Georgia State University Law Review

Volume 35
Issue 3 *Spring 2019*

Article 3

4-1-2019

Cybersecurity Oversight Liability

Benjamin P. Edwards
University of Nevada, Las Vegas William S. Boyd School of Law, benjamin.edwards@unlv.edu

CYBERSECURITY OVERSIGHT LIABILITY

Benjamin P. Edwards*

ABSTRACT

A changing cybersecurity environment now poses a significant corporate-governance challenge. Although some cybersecurity data breaches may be inevitable, courts now increasingly consider when a corporation's officers and directors may be held liable on theories that they acted in bad faith and failed to adequately oversee the corporation's affairs. This short essay reviews recent derivative decisions and encourages corporate boards to recognize that in an environment filled with increasing threats, a reasonable response will require devoting real resources and attention to cybersecurity issues.

TABLE OF CONTENTS

* Associate Professor of Law, University of Nevada, Las Vegas William S. Boyd School of Law. J.D., Columbia Law School. Thank you to Elizabeth Manriquez and the Wiener-Rogers Law Library at UNLV, who supported this project with outstanding research.

INTRODUCTION

Every year, data breaches and cybersecurity failures cause significant damage to American consumers and corporations.[1] Consider the harm from data breaches at Equifax, Inc. (Equifax) alone. In 2017, Equifax "announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers."[2] It also revealed that "credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed."[3] Putting the harm to consumers aside, the data breach did enormous damage to Equifax's shareholders, erasing $6 billion in market capitalization.[4] As with many data breaches, the revelation also triggered additional significant liabilities, including shareholder derivative actions.[5]

Notably, Equifax has not been the only company to have its valuation drop because of cybersecurity failures.[6] After Yahoo's

1. *See* IDENTITY THEFT RESOURCE CTR., 2017 ANNUAL DATA BREACH YEAR-END REVIEW (2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf [https://perma.cc/PB2Y-DF5E] ("The number of U.S. data breach incidents tracked in 2017 hit a new record high of 1,579 breaches.").

2. Press Release, Equifax, Equifax Announces Cybersecurity Incident Involving Consumer Information (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 [https://perma.cc/PB2Y-DF5E].

3. *Id.*

4. AnnaMaria Andriotis, Michael Rapoport & Robert McMillan, *'We've Been Breached': Inside the Equifax Hack*, WALL ST. J. (Sept. 18, 2017, 8:04 AM), https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318 [https://perma.cc/AD6C-7GNQ] ("[I]nvestors have shrunk Equifax's stock-market value by about $6 billion, or more than a third, in the past [ten] days.").

5. Meena Yoo, *Director Liability in a Data Breach Era*, FORDHAM J. CORP. & FIN. L. (Nov. 6, 2017), https://news.law.fordham.edu/jcfl/2017/11/06/director-liability-in-a-data-breach-era/ [https://perma.cc/NLM7-BBM8] ("Equifax faces an FTC investigation, congressional hearings, class actions[,] and derivative suits. However, its executives will likely escape liability.").

6. *See* Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1285 (2017) ("Yahoo faces the loss of $350 million from the proposed renegotiated Verizon acquisition. Under the renegotiated deal, Yahoo shareholders stand to lose hundreds of millions of dollars of value due to management's cybersecurity failures, which may become the source of a shareholder derivative cause of action.").

record-setting hack in 2014, Verizon renegotiated its asset purchase deal to trim the price paid by $350 million.[7] In practical effect, Yahoo's shareholders suffered a $350 million loss because the reduced purchase price meant that each shareholder received less than he or she would have had the data breaches not occurred or been handled more effectively.[8]

Shareholder derivative litigation in the wake of a significant data breach or cybersecurity incident has now become a predictable risk for corporate directors.[9] In recent years, shareholders have filed lawsuits in the aftermath of data breaches at Yahoo, Target, Home Depot, Wyndham, Wendy's, and others.[10] Although courts have halted many suits on procedural grounds, past suits, the Yahoo settlement, and increased awareness around cybersecurity issues now place corporate directors on notice that cybersecurity concerns must be taken seriously.[11]

