally* Stone v. Ritter, 911 A.2d 362 (Del. 2006). The *Stone* court stated that oversight liability would require a failure to monitor that rises to the level of disloyalty. *See id.* at 367. That court criticized the narrow circumstances in which such oversight liability claims survive, particularly considering exculpatory provisions under DEL. CODE ANN. tit. 8, § 102(b)(7) (2025). *Id.*

164. Miller, *supra* note 11, at 1163–64 (describing the consequences of the clarification in *Stone v. Ritter* that oversight claims fall under the duty of loyalty).

165. For example, courts can help do so by considering risk considerations that result in a narrower interpretation of the duty of oversight.

166. The increasing importance of information technologies to corporate governance lends itself to policy intervention.

and remotely visible [by] software."[167] Thus, information technologies that protect against cybersecurity risk are critical to Professors Stevelman's and Haan's observation, with "enhanced computing power and communications technology . . . . the internet had had a revolutionary impact on corporate affairs."[168] Moreover, "[c]yberthreats" as Professors Pace and Trautman, observe "have become so pervasive and dangerous that cybersecurity is now mission critical to *every* publicly traded U.S. company."[169] Cybersecurity and data occupy a central position in the modern economy.[170]

Corporate losses from inadequate cybersecurity illustrate the complex ways in which the board of directors could have taken action to prevent harm to the business. In 2014, a cybersecurity attack through an email to Sony executives allowed hackers to steal large amounts of internal emails and confidential data, "paralyz[ing]" Sony's operations and creating a public relations nightmare, all of which could have been prevented by adopting a few common cybersecurity safeguards.[171] In 2017, the credit reporting agency and data broker Equifax suffered a massive data breach that comprised 143 million records as a result from a failure to install a simple software patch—a lapse in competence that led to questioning of corporate duties pertaining to data security.[172] In 2021, "Colonial Pipeline, the largest fuel pipeline in the United States, suffered the most significant [cybersecurity] attack against U.S. energy infrastructure," resulting in severely limited access to gas and jet fuel.[173] In two 2021 Executive Orders, the U.S. President identified that securing information and communications technology presented an ongoing emergency and an "unusual and extraordinary threat" for the digital economy of the U.S.[174] In 2022, a federal grand jury found the former Chief Security Officer of Uber guilty on computer fraud conspiracy charges for a scheme to prevent dissemination of knowledge of multiple data breaches of Uber's databases by hackers.[175] Today, cybersecurity impact to corporations—which includes attacking, intruding, or meddling to breakdown computer networks, whether for financial gain or for fun—costs businesses billions of dollars annually and attracts unprecedent attention.[176]

---

167. Stevelman & Haan, *supra* note 15, at 197.

168. *Id.* at 196–97.

169. Pace & Trautman, *supra* note 11, at 937.

170. Michael J. Madison, *Tools for Data Governance*, 2020 TECH. & REGUL. 29, 30–31 (explaining that "we are sharing data, almost all of the time" and that authors have described data as a valuable resource like oil).

171. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 989–91 (2018).

172. William McGeveran, *The Duty to Data Security*, 103 MINN. L. REV. 1135, 1136 (2019).

173. Ido Kilovaty, *Cybersecuring the Pipeline*, 60 HOUS. L. REV. 605, 607–08 (2023); Seth Azubuike, *Cybersecurity Attacks: Regulatory and Practical Approach Towards Preventing Data Breach and Cyber-Attacks in USA*, 1 (July 21, 2021), https://ssrn.com/abstract=3878326; *see generally* John W. Goodell & Shaen Corbet, *Commodity Market Interactions with Energy-Firm Distress: Evidence from the Colonial Pipeline Ransomware Attack*, FIN. RSCH. LETTERS, Sept. 2022, at 1 (analyzing the Colonial Pipeline ransomware attack); *see also* Shaen Corbet & John W. Goodell, *The Reputational Contagion Effects of Ransomware Attacks*, 47 FIN. RSCH. LETTERS, Feb. 2022, at 1.

174. Exec. Order No. 14034, 86 Fed. Reg. 31423, 31424 (June 9, 2021) (Protecting Americans' Sensitive Data From Foreign Adversaries); Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021) (Improving the Nation's Cybersecurity).

175. U.S. Att'y's Off., N. Dist. of Cal., *supra* note 3.

176. Yuchong Li & Qinghui Liu, *A Comprehensive Reivew Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent* Developments, 7 ENERGY REP. 8176, 8176 (2021); Habibullah Asadi, *The Economic Impact of Cyberattacks in the United States*, (Aug. 9, 2022) (Student Thesis, City University of New York)

Cybersecurity is a regular concern for businesses in a world with regular cyberattacks and data breaches.[177] Businesses seek cybersecurity so as to be secure and free from danger, fear, or anxiety from various threats with data used in information and communication technologies.[178] Indeed, cybersecurity risk has reached a state of widespread crisis for modern businesses.[179] Cyber-attacks cause multitudinous problems for businesses, including millions of dollars of damage, legal liabilities, and negative impact on stock price and valuations.[180] Technological advances in computing and connectivity of devices and the board of directors' lack of familiarity with cybersecurity has exposed businesses to new risks of damage.[181]

In describing the undertheorized, yet growing phenomenon of cybersecurity risk on corporate governance, there are unique features that differentiate it from other types of risk.[182] Recent corporate governance scholarship and policy reports have suggested that

Timothy C. Summers, How Hackers Think: A Study of Cybersecurity Experts and Their Mental Models 4 (Qualitative Research Report in Doctor of Management Program, Weatherford School of Management, 2013), https://ssrn.com/abstract=2326634.

177. *See* John L. Mills & Kelsey Harclerode, *Privacy, Mass Intrusion, and the Modern Data Breach*, 69 FLA. L. REV. 771, 771 (2017).

178. Tabrez Y. Ebrahim, *National Cybersecurity Innovation*, 123 W. VA. L. REV. 483, 492–93, 495–98 (2020).

179. SEC, CYBERSECURITY & RESILIENCY OBSERVATIONS 1 (2020) (suggesting that cyber threats are significant and increasing for corporations); Craig A. Newman, *SEC Cyber Briefing: Regulatory Expectations for 2019*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Jan. 2, 2019), [https://perma.cc/JQS8-H2S7] (describing the grave threats of cybersecurity problems that are facing companies); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 17–18 (2018) (describing that companies are increasingly using users' personal data, which when the data is used in ways that reasonable users would not expect, there is a breach of fiduciary duties by abusing users' trust).

180. Benjamin P. Edwards, *Cybersecurity Oversight Liability*, 35 GA. ST. U. L. REV. 663, 664–66 (2019); *see also* Benjamin Dynkin & Barry Dynkin, *Derivative Liability in the Wake of a Cyber Attack*, 28 ALB. L.J. SCI. & TECH. 23, 25 (2018).

181. Sumner, Day & Mahoney, *supra* note 50.

182. In exploring cybersecurity risk and its importance as a central corporate law issue, it is useful to analyze its unique attributes—anonymity, scale relative to chance (or low probability with high negative impact), and its evolving nature—and its impact on assessment of the duty of oversight. Widescale disruption based on a low probability of rapid negative impact helps to distinguish it from other types of risks that may take a longer timeframe or may have a higher probability or may be inevitable. For example, environmental risks to corporations may take years or decades to result in corporate losses if unaddressed. As another example, wildfire risk and weather risk may be more likely to occur in certain regions and are routinely addressed in risk assessment of corporations.

directors have oversight over environmental and sustainability risk,[183] economic and financial shock risk,[184] corporate social responsibility risk,[185] and disruption risk in general.[186] In many of these domains, risk management is not simply a business and operational responsibility of management, but is a governance issue within the oversight responsibility of directors.[187]

First and foremost, cyberattacks present evidentiary problems with difficulty in identifying the source. The classic cybersecurity threat is a data breach, which refers to content or metadata that can be discretely stolen or misappropriated from a corporation.[188] Cyberattacks result in asset-losses for which it may be challenging to track and find evidence of violators and their objectives.[189] It is often difficult to classify the target of a cyberattack and discriminate between the source being a private entity or from a government.[190] Accordingly, cybersecurity risks are challenging to identify and may be anonymous. As a result, corporations face difficulties in attributing their cause to any corporate decision-making.[191]

Second, cybersecurity risk is unique in the sense that it can require continual monitoring. Cybersecurity risk is tough to predict based on technicalities of the breach, responsiveness, and risk and resiliency, and requires regulation observation for prevention of

183. *See, e.g.*, Andrew Gouldson & Jan Bebbington, *Corporations and the Governance of Environmental Risk*, 25 ENV'T & PLAN. C: GOV'T & POL'Y 4, 5–8 (2007); Dianne Saxe, *The Fiduciary Duty of Corporate Directors to Protect the Environment for Future Generations*, 1 ENV'T VALUES 243 (1992); Himmy Lui, *A Fiduciary Perspective on the State's Duty to Protect the Environment*, 20 AUCKLAND U. L. REV. 101 (2014); Benjamin J. Richardson, *Putting Ethics into Environmental Law: Fiduciary Duties for Ethical Investment*, 46 OSGOODE HALL L.J. 243 (2008); Max M. Schanzenbach & Robert H. Sitkoff, *The Law and Economics of Environmental, Social, and Governance Investing by a Fiduciary*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Sept. 20, 2018), [https://perma.cc/9M35-YBHC]; Megan Starr, *ESG's Relationship to Fiduciary—From Counter to Crucial*, STEYER TAYLOR CTR. ENERGY POL'Y & FIN. (May 27, 2015); ANDREW JOHNSTON ET AL., CORPORATE GOVERNANCE FOR SUSTAINABILITY (2019); UNEP FIN. INITIATIVE, FIDUCIARY DUTY IN THE 21ST CENTURY (2019), [https://perma.cc/LN5T-BQQW].

184. *See, e.g.*, Lyman P.Q. Johnson & Mark A. Sides, *The Sarbanes-Oxley Act and Fiduciary Duties*, 30 WM. MITCHELL L. REV. 1149, 1153, 1155 (2004); Orbach, *supra* note 11, at 1.

185. *See, e.g.*, Ben Branch & Jennifer Merton, *Fiduciary Duty and Social Responsibility*, BUS. QUEST (2017).

186. *See, e.g.*, Michael W. Peregrine & Kenneth Kaufman, *The Governance Implications of Business Disruptions*, CLS BLUE SKY BLOG (Jan. 12, 2018), [https://perma.cc/4JHQ-XWGU]; Orbach, *supra* note 11, at 1.

187. Lipton, Neff & Brownstein, *supra* note 143.

188. Mills & Harclerode, *supra* note 177, 777–79 (suggesting that data can be broken down into "content" and "metadata" and referring to metadata as information about the content data).

