CYBERSECURITY, RISK MANAGEMENT, AND HOW BOARDS CAN EFFECTIVELY FULFILL THEIR MONITORING ROLE

VICTORIA C. WONG*

ABSTRACT

In light of recent and well-publicized consumer data breaches, corporate directors and management are rightfully concerned about improving cybersecurity for the benefit of the firm, its shareholders, and consumers. Much attention has been focused on cybersecurity as a means for the board to fulfill its duty to monitor, as articulated under Caremark. Scholars and practitioners alike have forwarded recommendations to advise boards on how to improve security efforts as a means to avoid litigation. This article argues that such concerns are overblown, as a closer inspection of Caremark's progeny reveals that duty to monitor litigation will almost always fail. To demonstrate why this is so, this article uses two case studies involving the duty to monitor — the Target and Wyndham Hotel data breaches and resultant shareholder litigation. Although director liability is unlikely, recasting cybersecurity as a corporate governance concern explains why directors still wish to avoid shareholder litigation. Specifically, even absent the risk of personal liability, directors should and do consider reputational concerns, board reelection, and consumer reactions following a data breach. This article briefly concludes with board recommendations to avoid shareholder litigation in the context of cybersecurity.

TABLE OF CONTENTS

* J.D. Candidate Class of 2015, University of California, Davis; B.A. Social Welfare, University of California, Berkeley, 2012. Many thanks to Professor Thomas Joo for his invaluable guidance and feedback, and to the editors and staff of the U.C. Davis Business Law Journal. Thanks also to Gordy Davidson and Fenwick & West, whose institutional support provided access to Stanford's Directors' College 2014, which was the impetus for this article.

INTRODUCTION

Cyber attacks on major U.S. corporations are now commonplace and well publicized. For example, in 2013, Target experienced a data breach that impacted 70 million customers over a two-week period during the busy holiday season.[1] In the weeks leading up to the Target breach, Adobe announced that at least 38 million users were affected by a loss of customer data, and shortly after increased its estimate to 150 million.[2] In 2014, JPMorgan Chase experienced a cyber attack in the summer that compromised 76 million accounts,[3] hackers stole credit card information from 56 million Home Depot customers,[4] and eBay requested that 145 million users change their passwords following an attack where hackers stole email addresses, mailing addresses, passwords, and birth dates.[5] As Professor Zittrain has noted, "attacks have become so commonplace and widespread as to be indistinguishable from one another."[6]

In a data breach study, the Ponemon Institute reported that worldwide, the average cost to a company to investigate, notify, and respond to data breaches was $3.5 million USD in 2014, up 15% from 2013.[7] Target booked $148 million in expenses following its 2013 data breach for actual and pending breach-related claims, including claims by payment card networks.[8] Aside from data breaches'

---

[1] *See* Maggie McGrath, *Target Data Breach Spilled Info On as Many as 70 Million Customers*, FORBES (Jan. 10, 2014), http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers (describing the impact of the data breach on Target customers).

[2] *See* Alex Hern, *Did Your Adobe Password Leak? Now You and 150m Others Can Check*, GUARDIAN (Nov. 7, 2014), http://www.theguardian.com/technology/2013/nov/07/adobe-password-leak-can-check.

[3] Jessica Silver-Greenberg et al., *JPMorgan Chase Hacking Affects 76 Million Households*, DEALBOOK N.Y. TIMES (Oct. 2, 2014), http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=1.

[4] *See* Julie Creswell & Nicole Perlroth, *Ex-Employees Say Home Depot Left Data Vulnerable*, N.Y. TIMES (Sept. 19, 2014), http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?_r=0.

[5] *See* Jim Finkle et al., *EBay Asks 145 million Users to Change Passwords After Cyber Attack*, REUTERS (May 21, 2014), http://www.reuters.com/article/2014/05/21/us-ebay-password-idUSBREA4K0B420140521.

[6] Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 2011 (2006).

[7] *See Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis*, PONEMON INST. (May 5, 2014), http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis.