This essay contributes to the conversation around cybersecurity liability in shareholder derivative actions.[12] It assesses current shareholder efforts to hold corporate officers and directors

7. *Id.*

8. *Id.*

9. *See* Kevin M. LaCroix, *Target Corporation Cybersecurity-Related Derivative Litigation Dismissed*, D&O DIARY (July 9, 2016), https://www.dandodiary.com/2016/07/articles/cyber-liability/target-corporation-cybersecurity-related-derivative-litigation-dismissed/ [https://perma.cc/A36F-PZDE] ("For some time now, many commentators, including me, have been predicting that cybersecurity-related litigation could become an important part of the D&O litigation environment.").

10. *See Cyber Breaches: Lessons Learned from Shareholder Derivative and Securities Fraud Litigation*, CLEARY GOTTLIEB 2–6 (May 1, 2018), https://www.clearygottlieb.com/-/media/files/alert-memos-2018/cyber-breaches-lessons-learned-from-shareholder-derivative-and-securities-fraud-litigation-pdf.pdf [https://perma.cc/XWC3-ZANG] [hereinafter *Cyber Beaches*].

11. *See id.* at 1 ("[A]s cybersecurity issues become more ubiquitous, directors and officers will be increasingly on notice of data breach risks, and plaintiffs will more easily be able to argue that directors and officers should have been aware of the company's susceptibility to cyberattack and should have taken efforts to remedy the company's vulnerabilities.").

12. Although discussions about how to appropriately shape derivative liability for cybersecurity failures remains at an early stage, some commentators now view a corporate board being held liable for a cybersecurity failure as inevitable. *See* Benjamin Dynkin & Barry Dynkin, *Derivative Liability in the Wake of a Cyber Attack*, 28 ALB. L.J. SCI. & TECH. 23, 44 (2018) ("With the ever-rising number of data breaches, it is inevitable that a case will arise in which the [b]usiness [j]udgment [r]ule and the [d]emand requirement will not impede a claim, and [d]irectors will be held liable for insufficient or improper action or inaction.").

accountable for cybersecurity failures under state corporate law and how increasingly pervasive and salient cybersecurity risk may alter judicial thinking. Part II briefly reviews the framework for oversight liability in shareholder derivative cases.[13] Part III examines recent shareholder derivative actions arising out of cybersecurity failures and data breaches.[14] Part IV concludes by encouraging corporate boards to devote additional resources to cybersecurity as risks increase.[15]

I. The Oversight Liability Framework

Directors concerned about expanding shareholder liability for cybersecurity breaches may take some refuge behind the procedural, prudential, and substantive barriers insulating them from liability.[16] This Part briefly overviews the demand requirement, the business judgment rule, and the substantive standards commonly applied in shareholder derivative cases alleging some form of corporate oversight failure.

A. General Procedural Barriers

At the outset, a shareholder seeking to assert the corporation's rights in a derivative action must comply with general standing

13. *See infra* Part II.

14. *See infra* Part III.

15. *See infra* Part IV.

16. JEFFREY L. KWALL, THE FEDERAL INCOME TAXATION OF CORPORATIONS, PARTNERSHIPS, LIMITED LIABILITY COMPANIES, AND THEIR OWNERS 4 (4th ed. 2019). Although a cybersecurity breach may lead plaintiffs to file securities fraud actions as well, this article confines its focus to shareholder derivative actions alleging a breach of the duty of loyalty under state corporate law. For more information on the new event-driven, securities-litigation phenomenon, see John C. Coffee Jr., *The Changing Character of Securities Litigation in 2019: Why It's Time to Draw Some Distinctions*, CLS BLUE SKY BLOG (Jan. 22, 2019), http://clsbluesky.law.columbia.edu/2019/01/22/the-changing-character-of-securities-litigation-in-2019-why-its-time-to-draw-some-distinctions/ [https://perma.cc/M2RP-DLXV]. ("[T]he contemporary securities litigation playing field is dominated by three very different categories of cases: (1) traditional securities cases, which have grown both in number and even more in size; (2) merger objection cases, which characteristically have low merit but nonetheless give plaintiffs some leverage because of the defendants' fear of any disruption in the timing of their merger; and (3) event-driven cases, where the legal standards are not yet clear because few of these cases have yet produced an appellate decision.").