189. PERRY E. WALLACE, RICHARD J. SCHROTH & WILLIAM H. DELONE, CYBERSECURITY REGULATION AND PRIVATE LITIGATION INVOLVING CORPORATIONS AND THEIR DIRECTORS AND OFFICERS: A LEGAL PERSPECTIVE 7 (2015).

190. Kamra, *supra* note 63, at 6. Furthermore, identification of the source of the cyberattack, otherwise known as attribution, is significantly challenging since attackers often deliberately hide their identities. *See* Kristen E. Eichensehr, *Cyberattack Attribution as Empowerment and Constraint* 2, 7 (Univ. of Va. Sch. of L. Pub. L. and Legal Theory, Paper Series 2021-04, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3767471; PAUL A. FERRILLO, NAVIGATING THE CYBERSECURITY STORM: A GUIDE FOR DIRECTORS AND OFFICERS 6–9 (Bill Brown ed., 2015); 20–27, 31–35, 38 (2015); *see, e.g.*, Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 505, 508–09 (2019).

191. AHMAD KAMAL, THE LAW OF CYBER-SPACE: AN INVITATION TO THE TABLE OF NEGOTIATIONS 23, 28–29 (2005).

harm.[192] Response measures to cyberattacks are measured in short time periods and require routine patching of communication and information systems to avoid costly harm.[193]

Third, cybersecurity risk can be technologically complex and be of an evolving nature. Theoretical insights reveal that the class arms-race and the principal-agent problem results in a constantly evolving game between offensive cyber-attacks and defense cyber defensive measures.[194] Similar to the nation-state cyber conflict, corporations are constantly facing a technological cyber arms race between defensive and offensive information security to address the other side's expected plans.[195] Rapidly advancing information technologies expose vulnerabilities of defenders, which are continually behind in information and resources.[196]

In these ways, cybersecurity represents unique characteristics and risk considerations for corporations. Many corporations do not know what they should do to oversee and detect cybersecurity risks.[197] By distinguishing cybersecurity risk from other risks, it also provides a basis for unfolding of directors' duty of oversight duties, which is next explored in more detail.

B. Cybersecurity & Its Implications for the Duty of Oversight

The dynamics of the duty of oversight and concomitant issues of cybersecurity risk explored earlier in this Article raise several important implications that motivate normative analysis and prescriptions for the duty of oversight.[198] In utilizing cybersecurity risk as a case study, this Article argues for restructuring current duty of oversight doctrine so that corporate governance can better achieve its proper goals.[199] In so doing, this Article sheds new light on the ways in which cybersecurity challenges conventional interpretation about the duty of oversight.

---

192. Gurpreet Dhillon, *What to do Before and After a Cybersecurity Breach?*, *in* THE CHANGING FACES OF CYBERSECURITY GOVERNANCE SERIES 1, 2–6 (2015).

193. David E. Sanger, Julian E. Barnes & Nicole Perlroth, *White House Weighs New Cybersecurity Approach After Failure to Detect Hacks*, N.Y. TIMES (Mar. 14, 2021), [https://perma.cc/63J3-SMTJ].

194. Michael Brolley, David Cimon & Ryan Riordan, *Efficient Cyber Risk: Security and Competition in Financial Markets*, THE FINREG BLOG (June 22, 2020), [https://perma.cc/3ASS-M4NQ].

195. Tabrez Y. Ebrahim, *Artificial Intelligence in Cyber Peace, in* CYBER PEACE: CHARTING A PATH TOWARDS A SUSTAINABLE, STABLE, AND SECURE CYBERSPACE 117, 120 (Scott Shackelford, Frédérick Douzet & Chris Ankersen eds., 2022) ("Deterrence, mitigation, and preventative [measures] with the use of information technology include application security, attack detection and prevention, authorization and access control, authentication and identification, logging, data backup, network security, and secure mobile gateways."); Jeffrey L. Vagle, *Cybersecurity and Moral Hazard*, 23 STAN. TECH. L. REV. 71, 73–75 (2020) (describing information asymmetry between parties, which can be corporations and cyber-attackers, where imbalances of information and risk of cybersecurity result in a moral hazard problem); Derek E. Bambauer, *Cybersecurity for Idiots*, 106 MINN. L. REV. HEADNOTES 172, 177, 182 (2021) (suggesting that rapidly advancing technologies expose vulnerabilities and require continual technological innovation).

196. Bambauer, *supra* note 195, at 177, 182.

197. Josephine Wolff, *Models for Cybersecurity Incident Information Sharing and Reporting Policies*, 7 (43rd Rsch. Conf. on Commc'ns, Info. & Internet Pol'y, George Mason Univ. Sch. of L., 2015), https://ssrn.com/abstract=2587398.

198. *See* discussion *supra* Parts II.A.2, III.A.–III.B.

199. *See* discussion *supra* Part II.C.

1. Characterizing Cybersecurity

Because cybersecurity has received little scholarly attention compared to other risk considerations in corporate governance scholarship, this Part provides an overview. Data in the context of cybersecurity risk is information recorded by digital means that exceeds authorized access.[200] This Part characterizes cybersecurity as unauthorized access based on the degree to which intrusion by data and information technology affects business interests and creates a reasonable risk of its misuse.[201] Cybersecurity risk has necessitated corporations to identify, detect, and recover in the face of cyberattacks with the use of data.[202]

The difficulty of businesses in providing security against data breaches—or maintaining confidentiality, integrity, and guaranteeing timely and uninterrupted nature of information, including that of private information—occurs often by viruses and malware, impersonation, and preventing of accessing offerings and services.[203] Notable data breaches for businesses include those that have impacted Colonial Equifax,[204] Home Depot,[205]

200. Lauren Henry, *Information Privacy and Data Security*, 2015 CARDOZO L. REV. DE-NOVO 107, 112, 115; Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 224 (2018).

201. Chatterjee & Sokol, *supra* note 143, at 939.

202. Peter Swire & DeBrae Kennedy-Mayo, *The Risks to Cybersecurity from Data Localization—Organizational Effects*, 8 ARIZ. L.J. EMERGING TECHS. no. 3, at 1, 3 (2025) Sumner, Day & Mahoney, *supra* note 50; Madison, *supra* note 170, at 31 (defining data as being able to be "mined, produced, constructed, collected, prepared, cleaned, scrubbed, processed, analyzed, combined, sold, stored, and shared").

203. Kamra, *supra* note 63, at 4–6.

204. Press Release, Equifax, Equifax's Statement for the Record Regarding the Extent of the Cybersecurity Incident (Sept. 7, 2017), htm [https://perma.cc/ENQ9-M485] (stating that the Equifax cybersecurity incident that impacted U.S. consumers included: "names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers of 143 million U.S. consumers . . . credit card numbers of approximately 209,000 consumers . . . certain dispute documents with personal identifying information of approximately 182,000 consumers").

205. BRETT HAWKINS, CASE STUDY: THE HOME DEPOT DATA BREACH 7–8 (2015); Kosseff, *supra* note 173, at 1004.

HSBC,[206] McDonald's,[207] Sony,[208] Target,[209] Wendy's,[210] Wyndham Hotels,[211] and Yahoo.[212] Business leaders have become increasingly concerned with cybersecurity risk following cyber-attacks that have shut down the largest gasoline pipeline,[213] the largest meat packing company,[214] and some of the largest regional medical providers in the United States.[215] Trends in cybersecurity have become more evident to businesses, which are routinely targeted by "cyber weapons of mass destruction."[216]

As such, cybersecurity can be defined as ensuring "that those, and only those, authorized to access data or computer systems are allowed to do so"; yet the challenge of designing and implementing such a secure system that prevents unauthorized activity is very difficult at a technical level.[217] A state of cybersecurity entails controlling access rights of data to authorized users, preventing data losses, enabling mobile security, and providing incident response and resiliency, yet vulnerabilities are often impossible to prevent and susceptible to cyberattacks.[218] Technical factors contribute to cybersecurity breaches, including failure to implement adequate measures to ensure unauthorized users do not have access, encrypting data, and other safeguards to protect the data.[219]

Cybersecurity has become newsworthy in modern digital commerce.[220] Corporations' records and transactions are increasingly in digital form, including personal information

206. Mills & Harclerode, *supra* note 177, at 774.

207. Heather Haddon, *McDonald's Hit by Data Breach*, WALL ST. J. (June 11, 2021), [https://perma.cc/QBW3-K7YM].

208. Claire Lending, Kristina Minnick & Patrick J. Schorno, *Corporate Governance, Social Responsibility, and Data Breaches*, 53 FIN. REV. 413, 414 (2018); Peter Elkind, *Inside the Hack of the Century*, FORTUNE (June 25, 2015), [https://perma.cc/8WY9-PEQ2]; ANTONIO DESIMONE & NICHOLAS HORTON, SONY'S NIGHTMARE BEFORE CHRISTMAS: THE 2014 NORTH KOREAN CYBER ATTACK ON SONY AND LESSONS FOR US GOVERNMENT ACTIONS IN CYBERSPACE (2017).

209. Bundy et al., *supra* note 45, at 1662 (describing Target's data breach).

210. The Wendy's Co., Letter to Office of Attorney General, Consumer Protection and Antitrust Bureau (July 5, 2016), [https://perma.cc/X7N7-JU45].

211. Timothy Cornell, *Wyndam—A Case Study in Cybersecurity: How the Cost of a Relatively Small Breach Can Rival That of a Major Hack Attack*, CORP. COUNS. BUS. J. (Mar. 19, 2015), [https://perma.cc/59YQ-FLNN].

212. Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1233–34 (2017).

213. PAUL W. PARFOMAK & CHRIS JAIKARAN, CONG. RSCH. SERV., COLONIAL PIPELINE: THE DARKSIDE STRIKES (2021).

214. Fabiana Batista, Michael Hirtzer & Mike Dorning, *All of JBS's U.S. Beef Plants Shut by Cyberattack*, BLOOMBERG (May 31, 2021) (on file with the *Journal of Corporation Law*).

215. Steve Alder, *Ransomware Attack on Scripps Health Disrupts Patient Care*, HIPPA J. (May 4, 2021), [https://perma.cc/4JR9-AXTD]; Dan Margolies, *Ransomware Attack on Midwest Transplant Network Affects More than 17,000*, KCUR (May 3, 2021), [https://perma.cc/8HMQ-JG97].

216. Robert McMillian, Dustin Volz & Tawnell D. Hobbs, *Beyond Colonial Pipeline, Ransomware Cyberattacks Are a Growing Threat*, WALL ST. J. (May 11, 2021), [https://perma.cc/444R-B3NP].