[8] *See Target Provides Preliminary Update on Second-Quarter Expenses Related to the Data Breach and Debt Retirement*, TARGET (Aug. 5, 2014), http://pressroom.target.com/news/target-

direct costs to the corporation, they can impact profits and the bottom line months and even years following a breach.[9]

Large data breaches have negatively affected consumer behavior, loyalty, and trust in major retailers and corporations.[10] Shareholders have brought derivative suits based on data breaches, claiming that directors and officers breached their fiduciary duties, wasted corporate assets, grossly mismanaged the corporation, and other abuses.[11] Cybersecurity attacks implicate the board's duty of care and duty to monitor, and their effect on corporate governance continues to play out in courtrooms, boardrooms, and the press. Accordingly, consumers, shareholders, and scholars have called for board and management action vis- à-vis increased monitoring.[12]

This article argues that despite recent highly publicized data breaches and resultant shareholder litigation, in almost all cases, directors and officers will not be held liable for violating the duty to monitor. However, even absent the risk of liability, directors should still be concerned about the reputational impact of direct and derivative lawsuits, board reelection, consumer reactions, and the bottom line. To prevent shareholder litigation, boards should implement best practices to enhance their cybersecurity systems, such as board education, enhanced monitoring, crisis management plans, and changes to corporate culture that prioritize cybersecurity.

---

provides-preliminary-update-on-second-quarter-expenses-related-to-the-data-breach-and-debt-retirement; *see also* John Kell, *Target to Book $148 Million in Data-Breach Expenses*, FORTUNE (Aug. 5, 2014), http://fortune.com/2014/08/05/target-data-breach-profit (describing direct costs resulting from Target's data breach).

[9] *See, e.g.*, Elizabeth A. Harris, *Data Breach Hurts Profit at Target*, N.Y. TIMES (Feb. 26, 2014), http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html (explaining than the company's profits fell more than 40% in the fourth quarter and net earnings were down 46% from the same period in 2012); Angela Chen, *Supervalu Profit Down 23%, Data Breach Costs Weigh*, MARKETWATCH (Oct. 16, 2014), http://www.marketwatch.com/story/supervalu-profit-down23-data-breach-costs-weigh-2014-10-16 (describing a drop in quarterly earnings for a supermarket operator due to costs associated with a data breach).

[10] *See, e.g.*, Lauren Coleman-Lochner & Lindsey Rupp, *Target Seen Losing Customer Loyalty After Credit Card Breach*, BLOOMBERG BUSINESSWEEK (Dec. 25, 2013), http://www.bloomberg.com/news/articles/2013-12-24/target-seen-losing-customers-in-wake-of-card-data-breach (demonstrating the impact on consumer goodwill following a data breach).

[11] *See* Kevin LaCroix, *Target Directors and Officers Hit With Derivative Suits Based on Data Breach*, D&O DIARY (Feb. 3, 2014), http://www.dandodiary.com/2014/02/articles/cyber-liability/target-directors-and-officers-hit-with-derivative-suits-based-on-data-breach; *see also* Teri Robinson, *Shareholder Sues Wyndham Board Members Over Data Breaches*, SC MAGAZINE (May 7, 2014), http://www.scmagazine.com/shareholder-sues-wyndham-board-members-over-data-breaches/article/345989.

[12] *See infra* Part I.

I. CORPORATE LAW BACKGROUND & WHY DUTY TO MONITOR LITIGATION WILL FAIL

This Part provides relevant corporate law background regarding the duty to monitor (sometimes called the duty of oversight), a subset of the duty of care.[13] This Part also describes shareholder derivative suits pending in the district courts that seek to impose personal liability on directors for failure to monitor the corporation's cybersecurity risks. Finally, this Part analyzes why plaintiffs will fail in light of the standards set forth in *Caremark*, *Disney*, and *Stone*.

The first Delaware case to elucidate the board's duty to monitor was *In re Caremark International Inc.* ("*Caremark*"),[14] a derivative suit where shareholders sought to impose personal liability on directors for inadequate internal controls in violation of the board's duty to monitor.[15] Caremark, a healthcare and patient prescription management company, settled a $250 million claim with the U.S. government for Caremark's violation of the Anti-Referral Payments Law.[16] Shareholders claimed that Caremark's board failed to appropriately monitor and supervise the corporation's officers and employees, and that the board was unaware of the illegal activities giving rise to the government investigation and $250 million settlement.[17]