requirements, including continuous share ownership and the demand requirement.[17] Even in instances where a court allows a shareholder-plaintiff to proceed because demand would be futile, the business judgment rule or other limitations on derivative suits often cause courts to defer to corporate boards and dismiss derivative claims.[18]

1. The Demand Requirement

Because corporate law gives the power to manage a corporation to its board of directors, courts generally require shareholder plaintiffs to provide some compelling reason for allowing a shareholder to pursue a derivative action instead of simply allowing the board of directors to proceed as it sees fit.[19] Under Delaware law, a shareholder plaintiff lacks standing unless she first makes a demand on the board of directors to pursue a claim or otherwise shows that she should not have to make demand because demand would be futile.[20] Most shareholder plaintiffs avoid making demand on the board and attempt to plead demand futility in the hopes that a court will excuse them from having to comply with the requirement.[21]

Delaware courts evaluate demand futility differently depending on the nature of the challenge to the board. If a shareholder plaintiff seeks to challenge some actual decision made by the board, courts

17. *See* Spiegel v. Buntrock, 571 A.2d 767, 772–73 (Del. 1990) ("A basic principle of the General Corporation Law of the State of Delaware is that directors, rather than shareholders, manage the business and affairs of the corporation."). Shareholder derivative claims assert power normally belonging to a corporation's board of directors. *Id.* at 773. To protect the board's ability to manage a corporation, courts impose significant limits on derivative actions. *See id.*

18. *See* John Matheson, *Restoring the Promise of the Shareholder Derivative Suit*, 50 GA. L. REV. 327, 353 (2016) (explaining that there are "a panoply of devices supposedly designed to avoid the dreaded strike suit, with the result that the current path to resolution of derivative claims is not a straight line. Rather, a series of sidebar skirmishes now condemns the derivative claim to a circuitous route of substantive non-resolution.").

19. DEL. CODE ANN. tit. 8, § 141 (2019).

20. *See* Collins J. Seitz, Jr. & S. Michael Sirkin, *The Demand Review Committee: How It Works, and How It Could Work Better*, 73 BUS. LAW. 305, 306 (2018) ("The demand requirement balances the board's statutory authority and its accountability to the corporation and its stockholders. It requires a stockholder who seeks to litigate derivatively on the corporation's behalf to first demand that the board pursue the claim, unless she can plead particularized facts tending to show that demand would be futile.").

21. *Id.*

apply the test announced in *Aronson v. Lewis*.[22] That test asks a court to consider "whether, under the particularized facts alleged, a reasonable doubt is created that: (1) the directors are disinterested and independent and (2) the challenged transaction was otherwise the product of a valid exercise of business judgment."[23] A different test from *Rales v. Blasband* applies "where the board that would be considering the demand did not make a business decision which is being challenged in the derivative suit."[24] The *Rales* test may come into play in instances where: (1) most of the board has turned over, leaving new directors in charge; (2) the suit challenges something other than a business decision made by the board; or (3) a suit challenges a decision made by a different business entity that was acquired by the corporation.[25] The *Rales* test asks a court to "determine whether or not the particularized factual allegations of a derivative stockholder complaint create a reasonable doubt that, as of the time the complaint is filed, the board of directors could have properly exercised its independent and disinterested business judgment in responding to a demand."[26]

These tests effectively winnow out many claims. Shareholder claims may be more likely to proceed if they can show that "a majority of the board is biased by factors such as familial, financial, professional, and social ties or faces a real risk of personal liability for non-exculpated claims."[27]

2. The Business Judgment Rule

In instances where derivative plaintiffs challenge some decision made by the board of directors, courts often apply the business

22. Aronson v. Lewis, 473 A.2d 805, 814 (Del. 1984), *overruled by* Brehm v. Eisner, 746 A.2d 244 (Del. 2000).

23. *Id.*

24. Rales v. Blasband, 634 A.2d 927, 933–34 (Del. 1993).

25. *Id.* at 934.