217. Hurwitz, *supra* note 159, at 1501–04 .

218. SEC, CYBERSECURITY AND RESILIENCY OBSERVATIONS 2 (2020).

219. Dhillon, *supra* note 192, at 2–3.

220. Cybersecurity protects networks and computers against cyber-attacks and is subject to threats to the privacy of the owners of systems. Concerns include data exposure, identification, activity monitoring, website monitoring, data discovery, and enterprise communication. Ari Ezra Waldman, *Outsourcing Privacy*, 96 NOTRE DAME L. REV. REFLECTION 194, 197 (2021); Eran Toch et al., *The Privacy Implications of Cyber Security Systems: A Technological Survey*, ACM COMPUTING SURVS. Feb. 2018, at 1, 13–15.

about users, employees, consumers, clients, and accounts.[221] As a result, corporations are increasingly responsible for protecting and securing personal identifiable information.[222] Corporations are seeking to defend against harm from cybersecurity threats given that commercial interactions and the merchant-consumer relationships have become increasingly data reliant.[223] The increasing implications of cybersecurity has significant implications for corporate governance.[224]

2. Implications for Corporate Governance

This Part sheds new light on the intersection of cybersecurity risk and the duty of oversight to draw implications for corporate governance. Courts and scholarly accounts of the duty of oversight have highlighted its obligations concerning risk to corporate interests. In most narratives, directors can oversee risk and reduce the chance of corporate losses by for instance, implementing reporting or information systems or controls, not consciously failing to oversee corporate operations,[225] and partaking in a "reasonable board-level system of . . . reporting" of operations.[226]

First, while these measures are largely beneficial for many risks, earlier in this Article, I have shown that cybersecurity presents a risk that is of central concern to modern corporations and securing against cybersecurity presents new challenges.[227] For instance, cybersecurity data is inherently interdependent, and has an impact across scales both in space and time.[228] In the corporate context, many overlaps exists for data among employees, suppliers, competitors, customers, tools, products, services, contracts, and intangibles.[229] Data (as applied to the cybersecurity risk context), unlike other things that have risk, can be collected, managed, maintained, scrubbed, normalized, manipulated, and classified, stored, analyzed, predicted upon, and interpreted, and it can be changed and expanded upon rapidly.[230] As such, data is highly interconnected and interdependent among many actors, organizations, and assets. Of course, it is not surprising that businesses deploy data in a variety of ways which can impact a corporation's sense of cybersecurity. It is notable, however, that data is deployed by businesses within the firm and in interactions outside of the firm in ways that promote interdependencies, which may make the business susceptible to cybersecurity risk beyond the data itself.

---

221. Christopher Kuner et al., *The Rise of Cybersecurity and Its Impact on Data Protection*, 7 INT'L DATA PRIV. L. 73, 73 (2017).

222. *See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 774–75 (2020); DOMINGO-FERRER ET. AL., *supra* note 63, at 7.

223. Tabrez Y. Ebrahim, *Algorithms in Business, Merchant-Consumers Interactions, & Regulation*, 123 W. VA. L. REV. 873, 878 (2021); *see also* Faheem Ullah & M. Ali Babar, *On the Scalability of Big Data Cyber Security Analytics Systems*, 198 J. NETWORK & COMPUT. APPLICATIONS 1, 1 (2022).

224. Petac Eugen & Duma Petruţ, *Exploring the New Era of Cybersecurity Governance*, 18 'OVIDIUS' U. ANNALS, ECON. SCI. SERIES 358, 362 (2018).

225. *See generally* Stone v. Ritter, 911 A.2d 362 (Del. 2006).

226. SPAMANN, HIRST & RAUTERBERG, *supra* note 38, at 45 (quoting Marchand v. Barnhill, 212 A.3d 805, 821 (Del. 2019)).

227. *See* discussion *supra* Part II.A.2.

228. *See* discussion *supra* Part I.B; Madison, *supra* note 170, at 34.

229. Madison, *supra* note 170, at 40.

230. *Id.* at 31.

Second, while earlier this Article illustrated how cybersecurity risk can be monitored to describe commonalities between cybersecurity and risks in general, it is important to distinguish between their differential impact and their potential for spillovers.[231] While both data risk in the cybersecurity context and non-data risks can create corporate losses, cybersecurity can be an infrastructural resource and data use can create "spillovers in multiple fields, in both expected and unexpected ways."[232] Indeed, Professor Anya Bernstein and Professor Michael Madison have stressed how the ability to interact, overlap, and align with other systems presents its potential for multitudinous impacts beyond its source.[233] In addition to data's multiplicity of uses and its propensity for spillovers, the significant connections with computer and computing systems makes data an infrastructural resource.[234] Data as infrastructure is a distinguishing feature of data that enhances its risk for creating corporate losses when not adequately secured, not only against cyberattacks and data breaches, but also when expanded to new infrastructures. In sum, cybersecurity is a more expansive vehicle for susceptibility to risk relative to other non-data risks.

Going further, even in newly developing use cases of cybersecurity and in newly developing industries, data poses significant risk of corporate loss, while such potential is more limited with non-data-driven applications and for traditional brick-and-mortar industries.[235] While this Article has emphasized the flowing nature of data and its propensity to promote interconnections and interdependencies in businesses, data can certainly multiply into new scenarios as businesses' value becomes increasingly tied to information assets. The scope of data is more than its source, and data can cover and be connected to much more real estate than real property assets owned by a business.[236] Therefore, from a diffusion perspective, the ability of data to flow and establish interconnections is vaster than compared to other things with risks.[237]

Furthermore, cybersecurity is more aptly tied to businesses' value than more exogenous things with risk. Even as data flows and is interconnected with other aspects of a business, cybersecurity is still a key aspect that is associated with the business' infrastructure or real property assets.[238] For example, unlike exogeneous shock risk, like financial crises or pandemics, data associated with cyberattacks and data breaches is endogenous in being caused by market participants, whether easily identifiable or difficult to attribute the source.[239] And as noted earlier in this Article, data serves as an exchange that affects and

231. *See generally* Mark Verstraete & Tal Zarsky, *Cybersecurity Spillovers*, 47 BYU L. REV. 929 (2022) (analyzing "cybersecurity spillovers" and highlighting tools that can be used to identify "the most beneficial spillovers").

232. Madison, *supra* note 170, at 40; *see also* Verstraete & Tal Zarsky, *supra* note 231, at 946–47.

233. Anya Bernstein, *What Counts as Data?*, 86 BROOK. L. REV. 435, 435 (2021) (stating that "the same bit of information can be data for some purposes, just information for others"); Madison, *supra* note 170, at 39 ("Data depend on their reference and relationships to underlying phenomena. In that sense, data are evidence of something else.").

234. ELLEN P. GOODMAN, THE ATOMIC AGE OF DATA: POLICIES FOR THE INTERNET OF THINGS 9, 12–13 (2015).

235. Chatterjee & Sokol, *supra* note 143.

236. Stuart Mills, Who Owns the Future?: Data Trusts, Data Commons, and the Future of Data Ownership 5–7 (Sept. 24, 2019) (London Sch. Econ. & Pol. Sci.), https://ssrn.com/abstract=3437936.

237. DOMINGO-FERRER ET. AL., *supra* note 63, at 11–14.

238. Kamra, *supra* note 63, at 1, 3, 6.

239. *See* Ebrahim, *supra* note 178, at 493–98.

influences businesses, and as such, in the process of interaction, there is a close and continuous proximity with human society and cybersecurity risk.[240] By contrast, exogeneous shocks are difficult to govern, whereas data, which can cause endogenous shocks, are within an economy and can be subject to policy formulation and governance systems.[241] Therefore, from an integration perspective, the ability of data to be more closely grounded with the business compared to exogeneous risk cannot be precipitated by human action.

As such, cybersecurity is conventionally understood as providing what could be called a new dynamism in business.[242] Within this view, as this Article argues, the duty of oversight should be concomitantly tied to cybersecurity risk of corporations.[243] In sum, the role of data in business, sheds new light on the duty of oversight itself and its relationship with corporate obligations, to which this Article turns next.

3. Implications for the Duty of Oversight

The underappreciated implication of cybersecurity risk to the duty of oversight should promote new normative conceptualization for the duty of oversight and corporate obligations. The availability and proliferation of data in business and its role in cybersecurity risk mitigation promotes new normative assessments for the duty of oversight.[244]

The duty of oversight is conventionally understood as a fiduciary obligation of what could be called risk mitigation.[245] Within this risk management, the duty of oversight does not discriminate based on the nature of the risk or source of the risk. At least in a formal sense, risk is equal to all with fiduciary responsibility who oversee corporate interests, so long as the risk is critical to the business' operations.[246] Scholars have challenged the unitary view of risk in other areas of law by revealing the subtle ways in which risk operates differently with uses of technology in foreseeability analysis.[247] In particular, researcher

240. As a result, cybersecurity risk has some uniqueness since its contribution to business reveals other ways in which the duty of oversight should deviate from a unitary view of all types of risks.

241. *See generally* Jonas Soluk, Nadine Kammerlander & Alfredo De Massis, *Exogenous Shocks and the Adaptive Capacity of Family Firms: Exploring Behavioral Changes and Digital Technologies in the COVID-19 Pandemic*, 51 R&D MGMT. 364 (2021) (exploring how exogenous shocks can challenge the understanding of corporations' behavior).

242. GOODMAN, *supra* note 234, at 1–2, 7; Muhammad Tanbirul Islam, Md Fokhurl Islam & Juairiya Sawda, *E-Commerce and Cyber Vulnerabilities in Bangladesh: A Policy Paper*, 1 INT'L J.L. & SOC. 186, 186 (2022); Varun Chotia et al., *The Role of Cyber Security and Digital Transformation in Gaining Competitive Advantage Through Strategic Management Accounting*, 81 TECH. IN SOC. 102851, 102851 (2025).

243. *See* discussion *infra* Part II.B.4.

244. *See* discussion *infra* Part III.A.