Chancellor Allen described the duty to monitor in *Caremark* thusly, ""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 . . ." and that failure to comply with this responsibility could lead to director liability.[18] Moreover, "relevant and timely information" was essential to satisfy the board's supervisory and monitoring role under Delaware law.[19] However, Caremark's board ultimately prevailed on the duty to monitor claim because the court stated that "only a sustained or systemic 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."[20] Thus, the Chancery Court established the following test to find a breach of the duty of care with respect to the board's responsibility to "control" Caremark's employees (i.e., the duty to monitor): "(1) that the directors knew or (2) should have known that violations of law were

---

[13] *See* Stephen M. Bainbridge et. al., *The Convergence of Good Faith and Oversight*, 55 UCLA L. REV. 559 (2008).
[14] *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (1996).
[15] *See id.* at 968.
[16] *See id.* at 961.
[17] *See id.*
[18] *Id.* at 970.
[19] *Id.*
[20] *Id.* at 971.

occurring and, in either event, (3) that the directors took no steps in a good faith effort to prevent or remedy that situation, and (4) that such failure proximately resulted in the losses complained of."[21] The Court itself acknowledged that this test of liability was "quite high" and "demanding" in terms of what the plaintiff was required to allege and prove at trial.[22]

The *Caremark* court stated that the board's duty of care encompasses the duty to monitor, which is satisfied by adequate flow of information to the board.[23] Under *Caremark*, directors must make a "good faith effort" to ensure this flow of information. However *Caremark* did not fully define good faith, establish whether good faith came under the ambit of the duty of care or the duty of loyalty, or answer whether good faith was itself an independent fiduciary duty.

Caremark's progeny includes *In re Walt Disney Co. Derivative Litigation*[24] ("*Disney"*) and *Stone v. Ritter*,[25] which limited the duty to monitor and made it more difficult for plaintiffs to raise fiduciary duty violation claims. In *Disney*, the Delaware Supreme Court set forth several important doctrinal statements on the nature of the good faith requirement. The court opined that proof of "intentional dereliction of duty, a conscious disregard for one's responsibilities" could constitute bad faith sufficient to overcome the deferential business judgment rule.[26] *Disney* involved a shareholder derivative suit, where shareholders alleged director violations of the duty of loyalty and failure to act in good faith following the board's negotiations with and termination of then-CEO Michael Ovitz.[27] Although the Delaware Supreme Court provided some clarity regarding the definition of "bad faith," the question remained open as to whether, standing alone, a violation of the duty of good faith could form the basis of a shareholder derivative suit.[28]

The court answered this question in the negative shortly after *Disney*. In *Stone v. Ritter* ("*Stone*"), the Delaware Supreme Court approved both the *Caremark* standard and *Disney*'s definition of bad faith, formally establishing that "lack of good faith [is] a necessary condition to liability" for a duty of loyalty violation.[29] *Stone*, like *Caremark*, involved a shareholder derivative suit premised on the board's failure to exercise adequate oversight, which resulted in

---

[21] *Id.*
[22] *See id.*
[23] *Id.* at 970.
[24] *In re* Walt Disney Co., 906 A.2d 27, 62 (2006).
[25] Stone ex rel. AmSouth Bancorporation v. Ritter, 911 A.2d 362 (2006).
[26] *In re Walt Disney*, 906 A.2d at 63-64.
[27] *Id.* at 46.
[28] *See* Anne Tucker Nees, *Who's the Boss? Unmasking Oversight Liability Within the Corporate Power Puzzle*, 35 DEL. J. CORP. L. 199, 224 (2010).
[29] *Stone*, 911 A.2d at 365.

government investigations and civil penalties.[30] *Stone* did not purport to overrule any part of the *Caremark* decision, so the duty to monitor formally remains a subset of the duty of care. However, the *Stone* court stated that "the *Caremark* standard for so-called 'oversight' liability draws heavily upon the concept of director failure to act in good faith," and that failure to act in good faith is a violation of the duty of loyalty.[31] A duty of loyalty violation requires behavior that is more culpable than conduct that would violate the duty of care (i.e., gross negligence).[32]

As *Disney* and *Stone* make clear, plaintiffs must show bad faith in the board's conscious failure to act in the face of a known duty. This essentially renders the duty to monitor somewhat of a hybrid between the duty of loyalty and the duty of care. In other words, only behavior constituting "bad faith" satisfies *Caremark*'s requirement that a director failed to act in good faith, which implicates the duty of loyalty. Once this and the other *Caremark* elements are met, a duty to monitor claim (which falls under the ambit of the duty of care) can move forward. Despite the low success rate of *Caremark* claims and scholarly commentary that the *Caremark* standard is "virtually meaningless," shareholders continue to allege violations of the duty to monitor against directors at major corporations.[33]