26. *Id.*

27. Daniel Hemel & Dorothy S. Lund, *Sexual Harassment and Corporate Law*, 118 COLUM. L. REV. 1583, 1634 (2018).

judgment rule to defer to the board's discretion.[28] Although the precise contours of the business judgment rule have been widely debated, many see it as "a doctrine of abstention pursuant to which courts in fact refrain from reviewing board decisions unless exacting preconditions for review are satisfied."[29]

Delaware's Chancellor Allen described the business judgment rule as providing "that where a director is independent and disinterested, there can be no liability for corporate loss, unless the facts are such that no person could possibly authorize such a transaction if he or she were attempting in good faith to meet their duty."[30] In practical terms, this generally means that, absent evidence of some improper motive, courts will tend to defer to the business decisions made by boards of directors.[31] This effectively insulates directors from having their decisions second-guessed by courts simply because something unfortunate happened to the corporation.

B. The Substantive Standard

Although shareholder plaintiffs may pursue a variety of different theories in the wake of a cybersecurity incident, most claims tend to focus on oversight liability or the duty to monitor, which may be the "'the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment.'"[32] Establishing an oversight claim requires shareholder-derivative plaintiffs to show not just that the board made some mistake but that they acted in bad faith.[33] In *Stone*

28. *Id.* at 1629.

29. Stephen M. Bainbridge, *The Business Judgment Rule as Abstention Doctrine*, 57 VAND. L. REV. 83, 87 (2004).

30. Gagliardi v. TriFoods Int'l, Inc., 683 A.2d 1049, 1052–53 (Del. Ch. 1996).

31. *Id.* at 1053. The court further explained:

> Obviously, it is in the shareholders' economic interest to offer sufficient protection to directors from liability for negligence, etc., to allow directors to conclude that, as a practical matter, there is no risk that, if they act in good faith and meet minimal proceduralist standards of attention, they can face liability as a result of a business loss.

Id. at 1052.

32. City of Birmingham Ret. & Relief Sys. v. Good, 177 A.3d 47, 55 (Del. 2017) (quoting *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996)).

33. *Id.*

v. Ritter, the Delaware Supreme Court adopted *Caremark*'s[34] general standard for oversight liability.[35] There, it held:

> *Caremark* articulates the necessary conditions predicate for director oversight liability: (a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention. In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations.[36]

In adopting the standard, the Delaware Supreme Court reframed *Caremark* and situated it as a part of the general duty of loyalty, placing it outside the reach of exculpation clauses under Delaware corporate law.[37] In essence, corporate boards must take some steps to monitor and oversee the corporation's functions and reporting systems and pay some level of attention to information generated by

---

34. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 971 (Del. Ch. 1996).

> Generally where a claim of directorial liability for corporate loss is predicated upon ignorance of liability creating activities within the corporation . . . 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—will establish the lack of good faith that is a necessary condition to liability.

Id.

35. Stone *ex rel*. AmSouth Bancorporation v. Ritter, 911 A.2d 362, 369–70 (Del. 2006).

36. *Id.* at 370.

37. *See* DEL. CODE ANN. tit. 8, § 102(b)(7) (2019) (precluding a corporate charter from eliminating or limiting director liability "[f]or any breach of the director's duty of loyalty to the corporation or its stockholders"); Benjamin P. Edwards, *Conflicts, Confidentiality, and other Concerns: The Promise and Peril for Lawyers Serving on Corporate Boards*, 64 ROCKY MTN. MIN. L. INST. 3, 3–20 (2018) ("corporate law often imposes a non-waivable duty of loyalty to the corporation"). Of course, not all states follow Delaware. Nevada, for instance, only imposes liability for a liability for a breach of the duty of loyalty if there is "intentional misconduct, fraud[,] or a knowing violation of law." NEV. REV. STAT. § 78.138(7) (2018).

those systems. Ultimately, *Caremark* may "demand almost nothing beyond asking that *some* compliance system exists."[38]

II. Recent Decisions in Cybersecurity Cases

Despite the difficulties involved in pressing a derivative claim for some corporate oversight failure, shareholders have brought suits alleging oversight liability after many significant cybersecurity failures.[39] This Part reviews some relatively recent cases and pulls guidance from these decisions for corporate boards considering how to address the cybersecurity challenge.