245. Martin Lipton, John Savarese & Sarah K. Eddy, *Risk Management and the Board of Directors*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Sept. 30, 2023), [https://perma.cc/DL69-EYS5]

246. Marchand v. Barnhill, 212 A.3d 805, 809, 823–24 (Del. 2019).

247. *See, e.g.*, Amy L. Stein, *Assuming the Risks of Artificial Intelligence*, 102 B.U. L. Rev. 979, 983–84, 1034–35 (2022) (discussing the definition of risk and the impact on AI users); Andrew D. Selbst, *Negligence and AI's Human Users*, 100 B.U. L. REV. 1315, 1342 (2020) ("AI is . . . 'unpredictable by design.' From there, scholars argue that AI systems pose foreseeability problems."); Tania Leiman, *Law and Tech Collide: Foreseeability, Reasonableness, and Advanced Driver Assistance Systems*, 40 POL'Y & SOC'Y 250, 250 (2021) ("Increases in safety promised by ADS . . . may require a reassessment of the risks posed by 'un-augmented' human drivers, what is now foreseeable given the data generated by ADAS and wearable driver-monitoring technology."); *see generally* Ryan Calo, *Robots in American Law* (Univ. of Wash. Sch. of L., Rsch. Paper, Paper No. 2016-04,

Meiring de Villiers has noted that courts tailor risk assessment to different uses of technology, in say, foreseeability doctrine.[248]

Cybersecurity's relationship with the duty of oversight reveals other ways in which cybersecurity risk should be distinguished from other risks. First, the interdependent and interconnection properties of data in the context of cybersecurity makes it expansive since it permeates many aspects of corporate interests. In what may be considered a unitary model of the duty of oversight, courts subtly analyze corporate losses tied to conscious disregard, but the overarching doctrine remains formally the same regardless of the risk.[249] However, as this Article has shown, data in the cybersecurity context is interdependent and interconnected such that the culpability becomes more dispersed than with tangible risks.[250] Furthermore, the defining properties of data—volume, variety, and velocity of data, or respectfully, the amount of data, the variety of types of data, and the speed of data processing—fundamentally informs the interdependent and interconnected nature of data for cybersecurity risk.[251] As a descriptive matter, defending against risks of corporate losses (based on cyberattacks and data breaches) is simply more difficult with interdependencies and interconnections in high amounts, high variety, and high speeds.[252] As a result of cybersecurity risk requiring a process-oriented repetition for identifying and addressing data-intensive threats, a more granular and graded interpretation of utter failure and conscious failure within the duty to monitor is necessary.[253]

Second, cybersecurity's relationship with the duty of oversight reveals that the nature of attribution or source of the data risk impacts the circumstances and context of the corporate obligation.[254] In what may be considered a unitary view of the duty to oversee, corporate losses should be able to be traced to the source or attributed when there is inadequate oversight of operations.[255] However, data in the cybersecurity context possess characteristics that weaken or eliminate attribution when utilized for cyberattacks or causing

---

2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2737598 (discussing how robots can create risk for businesses).

248. Meiring de Villiers, *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, 30 HASTINGS COMM. & ENT. L.J. 419, 445–48 (2008); Meiring de Villiers, *Foreseeability Decoded*, 16 MINN. J.L., SCI. & TECH. 343, 365–69 (2015).

249. The Delaware Supreme Court observed in *Marchand v. Barnhill* that the nature of the risk matters. Specifically, the Court emphasized that when a risk is "mission critical" to the company's operations, directors may face heightened obligations to implement and monitor oversight systems. *Marchand*, 212 A.3d at 824.

250. *See* discussion *supra* Part II.B.2.

251. *See* discussion *supra* Part II.B.2.

252. For instance, corporate directors are more easily accountable for a conscious disregard in failing to implement a health and safety system to report of outbreaks rather than a failing to implement virus protection resulting in damage to computing systems that could spread away from the virus protection. Furthermore, interdependencies and interconnections of data create a need for a continuum in the standard for the duty of oversight on a sliding scale. As a result of cybersecurity risk requiring a process-oriented repetition for identifying and addressing data-intensive threats, a more granular and graded interpretation of utter failure and conscious failure within the duty to monitor may be necessary.

253. THOMAS J. SMEDINGHOFF, THE STATE OF INFORMATION SECURITY LAW: A FOCUS ON THE KEY LEGAL TRENDS 1 (2008).

254. *See* discussion *supra* Part II.B.2.

255. The point being made here is about the attribution challenges that cybersecurity presents to corporate law. One goal of this Article is to clarify the connection between these attribution difficulties and the doctrinal standard for oversight liability. Delaware law does not require directors to trace specific corporate harm to a known source, but rather to make a good-faith effort to implement and monitor systems for risk detection and

data breaches. The unique properties of data in the context of cybersecurity renders the duty of oversight doctrine unenforceable if courts cannot link corporate losses to a source or the source is too far removed. For instance, the board of directors cannot be held accountable if a business' computing system is shut down due to a cyberattack or data breach when there may be a number of actors could have caused the damage, such as whether an employee's disregard or an external threat's actions. Data breaches can mask attribution, and corporate harm may be far removed from the source to hold the board of directors accountable.

4. Implications for Cyber Risk Management

As a descriptive matter, this Article has shown that cybersecurity risk raises challenges for corporate governance and for the duty of oversight.[256] Scholarly accounts of cybersecurity risk have highlighted the ability of corporations to mitigate the shortcomings of the board of directors' decision making and inattention to risks that may result in corporate losses with various approaches, including directors and officers (D&O) insurance, crisis management, and officers' liability. In so doing, a corporation can enhance its ability to oversee cybersecurity risk in ways that are different and distinct from other types of risks. In this narrative, a corporation can reduce the impact of cybersecurity risk by taking proactive measures by responding effectively, just-in-time, and quickly to cyberattacks and data breaches. Of course, it is not surprising that corporations' cyber risk management is unique relative to other risks, but it is notable, however, that businesses are using these methods in ways that supplement the board of directors' monitoring of cybersecurity risks through alternative mechanisms. As such, the key implication lies in the extent to which these approaches—D&O insurance, crisis management, and the relationship between the board of directors and officers—differ cyber risk management in corporations compared to management of other risks.

First, by its very design, "D&O insurance policies cover a company's directors and officers for claims made against them in their individual capacities" and most such policies have been considered to cover cyber-related claims.[257] However D&O policies may require purchase of cyber extensions or additional specialized cyber risk insurance.[258] Some insurers offer endorsements to reduce ambiguity or expand, especially for early-stage regulatory investigations related to cyberattacks that may not qualify as covered claims under standard

compliance. This means that even if a cyber attack's source is obscure or multifactorial, courts may still look to whether the board of directors took reasonable steps to oversee information and reporting systems.

256. *See* discussion *supra* Parts II.A.2.–.B.2.

257. MEGHAN MAGRUDER ET AL., DO YOUR CYBER AND D&O POLICIES COVER EMERGING EXPOSURES ARISING OUT OF THE NEW NYDFS CYBERSECURITY REGULATIONS? 1, 1 (2018); DAN A. BAILEY, CHUBB, CYBER LOSS MITIGATION FOR DIRECTORS 26–28 (2023).

258. French, *supra* note 159, at 609 (discussing specialized cyber risk); *see generally* AIRMIC, DIRECTORS & OFFICERS LIABILITY, UNDERSTANDING CYBER DIRECTORS & OFFICERS LIABILITY RISKS AND BUYING INSURANCE 1 (2018) (discussing cyber extensions).

policies.[259] Many of the commercial general liability policies that offer cybersecurity coverage and other cyber-insurance policies are untested in courts.[260] Indeed, the insurance industry has evolved to fruitfully attempt to address cybersecurity risk with new terms such as "affirmative cyber" as referring to purpose-built policies and "silent cyber" as referring to not being built for cyber related losses.[261] Such D&O policies are rapidly evolving and recently insurers have added exclusions for data losses and attempted to remove coverage for most cyber losses from commercial general liability policies.[262] In this manner, it is critical for corporations to review gaps and limits in the insurance policy, and to maximize coverage for regulatory investigations.[263] Cyber insurance policies vary greatly but new policies are being developed to cover costs ranging from data breaches to crisis management and response.[264] At a high level, businesses cannot hope to prevent cyber intrusions, comprehensive cyber insurance will be necessary to close the gap for insured cyber losses.[265]

Second, cybersecurity's impact on directors' liability reveals changes in organizational behavior in response to cyberattacks and data breaches. Cybersecurity risks that result in cyberattacks and data breaches necessitate organizational crisis management responses.[266] Cybersecurity risk renders crisis management of social perceptions, ceremonial actions, and negative spillovers as necessary.[267] Businesses should not only be concerned with potential board of directors' liability for cyberattacks and data breaches, but they should have concern with appropriate organizational responses, crisis management strategic planning, and information flows between the board of directors and officers.[268]

Third, calibrating oversight liability for cybersecurity threats through a more collective approach within a business should become more prominent. Liability for the duty of oversight has conventionally been attributed to the board of directors in unitary fashion.[269] At least in a formal sense, liability for decision making could be attributed to other actors in a business, and as such, cybersecurity risk can recalibrate attribution of liability. This

259. D&O policies can and often do cover certain cyber-related claims—particularly where directors are sued for breach of fiduciary duty (such as a failure to oversee cyber risk) or where a cyber incident gives rise to a securities claim. These are not categorically excluded in mainstream policies, and coverage does not necessarily depend on a special cyber extension. It should not be implied that D&O coverage for cyber-related claims are always completely unavailable without such add-ons.

260. Hurwitz, *supra* note 159, at 1537.

261. Lubin, *supra* note 159, at 158; Kevin LaCroix, *Seeking Insurance for Cybersecurity-Related Losses*, THE D&O DIARY (Nov. 24, 2019), [https://perma.cc/3TBD-SWE3].

262. French, *supra* note 159, at 609.

263. Jacquelyn Burke & Rachel Katz, *D&O Coverage for Cyber and Privacy Related Exposure*, JDSUPRA (Nov. 20, 2019), [https://perma.cc/9ULS-6TH8].

264. *See, e.g.*, *Examining the Evolving Cyber Insurance Marketplace: Hearing Before the S. Comm. on Com., Sci., and Transp.*, 114th Cong. (2015).

265. Mark Camillo, *Cyber Risk and The Changing Role of Insurance*, 2 J. CYBER POL'Y 53, 62 (2017).

266. Bundy et al., *supra* note 45, at 1662 (describing Target's consumer data breach as a crisis and explaining that crisis response strategies can provide functional and reputational help).

267. Anastasiya Zavyalova et al., *Managing the Message: The Effects of Firm Actions and Industry Spillovers on Media Coverage Following Wrongdoing*, 55 ACAD. MGMT. J. 1079, 1079 (2012); Verstraete & Tal Zarsky, *supra* note 236.

268. *See* discussion *supra* Part III.C.

269. Weitzel, *supra* note 61, at 355–56 (explaining that, in 2023, "*Caremark* duties [were applied] to officers for *the first time*") (emphasis added).

calibration can happen in two possible ways: (1) first, raising the importance of officers and correspondingly introducing a horizontal fiduciary duty in alignment with cybersecurity risk, or (2) second, strengthening the role of the stand-alone risk committee. The horizontal fiduciary duty, which refers to a fiduciary duty owed between the board of directors and officers vis-à-vis one another, should become more prominent.[270] The horizonal fiduciary duty would complement the duty owed by officers and enable the board of directors to exonerate themselves for officers' failure in diligence with cybersecurity threats, while improving information sharing between the board of directors and officers.[271] As a result, there would be a redistribution of liability and strengthening of the importance of information flows between the board of directors and officers.[272] Additionally, a transition to a more collective approach, rather than a focus on unitary individual liability, could also arise from a standalone risk committee, which could focus on compliance and risk management to articulate and establish the corporation's risk tolerance and risk appetite.[273] Foremost, raising the importance and liability of officers or a risk committee would highlight the interdependencies and interconnectedness with data in the cybersecurity context. As a result, businesses would work more closely "with management to promote and more actively cultivate a corporate culture . . . that understands and implements . . . risk management."[274] The resulting focus on a standalone risk committee for overseeing and assessing cybersecurity risk would avoid the challenges of identifying a cybersecurity expert on the board or to search for one and the information costs associated with gathering details to make risk mitigation decisions.[275] While technically the board of directors would still be liable for inaction and inattention to cybersecurity risk, a more collective approach within businesses would increase officer liability and lead to an increased importance of the risk committee.