Shareholders have brought at least two derivative suits premised on the duty to monitor against directors of Wyndham Worldwide and Target Corporation following data breaches at each company. These claims were raised in federal district court based on diversity jurisdiction. The Wyndham shareholders filed suit in the District Court of New Jersey, applying Delaware law, because Wyndham is incorporated in Delaware and headquartered in New Jersey.[34] The Target shareholders filed suit in the District Court of Minnesota, applying Minnesota law, since Target is incorporated and headquartered in Minnesota.[35]

The first shareholder derivative suit is *Palkon v. Holmes* ("*Palkon*").[36] This suit was brought by Wyndham Hotel shareholders against directors of the hospitality giant, which experienced a data breach that exposed the personal data of more than 619,000 customers, leading to credit card fraud and identity theft.[37]

---

[30] *Id.* at 366.
[31] *Id.* at 369.
[32] *Id.*
[33] *See* Nees, *supra* note 28 at 205.
[34] *Corporate Governance – Highlights*, WYNDHAM WORLDWIDE, http://investor.wyndhamworldwide.com/phoenix.zhtml?c=200690&p=irol-govhighlights (last visited Dec. 21, 2014) (see Governance Documents, specifically Wyndham's Certificate of Incorporation).
[35] *See* Kulla v. Steinhafel, 2014 WL 2116594 (2014).
[36] Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 WL 5341880, at *1 (2014).
[37] *Id.*

Shareholders alleged that directors' "negligent inattention to cybersecurity allowed massive thefts of customer data on three occasions."[38] The complaint also states that "[Wyndham's] vendor stopped providing security updates . . . more than three years before the intrusions," and that as a result of these deficiencies, the corporation "unreasonably and unnecessarily" exposed customers' sensitive personal information.[39]

The *Palkon* court, applying Delaware law, dismissed the plaintiff's complaint because of problems with the plaintiff's demand. The shareholders made a demand in 2013, which the board refused, and the shareholders filed a complaint in early 2014, alleging inadequate monitoring leading to the data breach. Wyndham moved to dismiss in June, arguing that the 2013 demand refusal was a good faith exercise of the board's business judgment, that the complaint failed to state a claim upon which relief can be granted, and that any alleged damages were speculative and unripe.[40] The plaintiff opposed the motion to dismiss, arguing that the demand refusal was conflicted and that the directors predetermined the refusal before conducting a reasonable investigation.[41] The court rejected the plaintiff's opposition motion, holding that there was no conflict of interest and that the strong presumption of the business judgment rule favors the board, even if the board only conducts a cursory investigation before refusal.[42] Because the court did not reach the merits of the case, they will be evaluated under *Caremark* below.

For the purposes of this article, the Target claim will also be evaluated under Delaware law. In Minnesota, the board's responsibilities and duties are codified in Business Corporations Code sections 302A.201 ("Board") and 302A.251 ("Standard of Conduct").[43] According to the legislative history of these statutes, they are based on the Delaware General Corporation Law ("DGCL"), especially DGCL section 141(a), which tasks the board with managing the corporation but allows directors to delegate management responsibilities.[44] Delaware case law is cited in the legislative history pertaining to the board's ability to delegate its responsibilities.

The Minnesota legislature's General Comments to section 302A.201 state that "the duty of oversight and the liability for the actions of those persons or

---

[38] *Wyndham Directors at Fault for Cybersecurity Lapses, Mass Info Theft, Suit Says*, 29 WESTLAW J. CORP. OFFICERS & DIRECTORS LIABILITY 1, 3 (2014).

[39] *Id.*

[40] *Palkon*, 2014 WL 5341880, at 2.

[41] *Id.* at 3-6.

[42] *Id.* at 6-7.

[43] *See* MINN. STAT. ANN. §§ 302A.201 & 302A.251 (West).