A. Wyndham

Between 2008 and 2010, Wyndham Worldwide Corporation (Wyndham) repeatedly lost information to hackers.[40] After the data breach emerged, the Federal Trade Commission (FTC) brought an enforcement action against Wyndham over its security practices.[41] In 2012, a Wyndham shareholder wrote to Wyndham's board and demanded that it instigate litigation based on the breaches and on account of its inadequate data security.[42] In response to the demand, Wyndham's board of directors met and considered the request before ultimately deciding not to pursue the claims suggested by the shareholder's demand.[43] After the board refused to act on the shareholder's demand, the shareholder filed suit in the United States District Court for the District of New Jersey.[44]

---

38. Donald C. Langevoort, Symposium, Caremark *and Compliance: A Twenty-Year Lookback*, 90 TEMP. L. REV. 727, 729–30 (2018).

39. Claire Loebs Davis, *5 Securities Litigation Issues to Watch in 2016*, LANEPOWELL (Jan. 19, 2016), https://www.dandodiscourse.com/2016/01/19/5-securities-litigation-issues-to-watch-in-2016/ [https://perma.cc/5VMK-USFB].

40. Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 WL 5341880, at *1 (D.N.J. Oct. 20, 2014) ("On three occasions between April 2008 and January 2010, that information was stolen. Hackers breached WWC's main network and those of its hotels.").

41. *Id.*

42. *Id.*

43. *Id.* at *2.

44. *Id.*

The court reviewed Wyndham's decision not to act on the shareholder's demand under the deferential business judgment standard.[45] It found that the board had conducted a reasonable investigation before it rejected the plaintiff's demand.[46] At the outset, the board was already well familiar with the cybersecurity issues and "had already discussed the cyber-attacks at fourteen meetings from October 2008 to August 2012."[47] Additionally, the board's audit committee had also discussed the cybersecurity issues at length, and Wyndham had hired third-party experts to investigate and issue cybersecurity recommendations.[48] Given the amount of information in the board's hands and the steps it had taken to address the issue, the court simply applied the business judgment rule and dismissed the claim.[49]

B. Target

In 2013, Target fell victim to cyber thieves who obtained personal and financial information for millions of Target's customers.[50] After shareholders filed five different derivative actions and delivered one demand to the board, Target created the "Special Litigation Committee"[51] (SLC) to investigate and vested it with full power over the issue.[52] The SLC conducted an enormous investigation and, in a ninety-one-page report, ultimately concluded that it would not be in Target's best interest to pursue litigation against its officers and directors.[53] In reaching this conclusion, the SLC reviewed Target's

45. *Id.* at *3 (citing Spiegel v. Buntrock, 571 A.2d 767, 773–74 (Del. 1990)) ("If a board of directors refuses to pursue a shareholder's demand, that decision falls under the purview of the 'business judgment rule.'").

46. *Palkon*, 2014 WL 5341880, at *4.

47. *Id.* at *5.

48. *Id.* at *2.

49. *Id.* at *7.

50. Memorandum of Law of the Special Litig. Comm. of the Bd. of Dirs. of Target Corp. in Support of its Motion for Approval and Dismissal at 2, Davis v. Steinhafel, No. 0:14-cv-00203-PAM-JJK (D. Minn. May 6, 2016), 2016 WL 2905335 [hereinafter Memorandum of Law].

51. For general information about special litigation committees, see Charles W. Murdock, *Corporate Governance—The Role of Special Litigation Committees*, 68 WASH. L. REV. 79 (1993).