C. Policy Considerations for the Duty of Oversight

The importance of cybersecurity with the duty of oversight raises important implications for fiduciary obligations of the board of directors.[276] In addition to pragmatically reforming the duty of oversight's treatment of cybersecurity risk, this Article suggests there

270. Asaf Eckstein & Gideon Parchomovsky, *Towards a Horizontal Fiduciary Duty in Corporate Law*, 104 CORNELL L. REV. 803, 810–11, 841–47 (2019) (defining "horizontal fiduciary duty" as "a fiduciary duty among directors and corporate officers vis-'a-vis one another").

271. *Id.* at 808–10; *cf.* Johnson & Millon, *supra* note 105, at 1600–01 (discussing the ambiguity in whether and to what extent officers and directors have different fiduciary duties).

272. *Cf.* Shapira, *supra* note 93, at 131–32, 138 (describing how a positive consequence of *Boeing* is that it incentivizes information flows).

273. Alan S. Gutterman, *Compliance and Risk Management Committee*, 1 (Dec. 1, 2020), https://ssrn.com/abstract=3833592.

274. Lipton, Niles & Miller, *supra* note 63.

275. Martin Edwards, *Expert Directors*, 90 U. COLO. L. REV. 1051, 1080–83, 1102–04 (2019) (describing the benefits of experts on the board).

276. As such, the specific context of duty of monitoring with cybersecurity risk suggests that data and information technology have become a dominant part of a modern corporation's architecture and operations.

are important policy considerations for cybersecurity law and policy, corporate governance, and corporate law.[277]

This Part turns the policy considerations of these findings to conclude that cybersecurity risk is unique, why the duty of oversight should evolve, and how reevaluation of how the duty of oversight should happen. As such, this Part suggests that just as the law should impose a special duty to directors for adopting and overseeing information and reporting systems, corporate law should provide guidance on directors' liability pertaining to implementing and overseeing compliance systems that effectively govern the corporation's cybersecurity with internal data gathering, reporting, and communication architecture.[278]

This is an important realization given that businesses are exposed to more cybersecurity risks with time.[279] The presumption that the corporate harms are easy to detect and attribute to decision making by directors assumes a basic point: risks are tangible, detectable, and easy to attribute. However, law and technology scholars have explored how data risks are have unique properties.[280] Considering that Delaware courts have not provided adequate guidance about the duty of oversight, which itself has been considered a difficult theory for plaintiffs to win on judgment, it is highly likely that as cybersecurity risk multiplies for corporations, that plaintiffs will need to provide an even higher degree of specificity in shareholder derivative suits.[281]

Importantly, this critique of the duty of oversight arises when cybersecurity and information technology becomes an increasing concern for businesses. Boundary setting with technology has attracted criticism on several normative grounds outside of the dominant objective of the law keeping pace with technology.[282] In particular, commentators have argued that law and policy should not seek technological specific evaluation given that technology changes and does so quickly. Other commentators have advocated that corporate law should be more attentive to cybersecurity and have argued that data will be

277. In particular, it suggests that cybersecurity provides valuable insight for determining a duty of oversight claim that traditionally requires showing that the lack of oversight is so bad that it constitutes bad faith. It is an assessment of good faith if information governance is a key role for directors.

278. *Cf.* Pace & Trautman, *supra* note 11, at 937 ("[C]ybersecurity is now mission critical to *every* publicly traded U.S. company."); *see also* Stevelman & Haan, *supra* note 15, at 184 (arguing a need for boards to actively "engage in information governance in the deliberative construction of the firm's internal data gathering, reporting, and communications architecture").

279. *See generally* Scott J. Shackelford, *Should Your Firm Invest in Cyber Risk Insurance*, 55 BUS. HORIZONS 349 (2012) (arguing that "firms must take a proactive stance toward managing cyber attacks—not only for their wellbeing, but also to enhance overall cybersecurity and help secure critical national infrastructure").

280. For instance, due to data's challenges with attribution and anonymity, flow, interdependencies and interconnectedness, among other issues, courts would find it more difficult to ascertain whether the board of directors' inattention and inaction resulted in harmful activities and corporate losses. Also, another consideration is that data's expansiveness and evolving nature tends to make the duty to monitor a more interpretive challenge.

281. *Assessment*, *supra* note 11, at 210–11 (criticizing Delaware's lack of "adequate guidance" about "when the duty to monitor should apply" and generally criticizing Delaware for construing the duty to monitor such that it is "undesirably difficult for plaintiffs to bring forward duty to monitor claims"); Pace & Trautman, *supra* note 11, at 887 (quoting Chancellor Allen's view that *Caremark* claims are "the most difficult" shareholder derivative suit claims).

282. *See generally* Thibault Schrepel, *Law + Technology*, J.L. & TECH. TEX. 1 (2023) (exploring how the combination of law and technology can be used for "the common good").

the dominant paradigm of commercial exchange in the near term.[283] This Article is sympathetic to the later viewpoint.[284] These observations naturally give rise to some important policy questions, including: What should be the role of the nature of the risk in the conceptualization of the duty to monitor?[285] This is somewhat ironic given that, risk by itself is a vast academic field with many interpretative methodologies, some of which (or at least exacerbate) many of the challenges that come with conceptualizing and interpreting risk-related decision making in practice.[286] For a variety of reasons, however, risk evaluation in corporate governance is highly complex with many possible frameworks.[287] Additionally, at a broader level, this Article urges greater technological realism in corporate governance and policy when pertaining to the duty of oversight. Specifically, what should the role of data and information technology be in interpreting and reforming the duty to monitor?[288]

Various reforms could enhance the duty of oversight's capacity to internalize the externalities of data risk.[289] These decidedly technologically driven proposals would help internalize negative externalities with data risk in two ways. First, it would be an information-forcing mechanism that would generate information about cybersecurity risks from particularly knowledgeable sources—cybersecurity executives or professionals that report to them. In so doing, this proposal sidesteps SEC regulatory proposals, which are limited in these that it is lack expertise with data risk and its knowledge would be external to the business assessing that risk. Second and more importantly, this requirement of disclosure and organizational expertise would function as a consideration-forcing mechanism that would compel businesses to identify and evaluate potential data risks harms and implication for potential corporate losses. Disclosure and organizational refinement may motivate redesign of the risk management procedures and strategies in a business.[290]

---

283. *See generally* David F. Larcker, Peter C. Reiss & Brian Tayan, *Critical Update Needed: Cybersecurity Expertise in the Boardroom*, ROCK CTR. FOR CORP. GOVERNANCE, Nov. 2017, at 1 ("Cybersecurity is an important risk facing companies and their shareholders".).

284. Importantly, however, the Article reveals how the duty of oversight falls short even when considering cybersecurity risk. Even within the traditional paradigm of the duty of oversight, efforts that directors must take to detect possible risk of harm, the doctrine's standard is strict and ignores that it may be more accurate to describe board of director liability in terms of a continuum of strictness of liability. Thus, even advocates for considering cybersecurity risks should favor correctives to impose only strict fault-based liability to better achieve the corporate fiduciary goal of preventing ignorance and passivity by the board of directors. Said another way, *Caremark* liability already holds that directors have a duty to implement and monitor compliance systems, which are applicable to a variety of risks, but this duty would be overbroad when considering cybersecurity risk for reasons and explanations provided in this Article.

285. One argument that can be pursued in a future law review article is that it can play a more contextual and granular role.

286. *See generally* Hofmann & Scordis, *supra* note 152 (exploring "how to price risk according to how risks interact within the firm").

287. OFF. OF THE COMPTROLLER OF THE CURRENCY, *supra* note 151, at 3–5.

288. One possibility is a more contextual and granular approach that incorporates a continuum to help internalize the unique informational properties of data. Within this proposal, courts could assess whether a business provided adequate disclosure of significant potential for data risk and implemented data risk assessment with the creation of a CIO or CDO position.

289. Wolff, *supra* note 197, at 3.

290. *See generally* Christoph Van der Elst, *The Risk Management Duties of the Board of Directors* (Fin. L. Inst., Working Paper No. 2013-02, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2267502.

The nature and source of potential reforms could range from a variety of perspectives—a cybersecurity information-sharing framework from a federal or risk management perspective, to a fiduciary duties framework from a corporate law framework. This Article assess changes to Delaware doctrine and corporate governance practices, and the related legal regimes that are implicated and how the proposals may be implemented in practice.[291] While these normative proposals provide a starting point of a framework for the examination of the effects of cybersecurity on the duty of oversight, future studies can investigate the characterization and ramifications of risk in a more in-depth manner.[292] These proposals are more than best practices for corporations—instead they serve as a call for statutory reform. Notably, these proposals dovetail with actual and proposed practices with financial risk,[293] such with the implications of the Sarbanes-Oxley Act of 2002 on fiduciary duty analysis, as well with environmental risk and corporate social responsibility measures.[294]

In recent years, scholars have fruitfully explored the importance of policy levers in supplementing and promoting new ways to assess liability in corporate fiduciary duties. Risks that can cause corporate harm are different based on the nature of the risk, and this Article questions the foundational belief that a strict standard, in and of itself, will achieve the normative objectives of the duty of oversight.

III. TOWARDS NEW INTERPRETATIONS FOR THE DUTY OF OVERSIGHT

While the primary aim of this Article is to cast doubt on the current interpretation of the duty of oversight as a fiduciary duty for directors in corporate law, its finding warrants normative evaluation as well.[295] Having established that the goal of fiduciary duties is to prevent bad deeds by deterring and punishing them, the Article assessed the duty of oversight to suggest that it is hard to define, and its broad application makes it difficult for it to offer much deterrence or punishment.[296] As suggested, the duty of oversight as a fiduciary duty, like all equitable doctrines, was established to avoid the formulaic application of strict rules, and replacing clear rules with vague boundaries effectively allowed it to set more slowly as courts kept stretching the mold to encompass new relationships.[297]

Courts shaped the duty of oversight by evaluating different situations in varying levels of risk to evaluate a potential failure to implement or oversee a robust compliance program.[298] The duty of oversight claims (also known as *Caremark* claims), fit under the duty

291. *See* discussion *supra* Part III.B.

292. *See* discussion *supra* Part III.C.

293. These proposals also dovetail with the Sarbanes-Oxley Act of 2002, which imposed internal controls and reporting obligations to mitigate financial reporting risk.

294. *See* Johnson & Sides, *supra* note 184, at 1153–55; THE SARBANES-OXLEY ACT OF 2002: A CULMINATION OF CORPORATE REFORM INITIATIVES BY THE BUSH ADMINISTRATION, THE SEC AND CONGRESS (2002); Gouldson & Bebbington, *supra* note 183, at 4; Branch & Merton, *supra* note 185, at 5; *see also* Lisa M. Fairfax, *The Sarbanes-Oxley Act as Confirmation of Recent Trends in Director and Officer Fiduciary Obligations*, 76 ST. JOHN'S L. REV. 953 (2002).