52. Memorandum of Law, *supra* note 50, at 3, 5.

53. *Id.* at 2.

data security before the breach and the significant changes made after the incident.[54] At the SLC's request and without any opposition from the plaintiffs, the court ultimately dismissed the derivative litigation.[55]

C. Home Depot

In 2014, Home Depot revealed that it had suffered one of the largest data breaches in history with hackers obtaining access to fifty-six million customer credit card numbers.[56] Hackers exploited a vulnerability at a third-party vendor and then used the vendor's access to Home Depot's network to install malware and steal data from Home Depot.[57] Shareholder derivative claims soon followed, alleging that Home Depot's board "breached their duty of loyalty to Home Depot because [they] failed to institute internal controls sufficient to oversee the risks that Home Depot faced in the event of a breach and because they disbanded a [b]oard of [d]irectors committee that was supposed to have oversight of those risks."[58]

The Northern District of Georgia ultimately dismissed the claims because the plaintiffs failed to establish that demand was futile.[59] Applying Delaware law and following *Rales*, the court explained that pleading demand futility would require the plaintiffs to allege particularized facts creating "'a reasonable doubt that, as of the time the complaint is filed, the board of directors could have properly exercised its independent and disinterested business judgment in responding to a demand.'"[60] In assessing the demand-futility standard for the oversight claim, the court explained that the "[p]laintiffs

54. *Id.*

55. *See Cyber Breaches*, *supra* note 10, at 3.

56. Kevin LaCroix, *Home Depot Settles Data Breach-Related Derivative Lawsuit*, D&O DIARY (May 1, 2017), https://www.dandodiary.com/2017/05/articles/cyber-liability/home-depot-settles-data-breach-related-derivative-lawsuit/ [https://perma.cc/YD75-UDQR].

57. *In re* Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1321 (N.D. Ga. 2016) ("The hackers used a third-party vendor's user name and password to enter into Home Depot's network.").

58. *Id.*

59. *Id*. at 1332.

60. *Id.* at 1324 (quoting Rales v. Blasband, 634 A.2d 927, 934 (Del. 1993) (emphasis removed)).

essentially need to show with particularized facts beyond a reasonable doubt that a majority of the [b]oard faced substantial liability because it consciously failed to act in the face of a known duty to act."[61]

Although the facts alleged did not clear the "incredibly high hurdle" for pleading demand futility in this context, the court did criticize the board's conduct.[62] In "hindsight" it noted that "the implementation of the plan [to fix security problems] was probably too slow[] and that the plan probably would not have fixed all of the problems Home Depot had with its security."[63] The court stressed that boards do not need to make perfect decisions—simply reasonable ones.[64] Under Delaware law, so long as outside directors "pursued any course of action that was reasonable, they would not have violated their duty of loyalty," even if other actions would have been better.[65]

D. Yahoo

Breaking new ground as the first data-breach derivative settlement to recover funds for shareholders, Yahoo paid out $29 million in monetary damages, settling allegations that Yahoo's directors breached their fiduciary duties.[66] Over a period of years, Yahoo suffered a series of massive data breaches affecting over one billion user accounts, setting a series of records for the largest data breaches ever announced.[67] The derivative suits alleged that the Yahoo defendants knew about the data breaches long before revealing the

61. *Id.* at 1325.

62. *Id.*

63. *In re Home Depot*, 223 F. Supp. 3d at 1327.

64. *Id.* (quoting Lyondell Chemical Co. v. Ryan, 970 A.2d 235, 243 (Del. 2009)).

65. *Id.* at 1326 (emphasis removed).

66. Craig A. Newman, *Lessons for Corporate Boardrooms from Yahoo's Cybersecurity Settlement*, N.Y. TIMES (Jan. 23, 2019), https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html [https://perma.cc/26YB-UBJM] (explaining that the Yahoo settlement "marked the first time that shareholders have been awarded a monetary damages in a derivative lawsuit related to a data breach").