295. *See* discussion *infra* Part III.A.

296. *See* discussion *supra* Parts I.A.–.B.; *see also* discussion *infra* Part III.A.

297. *See* discussion *supra* Part I.B.

298. *See discussion supra* Part I.B.

of loyalty.[299] Since a bad faith refusal to oversee by a director was considered disloyal, they became known as "the most difficulty theory in corporat[e] law upon which a plaintiff might hope to win a judgment."[300] A string of successful recent duty of oversight cases (*Caremark* claims surviving a motion to dismiss), while noteworthy for raising compliance as a key corporate governance and suggesting *how* directors must act, did not provide insight on *why and when* directors must act.[301] Following the recent seemingly reinvigorated duty of oversight—cases where the once-insuperable *Caremark* pleading hurdle was overcome—"mission critical" situations have required directors to proactively oversee compliance.[302]

Following the new trends in duty of oversight liability, which have attracted the attention of scholars and practitioners alike, the preceding Part questioned the duty of oversight on many levels.[303] Indeed, as the duty of oversight has become reinvigorated, this Article has argued that scholarly commentary in response is moving the normative debate backwards—redirecting attention away from all of the problems associated with *oversight* with mechanisms for review of director activities in the area of risk management.[304] Scholarly response has moved away from inconsistencies with addressing judicial interference with internal business decisions,[305] away from the difficulties with the judgement of risk-taking activities,[306] and away from the promise with enhancing the quality of disclosure of risks,[307] among other considerations.[308] By contrast, the conversation has moved towards a focus on *duty* (as an aspect of the duty of oversight) in isolation, which provides a normative constraint on the attribution of accountability to directors, without assessment of the function and meaning of oversight.[309] In essence, the conversation has moved towards

299. A bad faith refusal to oversee by a director is considered disloyal. Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006).

300. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996).

301. *See e.g.*, Marchand v. Barnhill, 212 A.3d 805 (Del. 2019); Goodman v. Boeing Co., 127 Wn.2d 401 (Wash. 1995); Teamsters Local 443 Serv. & Ins. Plan v. Chou, No. 2019-016, 2020 WL 5028065 (Del. Ch. Aug. 24, 2020); Hughes v. Hu, No. 2019-0112, 2020 WL 1987029 (Del. Ch. Apr. 27, 2020); Clovis v. Clovis, 1969 OK 170 (Okla. 1969).

302. Pace & Trautman, *supra* note 11, at 896 (explaining that directors face greater liability for oversight, as "future *Caremark* liability will be centered on failure to provide board-level oversight of mission critical risks").

303. *See* discussion *supra* Part II.

304. *See* discussion *supra* Parts II.B.3, II.C.

305. Judicial intervention in internal business decisions is not a matter of simply overturning bad business choices. It is about ensuring that those making the decisions are acting in compliance their fiduciary duties, with due care, in good faith, and with a proper system of oversight in place to safeguard the company's interests and prevent harm.

306. As has been discussed, the duty of oversight is crucial for ensuring responsible governance and decision-making within corporations. The point raised here is that while courts generally defer to the expertise of directors, they also maintain a role in reviewing actions that may be unlawful, arbitrary, capricious, and harmful. The challenge lies in balancing these competing values to promote accountability while avoiding undue interference with legitimate risk-taking activities that are essential for progress and innovation.

307. Ultimately, the interplay between judicial oversight and enhancing risk disclosure is a continuous process of evolution and adaptation, aiming to strike the optimal balance between legal compliance and the provision of high-quality, actionable information for investors.

308. Hurt, *supra* note 28.

309. It should be emphasized that scholars and courts should more squarely address the issue of what oversight refers to and should mean in corporate governance. This would entail explaining what the duty of oversight should specifically be when a new circumstance applies and defining what the term "oversight" means.

questioning all of kinds of director decisions, rather than assessing the *overseeing* itself.[310] Significant doctrinal hurdles remain. Even if duty of oversight claims survive a motion to dismiss, these hurdles should be assessed or else there will be more lawsuits every time corporations experience disruptions seeking to attribute liability to directors.[311]

Turning to theoretical insights and normative analysis, this Part assesses what should be done about the duty of oversight. In particular, the unique role and prevalence of cybersecurity as a growing central corporate concern warrants some deviation from traditional interpretations.[312] The current interpretation of the duty of oversight raises the question of how exactly should oversight of risk be enforced in corporations. Constructing potential answers gives more reason to doubt that the current characterization of the duty of oversight is appropriate.[313]

A. Theoretical Insights and Normative Analysis

In addition to pragmatically reforming corporate law's treatment of the duty of oversight, the proposal to apply cybersecurity insights in director duties also holds implications for corporate governance, law, and policy. Observers of corporate governance will recognize that this proposal represents a subtle but significant variation of scholars' information governance proposal that "justifi[ed] the ongoing legal shift in favor of enhanced *Caremark* duties by recognizing the creation of and attendance to informational architecture as a core role of the board."[314]

In theory, cybersecurity practices that support (or fail to support) directors' collection and analysis of information germane to remediating problems is an emergent fiduciary duty, given that nearly every facet of corporate affairs are becoming controlled by software.[315] As we have seen, however, the duty of oversight has not been effective in inducing directors to adopt effective compliance functions or assert truly effective oversight over compliance functions since directors have had discretion over a corporation's compliance system and oversight nature.[316] Nonetheless, this proposal to apply cybersecurity lessons in duty of oversight analysis captures much of the insight of the difficulties with oversight risk.[317] Recall risk assessment has shifted liability to directors when there is corporate harm, such as when a crisis or disruption results in questioning directors' decision-making with having in place an appropriate system that oversees compliance issues.[318] In this situation, evaluation of directors' conscious disregard of their duties is impossible because it necessitates review in hindsight of the particularized facts that the directors should have

310. *See* discussion *supra* Part II.A.1.

311. *See* Trautman, *supra* note 11, at 275–76 (highlighting famous cases involving "[s]urvival threatening disasters").

312. *See* discussion *supra* Part I.A.2.

313. An aim of constructing answers or providing proposals is to give guidance to states about how they may or may not follow Delaware law. An aim of these prescriptions is for states to make considerations as they evaluate their potential adoption.

314. Stevelman & Haan, *supra* note 15, at 268.

315. *Id.* at 196–97, 270.

316. Jennifer Arlen, *How Directors' Oversight Duties and Liability Under Caremark Are Evolving*, OXFORD BUS. L. BLOG (Mar. 2, 2023), [https://perma.cc/Y3BW-RBVG].

317. *See* discussion *supra* Part II.B.

318. OECD, *supra* note 105, at 7; Orbach, *supra* note 11, at 15.

known; it is hard to know whether they could have done anything to stop the result. Similarly, such hindsight assessment is critical to the evaluation of classic situations where corporate harm results based on situations with some element of risk—whether cybersecurity, economic, environmental, natural disaster, pandemic, political, tort, weather, or wildfire. While technically one could still subject the corporate harm to the personal liability of the directors' conscious disregard with failure to implement a monitoring and reporting system, equity weights against doing so. Thus, in both the context of risk assessment and directors' mental state and awareness, an assessment in hindsight is justified only when there is bad faith.

When a director fails to act, the key difference between the analysis under the duty of care and the duty of loyalty rests upon the extent of the omission. Duty of oversight implicates both duty of care and duty of loyalty (as noted by Delaware courts in *Caremark* and *Stone*),[319] and as such, duty of oversight claims do not fit comfortably in the duty of loyalty analysis.[320] Under the duty of care, the failure to act applies when there is negligence and gross negligence, but when the omission is so significant that it constitutes bad faith then there is a breach of the duty of loyalty under duty of oversight.[321] Accordingly, a director is liable for a duty of oversight claim based on the extent of bad faith,[322] which in corporate law is a legal term that refers to a defendant's knowledge or intent in committing wrongdoing.[323] In many ways, a duty of oversight claim looks like a duty of care claim but with a lighter degree of bad faith.[324] Specifically, a director is liable for a breach of the duty of oversight when there is a failure to make a good faith effort to exercise the duty of care.[325] Considering the extent to which the directors' failure to act is either intentional or unintentional seems more logical towards classifying the behavior into either duty of loyalty and duty of care respectively.

The nature of classifying a failure to act as intentional or unintentional (along with the associated challenging bad faith assessment) has likely contributed to the duty of oversight

319. However, it should be noted that *Stone* makes clear that liability under a duty of oversight theory requires a breach of the duty of loyalty, specifically through bad faith conduct. Stone v. Ritter, 911 A.2d 362, 369 (Del. 2006) (recognizing that failure to oversee claims survive exculpation only if they are grounded in loyalty via bad faith).

320. Weitzel, *supra* note 61, at 354 (stating that "*Caremark* claims do not fit comfortably into the duty of loyalty because a failure to act would typically fall under the duty of care, which covers negligence and gross negligence").

321. *Bad Faith*, BLACK'S LAW DICTIONARY (6th ed. 1990) ("[I]mpl[ying] the conscious doing of a wrong because of dishonest purpose or moral obliquity; it is different from the negative idea of negligence in that it contemplates a state of mind affirmatively operating with furtive design or ill will.").

322. To be more specific, the conscious disregard of known risks is the operative standard under duty of oversight (or *Caremark*) liability.

323. Meghan Roll, *The Delaware Supreme Court Does Not Scream for Ice Cream: Director Oversight Liability Following* Marchand v. Barnhill, 57 SAN DIEGO L. REV. 809, 817 (2020) (noting that *Marchand v. Barnhill* was the first *Caremark* claim to proceed beyond the pleading stage at the Delaware Supreme Court); Clovis v. Clovis, 1969 OK 170 (Okla. 1969) (ruling for plaintiffs); *see* Shapira, *supra* note 11, at 1862–66 (explaining "bad faith" and pointing to other recent successful *Caremark* claims and arguing these claims will succeed more frequently).

324. To reiterate, the conscious disregard of known risks is the operative standard under duty of oversight (or *Caremark*) liability.

325. Marchand v. Barnhill, 212 A.3d 805, 824 (Del. 2019) ("If *Caremark* means anything, it is that a corporate board must make a good faith effort to exercise its duty of care. A failure to make that effort constitutes a breach of the duty of loyalty.").

claims traditionally failing and being what has been considered the most difficult theory in corporate law for a plaintiff. In essence, the risk assessment of cybersecurity compliance offers a case study and motivation for shedding light on the theoretical implications and normative analysis of bad faith in duty of oversight analysis.[326] Given that data has become a dominant part of a modern corporation's operations, scholars and courts should be emboldened to consider shifting of mission critical risks as being evaluated under a duty of care analysis or as being attributed to officers.[327]

The radical transformation of overseeing compliance under a duty of care analysis or attribution of liability to officers would mitigate the complexity of assessment with bad faith and bad faith under the duty of oversight.[328] The drastic nature of cybersecurity breaches—which completely impacts or harms a corporation's operations—motivates this proposed shift away from assessing an essential part of a corporation's operations towards assessing negligence with putting in place systems that would need compliance of a risk or shifting the liability to some other aspect of a corporation (such as with officers or through a committee, such as an audit committee or a risk committee).[329] While cybersecurity risk assessment offers a practical proposal to enhance treatment of cybersecurity as a risk that causes disruption, it also sheds light on the broader relationship of the fiduciary law and the duty of oversight.[330] As noted above, this Article has criticized the duty of oversight by highlighting the fundamental challenges with assessing risks that cause corporate harm and are based on bad faith.[331] Given those challenges and common justifications for duty of care analysis[332]—such as exercising an informed business judgment as a rebuttable presumption in duty of care analysis of shifting liability to some other area of corporate law—then bad faith analysis loses significant force.

B. Prescriptions

The importance and prevalence of cybersecurity risk to corporations has raised important theoretical implications for the duty of oversight and the standard for its assessment.[333] But if cybersecurity is a mission critical risk, as Professors Pace and Trautman claim, then what happens and what should be the liability every time there is a cyberattack causing corporate harm?[334] The idea that the law would hold directors personally liable for

326. *See* discussion *supra* Part II.B.

327. *See* discussion *supra* Part III.C.

328. *See* discussion *infra* Part III.C.

329. *See* discussion *supra* Part II.B.

330. *See* discussion *supra* Part II.B.

331. *See* discussion *supra* Parts I.B.–II.A.

332. Relatedly, it is helpful to address the implications of Delaware General Corporate Law (DGCL) § 102(b)(7), which eliminates personal liability for breaches of the duty of care. That provision is one reason Delaware courts have cabined oversight liability within the duty of loyalty—specifically through bad faith. A shift toward a duty of care framing could inadvertently eliminate director liability for oversight failures entirely. The context and point here is that courts might consider evaluating failures related to cybersecurity oversight under a duty of care framework rather than through the current loyalty-based oversight doctrine. This proposal is described more in Part III.B.2.

333. *See* discussion *supra* Parts I.A.2., III.A.

334. Pace & Trautman, *supra* note 11, at 896 ("[C]ybersecurity has become mission critical for every large company.").

failure to monitor an exogenous and disruptive risk without the need for fundamental restructuring of fiduciary duties looks even more far-fetched. If the criteria for assessing whether the duty of oversight was met when there is a data breach and not in place any reporting an information system or controls, then the duty becomes nothing more than the duty of care (a topic that this Part turns to as a potential proposal).[335] If the proposal to monitor a corporation's cybersecurity efforts were defensible in one time period and indefensible in another time period, then would it do the same for all other types of risks? Should, or can, the duty of oversight deter bad conduct by directors in corporations? And how exactly would the oversight of cybersecurity risk, or any type of risk for that matter, be enforced? Professors Pace and Trautman are strikingly unclear on these questions, and other scholars have yet to address this question. Reconstructing from their article potential answers gives still more reasons to doubt that the current fiduciary characterization of the duty of oversight is appropriate and other proposals are necessary as adequate responses.

Turning to prescriptions, this ensuing Part questions the current interpretation of the duty of oversight and its locus in corporate governance. It provides proposals and recommendations for a shifting the duty of oversight. It argues, not surprisingly, that the appropriateness of the duty of oversight should depend on risk.

1. Situating the Duty of Oversight Under the Duty of Care

If corporate law wants more accountability for corporate decision making, but not under the duty of oversight (that is part of duty of loyalty analysis), then the obligation to come forward and to suggest appropriate standards of conduct is the duty of care. Revitalization and clarification of the duty of care may help corporate boards avoid the types of corporate governance failures that led to catastrophic losses by major financial institutions (such as AIG, Bear Stearns, Citigroup, Goldman Sachs, and Lehman Brothers).[336] It is well settled that directors owe a duty of care to the corporation, and shifting the duty of oversight to be under the duty of care analysis would address the inadequacies of oversight of corporate compliance with risk oversight.[337] The list of things to be overseen by directors is extensive, almost limitless, when considering various risks faced by corporations.[338] That is why directors deserve and receive protection under the business judgement rule, and in doing so, it becomes tougher to avoid when considering the need of appropriate conduct by directors.[339]

Thus, as this Part builds upon the previous analysis, it recommends a shift in the doctrine within director obligations by subsuming the duty of oversight into duty of care analysis. This Part frames this proposal as a call for legislative or doctrinal reform rather than

335. *See* discussion *infra* Part III.B.1.

336. *Duty*, *supra* note 11, at 718; Hurt, *supra* note 28, at 253–57, 280–84.

337. *See* discussion *supra* Parts II.A.1–.2.

338. Orbach, *supra* note 11, at 15 (stating that "the oversight duty applies to only legal risks" and that "directors cannot be held accountable for corporate losses arising from failures to monitor climate change risks, wildfire risks, and cybersecurity threats").

339. Philip C. Sorensen, *Discretion and Its Limits—An Analytical Framework for Understanding and Applying the Duty of Care to Corporate Directors (And Others)*, 66 WASH. U. L.Q. 553, 554 (1988) (noting, however, that the use of the business judgment rule to avoid responsibility "grows tiresome," as the rule was not intended to protect directors in the face of blatant, ongoing corporate malfeasance).

a reinterpretation of existing case law.[340] To differentiate this proposal from the latter one (shifting the duty of oversight to officers), and to use language consistent with fiduciary duties in corporate law, it proposes that oversight as a failure to act be appropriately assessed as a failure to act under the duty of care as negligent or gross negligent behavior.[341] Working within this framework, this Part proposes that courts apply duty of care analysis of negligence and gross negligence in assessing oversight of risks, such as cybersecurity, which would seem more logical to include as breaches of duty of care.[342]

A general requirement of assessing under the duty of care would eliminate the need for courts to make difficult decisions as to whether a failure to implement a monitoring and reporting system was bad faith or not and was unintentional or not, as would be under duty of loyalty analysis.[343] Furthermore, it would encourage a greater exercise of informed business judgement by directors in paying attention to implementing a monitoring and reporting system and to risk assessment in general. As such, it has the most potential to shift norms within corporate governance towards directors' embracing oversight of risks in a good faith and honest belief that actions taken were in the best interests of the corporation.[344]

A duty of care analysis that comprises a duty of oversight as well would have the potential to change how corporations do business. It could also build more trust between shareholders and directors in corporations and in our society in ways that existing models and reformations of corporate governance have failed to achieve. It is worth nothing, as this Article concludes, this prescription does not by itself solve all the problems associated with overseeing of risk in corporate law. But the duty of care must play a special role in these efforts for two important reasons. First, the duty of care is a tool and standard that corporate governance has been using for decades to deal with such problems. Issues of assessment of judgment have typically been thought of in terms of care, and this model has done a good job overall, though like many academic models it has succeeded better at offering meaningful reform. Second, reformation along these lines is very much feasible and should stand a good chance of success.

This Article argues that a duty of oversight framed along the lines of duty of care offers a way of reform for the duty of overseeing risk as well as a broader mode of corporate governance. A duty of oversight analysis in the duty of care would be a revolution in corporate law, but it would fit alongside other criteria of duty of care. A sea of change is

340. It should be noted that this is a provocative and ambitious proposal, and that the goal is to reframe oversight liability as a form of duty of care liability. In so doing, it should be acknowledged that the extent to which this proposal departs from current Delaware doctrine, especially considering *Stone v. Ritter* and the limitations imposed by the DGCL § 102(b)(7). Delaware law now requires *Caremark* claims to be grounded in duty of loyalty because directors are exculpated from liability for breaches of the duty of care—even gross negligence.

341. *See* Melvin A. Eisenberg, *The Duty of Care of Corporate Directors and Officers*, 51 U. PITT. L. REV. 945, 951–52 (1990) (describing the duty to monitor as a duty of care).

342. *Cf. In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 970–71 (Del. Ch. 1996) (conceiving, before *Stone v. Ritter*, of duty to monitor violations as related to the duty of care).

343. William F. Kennedy, *Standard of Responsibility of Directors*, 52 GEO. WASH. L. REV. 624, 648 (1983) (proposing to "dispel semantic confusion" by re-defining the duty of care to include duties of "attention," "inquiry in specified cases," and "to be informed when acting on a specific matter").

344. This proposal also has some limitations with expanding the scope of the duty of care to include an exception with the business judgment rule.

exactly what is needed to deal with the duty of oversight and with the growing consensus that cybersecurity is a central concern of corporate law.

2. Shifting the Duty of Oversight to Officers

Building on earlier analysis, this Part argues that the duty of oversight should be shifted to another aspect of the corporation, thereby resulting in a more collective approach to assessment of liability for implementing a monitoring and reporting system. The recalibration of oversight liability through a more collective approach within a business sheds more light on the broader relationship between attribution of liability and risk management, which has become a more prominent part of corporate governance. This is a compelling and timely proposal, particularly in light of recent Delaware case law recognizing that officers, similar to directors, owe fiduciary duties that may include oversight responsibilities.[345] Recently, the Delaware Court of Chancery held that the duty of oversight also applies to corporate officers *In re McDonald's Corp. Stockholder Derivative Litigation*, which reasoned that officers are the ones who are responsible for running the business of the corporation, for important day-to-day operational decisions, and supervising employees such that officers may be more informed than directors.[346] The elevation of the role of officers in overseeing risk,[347] especially in areas such as cybersecurity where they often have superior access to operational details, makes practical sense.

Liability for the duty of oversight has conventionally been attributed to the board of directors in unitary fashion.[348] At least in a formal sense, liability for omissions could be attributed to other actors in a business, and as such, risk management can recalibrate attribution of liability. This calibration can happen in two possible ways: (1) first, raising the importance of officers and correspondingly introducing a horizontal fiduciary duty, which is a novel legal theory that has been introduced in corporate law scholarship, or (2) second, strengthening the role of the stand-alone risk committee.[349] The horizontal fiduciary duty, which refers to a fiduciary duty owed between the board of directors and officers vis-à-vis

345. *In re* McDonald's Corp. S'holder Derivative Litig., No. 2021-0324, 2023 Del. Ch. LEXIS 23, at *4 (Del. Ch. Jan. 25, 2023) (holding that the duty of oversight also applies to corporate officers).

346. Doug Raymond, Todd Schiltz & Christina Ledondici, *Recent McDonald's Case is a Game Changers for Duty of Oversight*, DIRS. & BDS. (Mar. 7, 2023), [https://perma.cc/F3EK-Y6W4].