67. For a discussion of the Yahoo breaches in greater detail and context, see Trautman, *supra* note 6, at 1233–34.

information to the public and that they sought to cover up and hide the breach.[68] The settlement stands out for a number of reasons. As Kevin LaCroix highlighted:

> [T]here are certain features of the Yahoo situation that may make the circumstances somewhat unique. For starters, it appears to involve the largest ever data breach. There also is the very unfortunate circumstance of the long lag-time between the date of the breach and the time when Yahoo finally got around to disclosing the breach. Moreover, there is the very specific aspect of the case in which Verizon renegotiated the price of its asset acquisition, reducing the value of the deal by $350 million, which represented a very significant and undeniable financial consequence resulting from the data breach. Few other cases are going to involve anything like this combination of circumstances.[69]

The Yahoo derivative litigation may have also settled for real money because of statements in Yahoo's $35 million settlement with the Securities and Exchange Commission (SEC).[70] In particular, the SEC found that "Yahoo senior management . . . did not properly assess the scope, business impact, or legal implications of the breach, including how and where the breach should have been disclosed in Yahoo's public filings."[71] The SEC also declared that Yahoo's "senior management and legal teams" learned "[w]ithin days" about the information security team's discovery of the breaches in

68. Kevin LaCroix, *Yahoo Data Breach-Related Derivative Suit Settled for $29 Million*, D&O DIARY (Jan. 21, 2019), https://www.dandodiary.com/2019/01/articles/cyber-liability/yahoo-data-breach-related-derivative-suit-settled-29-million/#more-17535 [https://perma.cc/F9PN-84ES] (explaining that the suits alleged that Yahoo "knew about the data breaches long before they were disclosed to the public and that instead of disclosing that the data breaches had taken place the defendants sought to cover up the breaches").

69. *Id.*

70. In the Matter of Altaba Inc., f/d/b/a Yahoo! Inc., Respondent, Securities Act of 1933 Release No. 3937, Fed. Sec. L. Rep. (CCH) ¶ 75167 (Apr. 24, 2018) [hereinafter In the Matter of Altaba Inc.].

71. *Id.*

December 2014.[72] Attempting to explain the delay between discovery and revelation, Yahoo's 2016 Annual Report claimed that "certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally" about the breach. [73] It also averred that its independent committee "did not conclude that there was an intentional suppression of relevant information."[74]

Yahoo may have faced more significant risk from shareholder oversight claims because the long delay between the internal discovery and public revelation might allow a court to conclude that Yahoo consciously disregarded the information that senior leaders received about the breach. A court might be skeptical that Yahoo—a data company—did not comprehend the implications of a data breach.

CONCLUSION

Ultimately, courts will often hesitate before imposing liability for a cybersecurity failure because, in a real sense, a corporation suffering a data breach is the victim of a crime. Yet there may be some instances where courts should impose liability for cybersecurity failures. Consider the equities in an analogous situation. If bandits attack and loot a trade caravan, the organizers of the expedition suffer alongside its investors and passengers. The caravan's masters should not be held personally liable to investors simply because bad things happened. The world is full of risks. On the other hand, investors have a legitimate grievance if a caravan knowingly enters dangerous territory without acquiring at least some reasonable degree of protection. Because well-organized brigands may overwhelm even a

72. *Id.*

73. Yahoo! Inc., Annual Report 47 (Form 10-K) (Mar. 1, 2017), https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm [https://perma.cc/GW6D-6KU7].

74. *Id.*

reasonable complement of guards, courts should not second-guess most security decisions.

Yet as cybersecurity incidents accumulate, the floor for a reasonable data security program must rise. The risks facing large corporate operations now grow increasingly well-known and salient. Good-faith operations will pay serious attention to these risks. A corporate board that neglects the issue and ignores recommendations and requests from its cybersecurity staff does so at its peril. At the least, the Yahoo settlement counsels in favor of a robust reaction to the discovery of a data breach.[75]

In the final analysis, state corporate law's influence and the threat of shareholder oversight claims may stand in the shadow of other regulatory and market pressures driving corporate actors to improve their cybersecurity operations. Notably, the SEC recently released a report on cybersecurity connecting cybersecurity to issuers' obligations to maintain adequate internal controls.[76] These and other efforts to increase data security may apply greater pressure than state corporate law. As regulators ramp up their activities in this space, their findings and enforcement actions may also provide key facts and insights for shareholder plaintiffs considering oversight claims.

75. In the Matter of Altaba Inc., *supra* note 70.

76. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public companies and Related Internal Accounting Controls Requirements, Securities Act Release No. 84429 (Oct. 16, 2018).