347. As a practical matter, many officers assume that they have an obligation under the duty of oversight akin to that owed by directors under the *Caremark* case. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996). It should be noted that some scholars and practitioners have argued that officers should or do owe a duty of oversight. In re *McDonald's Corp. Stockholder Derivative Litig.* is a case that marks for the first time that this duty was explicitly acknowledged by a Delaware court. *McDonald's Corp. S'holder Derivative Litig.*, 2023 Del. Ch. LEXIS 23, at *349–50. This Part of the Article proposes shifting of the duty of oversight to officers, and while elevating the role of officers in monitoring risk—especially in areas like cybersecurity where they often have superior access to operational detail—may make sense, there are a number of questions that need to be assessed by courts related to officer liability, and these include: (1) how does *Caremark* doctrine apply to officers, who play a different role in corporate governance than directors do?; (2) why can directors not be trusted to decide whether to sue officers, for whom *Caremark* analysis should apply differently?; and (3) why would Delaware corporation law's fiduciary duties apply to officers rather than the agency law fiduciary duties of the state where they are employed?

348. *See supra* note 269 and accompanying text.

349. *See* discussion *supra* Part II.B.4.

one another, should become more prominent.[350] The horizontal fiduciary duty would complement the corporate duty owed by officers and enable the board of directors to exonerate themselves for officers' failure in diligence with risks and threats,[351] while improving information sharing between the board of directors and officers.[352]

As a result, there would be a redistribution of liability and strengthening of the importance of information flows between the board of directors and officers.[353] Additionally, a transition to a more collective approach, rather than a focus on unitary individual liability,[354] could also arise from a standalone risk committee, which could focus on compliance and risk management to articulate and establish the corporation's risk tolerance and risk appetite.[355] Foremost, raising the importance and liability of officers or a risk committee would highlight the interdependencies and interconnectedness, such with information technology driven monitoring and reporting systems in the cybersecurity context. As a result, businesses would work more closely with management to "promote and actively cultivate a corporate culture . . . that understands and implements . . . risk management."[356] For example, the resulting focus on a standalone risk committee for monitoring and assessing cybersecurity risk would avoid the challenges of identifying a cybersecurity expert on the board or to search for one and the information costs associated with gathering details to make risk mitigation decisions.[357] While technically the board of directors would still be liable for inaction and inattention to risks, such as cybersecurity risk, a more collective approach within businesses would increase officer liability and lead to an increased importance of the risk committee.[358]

---

350. Eckstein & Parchomovsky, *supra* note 270, at 808–11, 841–47 (2019) (defining horizontal fiduciary duties).

351. It should be noted that fiduciary duties typically run vertically, wherein officers and directors owe duties to the corporation and its shareholders but not to one another. A horizontal fiduciary duty refers to the idea that directors and officers of a corporation should owe fiduciary duties (such as the duty of care and duty of loyalty) to each other, in addition to the duties they already owe to the corporation and its shareholders. *Id.* at 810. This concept is not currently a widely recognized or established part of corporate law, but instead is, a legal concept introduced by legal scholars to encourage better accountability, collaboration and overall performance of the board of directors.

352. Eckstein & Parchomovsky, *supra* note 270, at 810 (arguing that horizontal fiduciary duties would result in "improved information-sharing and decision making"); Johnson & Millon, *supra* note 105, at 2–3.

353. *See supra* note 272 and accompanying text.

354. It should be noted that while courts may recognize that officers can be held liable for oversight failures, directors likely cannot fully insulate themselves by pointing to officer misconduct. Under *Caremark*, directors retain a non-delegable duty to make a good faith effort to implement and monitor compliance systems. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996).

355. *See generally* Gutterman, *supra* note 273 (describing how to structure a compliance and risk management committee).

356. Lipton, Niles & Miller, *supra* note 63 (advocating for this integrated approach to oversight).

357. Edwards, *supra* note 275, at 1102–07 (describing the benefits for boards of cybersecurity experts, including reduced information costs).

358. A greater importance should be placed on officers to work with a risk committee in evaluation of oversight liability. First, it helps focus accountability on officers and a specialized committee that would have the most relevant expertise for risk analysis. Second and relatedly, it mitigates liability for directors that is challenging to assess for corporate losses, while allocating responsibility in a manner that would make it easier to assess liability. By aligning liability with expertise, there would be a reduction in uncertainty for courts in assessing challenging oversight standards of review. *See* OECD, *supra* note 105, at 7 (stating that "[c]orporate governance should therefore ensure that risks are understood, managed, and, when appropriate, communicated"); Gutterman, *supra* note 273, at 19; Lipton, Niles & Miller, *supra* note 63.

C. Future Directions

Broadening perspective, this Article has suggested that there should be greater attention to shaping of the duty of oversight doctrine. As noted, traditional views of the duty of oversight have focused on whether there are adequate information systems or controls,[359] oversight of corporate operations,[360] and "reasonable board-level system[s] of . . . reporting" of operations.[361] These actions are valuable yet challenging to assess in determining whether directors have adequately performed their duty of oversight duties. As this Article has shown, cybersecurity also significantly challenges the assessment of the board of directors' liability with the duty of oversight.[362] While some scholars have richly pursued normative assessments to the duty of oversight, more attention to its implication and policy considerations is warranted.

Along these lines, the theoretical contributions of this Article define a framework for further examination of the effects of cybersecurity on the duty of oversight.[363] At a broader level, this Article has urged greater attention to cybersecurity in corporate fiduciary obligations and has relied on theory and normative assessments to argue for considering new prescriptions.[364] These are conceptualizations that can be evaluated and tested as more cyberattacks and data risk result in losses to corporations. As such, this Article calls for further examination of these principles across a diverse set of corporations as future research studies.

While it is important to understand the ways in which cybersecurity impacts the duty to monitor, it also important to contextualize these effects within the broader risks that shape corporate fiduciary obligations. Directors operate among dynamic and constantly evolving external risk factors that are subject to a myriad of forces beyond cybersecurity risk.[365] There are a host of other non-cybersecurity risks that also could influence the interpretation of the duty of oversight. The long-standing scholarly debate over whether directors should be liable for failing to oversee and respond to harmful activities may encounter other proposals based on non-cybersecurity risk to reinterpret the duty of oversight. Subsequent work should explore these non-cybersecurity risks, such as currently newsworthy pandemic risks and financial shock risks, and verify whether the duty of oversight should require a contextual and granular approach. A classification of risk represents an innovative means to analyze the provision of oversight and how courts should differentiate

359. Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006).

360. *Id.*

361. SPAMANN, HIRST & RAUTERBERG, *supra* note 38, at 45 (quoting Marchand v. Barnhill, 212 A.3d 805, 821 (Del. 2019)).

362. *See* discussion *supra* Part II.B.2.

363. *See* discussion *supra* Part II.A.2 (referencing the emergence of cybersecurity as a central concern); *see also* discussion *supra* Part II.B.2 (referencing cybersecurity's implications for corporate governance).

364. *See* discussion *supra* Part III.A (referencing the theoretical insights into a new duty of oversight); *see also supra* Part III.B (referencing policy prescriptions).

365. Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. COMPUT. & INFO. L. 313, 314–17 (2011) (providing a structure for oversight that includes IT).

between the nature of the risk before determining liability.[366] To understand the broad ramifications that risk classification confers over the duty of oversight, one must further understand the nature of risk. For a deeper analysis in a future study, risk can be considered as "an uncertainty that matters" and with "the potential to affect outcomes."[367] Since various definitions abound for risk in academic literature, a future study can characterize risk so as to encompass, in some part or in full, "*probabilistically measurable uncertainty*,"[368] "ontological uncertainty,"[369] or "decisions with incomplete data and uncertain knowledge."[370]

Notably such risk classification and risk factors tend to have some properties akin to data pertaining to cybersecurity, particularly such as interdependencies and interconnectedness. Similarly, assessment of such properties could raise normative concerns over harms to businesses in the absence of the board of director actions. A future study could compare the inherent characteristics and effects of non-data risks with data risks to assess how the duty to oversight should treat them similarly or differently. Importantly, this assessment would have a real effect on the board of directors' behavior towards risk management and managerial oversight.

CONCLUSION

Scholars have debated whether the director duty of oversight in corporate law should hold directors liable for events that caused corporate harm. Corporate law has imposed personal liability on directors for failure to adopt effective internal compliance functions, yet few claims have survived the pleading hurdles. A string of recent successful duty of oversight claims survived a motion to dismiss and signaled enhanced directors' oversight duties. A changing view of the duty of oversight—what was once considered the most difficult corporate law theory a plaintiff may hope to win a judgment on—raises new questions: Is a stricter duty of oversight era a coincidence or based on context? If there is a resurgence in directors' oversight duties, then how should the duty of oversight be construed? What will be the effects and implications to directors and for corporate governance? And should the duty of oversight distinguish claims based on wrongful conduct and on perceived excessive risk taking?

This Article has shown new light on the longstanding debate in corporate law over the interpretation and scope of the fiduciary duty of directors' conduct that results in corporate harm. An influential body of theory holds that directors' decisions should be insulated from shareholder complaints and judicial hindsight bias. Conversely, recent scholarship and recent cases have suggested that directors now face a threat of duty of oversight liability if they ignore "mission critical" risks. A reinvigorated duty of oversight has the potential to

366. It should be noted that the concept of risk can be characterized as involving uncertainty about the effects and implications of an activity with respect to something of value and embodies the potential for undesirable consequences.

367. Filipe Lemos, *On Risk–Building a Definition*, 1 (Mar. 2, 2016), https://ssrn.com/abstract=2734050.

368. Tobias Mahler, *Defining Legal Risk*, *in* COMMERCIAL CONTRACTING FOR STRATEGIC ADVANTAGE POTENTIALS AND PROSPECTS: CONFERENCE PROCEEDINGS 1, 8 (2007).

369. Lemos, *supra* note 367, at 4 (defining "ontological uncertainty" as "[u]nknowable unknowns," that is, the kind of uncertainty that, at a given time, cannot be remediated through any process or insight).

370. MICHAEL MASSIE & A. TERRY MORRIS, RISK ACCEPTANCE PERSONALITY PARADIGM: HOW WE VIEW WHAT WE DON'T KNOW WE DON'T KNOW 2 (2011).

change what duties directors owe to a corporation and distinguishing among the type of risk that led to corporate harm seems inconsistent with existing duties and limitations. This Article has introduced a novel distinction to argue against the reinvigoration of the duty of oversight. It has distinguished directors' duty of oversight for its failure to act upon risk that causes corporate harm would be unmanageable and unwise. If this Article's main arguments have been persuasive, the burden is on the supporters of the duty of oversight to clarify how it can be reconciled with cybersecurity that has become of prime importance in the modern corporation.

More substantially, this Article highlights the importance of cybersecurity as a case study and as central corporate concern in effectively assessing directors' decision making in hindsight. Turning to normative considerations and prescriptions, this Article has argued the current interpretation of the duty of oversight is ill suited, has illustrated the need to revitalize duty of care analysis, and has proposed shifting the duty of oversight within corporate governance to ameliorate its deficiencies.