[44] *See* MINN. STAT. ANN. § 302A.201; *see also* DEL. CODE ANN. tit. 8, § 141 (West) ("Board of directors; powers; number, qualifications, terms and quorum; committees; classes of directors; nonstock corporations; reliance upon books; action without meeting; removal").

committees remains, however, with the board," and describes this development as "new to Minnesota statutory corporate law."[45] Section 302A.251, establishing standards of conduct, requires that the directors discharge their duties in good faith and allows reliance on information presented by certain employees, auditors, and board committees.[46] Notes of decision to these statutes do not include cases that address the duty of oversight, and general searches for "duty of oversight" and "duty to monitor" do not yield relevant results. This indicates that Minnesota courts have not had the opportunity to meaningfully develop the contours of this duty. Based on the legislative history of Minnesota's Business Corporations Code, it is likely that courts applying Minnesota law to duty to monitor claims will rely heavily on Delaware case law. Thus, in evaluating the Target shareholder claims involving the duty to monitor, the District Court will likely look to Delaware case law for guidance.

Kulla v. Steinhafel ("*Kulla*")[47] involves four consolidated shareholder derivative suits against Target's directors, asserting that directors consciously failed to act despite numerous warnings about the risk of potential security breaches at Target stores.[48] Shareholders allege that directors received warnings as early as 2007 from data security experts, who informed the board about the possibility of a "point-of-sale" security breach that could impact as many as 58 million card accounts.[49] Despite these warnings, Target's board and management "failed to ensure that Target complied with basic industry standards for protecting consumer information."[50]

Thus, the shareholders bring suit for breach of fiduciary duty, unjust enrichment (a confusing claim not further explained nor substantiated in the complaint or pre-consolidation court documents), and corporate waste. To show corporate waste, the plaintiff must prove that directors exchanged corporate assets for essentially no consideration (or unreasonably little consideration).[51] This strategy is likely a dead end for most plaintiff-shareholders because the test for corporate waste is difficult to meet. The Target shareholders premise their corporate waste claim on the data breach investigation costs, profit losses due to discounts to lure back customers, consumer class action payouts, and improper compensation to directors who breached their duty to monitor.[52] This claim is likely to fail because Target's directors can credibly argue that these expenditures

---

[45] *See* MINN. STAT. ANN. § 302A.201 (referring to the "Reporter's Notes – General Comment" section for a description of the state of the doctrine in Minnesota).
[46] *Id.* § 302A.251.
[47] *Kulla*, 2014 WL 2116594.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] Brehm v. Eisner, 746 A.2d 244, 263 (2000).
[52] *Kulla*, 2014 WL 2116594.

do not waste corporate assets. The directors can claim they reasonably believed that discounts and promotions would have a positive net effect in the long term. For example, such promotions could lure back customers and investigation costs could improve Target's security systems for the future.

The shareholders seek monetary relief for damages suffered by Target. Additionally, the shareholder plaintiffs seek improvements to Target's corporate governance structure "that will restore consumer confidence in the Company's ability to protect its customers' sensitive personal and financial information."[53]

In both *Palkon* (assuming the court had reached the merits) and *Kulla*, the shareholders are unlikely to prevail on their claims. *Caremark* consciously established a high bar for plaintiffs to prevail on a theory based on breach of the duty to monitor, essentially requiring shareholder plaintiffs to prove that no internal controls existed. The *Palkon* court stated that dismissal did not require discussing the claim's merits, but noted that a *Caremark* claim in the context of data breaches was a "novel theory."[54]

In a footnote, the *Palkon* court observed that, based on the facts alleged in the complaint, the plaintiffs "concede[d] that security measures existed when the first breach occurred, and admits the Board addressed such concerns numerous times."[55] This will likely be the result in many shareholder derivative claims based on inadequate cybersecurity. In other words, plaintiffs will often be able to point to specific instances where the board was warned about security problems or took actions that, in hindsight, might be viewed as "relaxing" cybersecurity (for example, that Wyndham's computer security vendor stopped supplying updates years before the breaches). However, to meet the *Caremark* standard for failure to monitor, the plaintiffs must show that *no* internal controls existed. The fact that a corporation employs data security employees, has contracts with security vendors, and receives periodic reports about the status of the company's cybersecurity will easily defeat the claim that directors did not take adequate steps to inform themselves of risk. The *Palkon* shareholders would have run into this challenge because they could not, and did not, allege that Wyndham had absolutely no cybersecurity measures in place.

In the Target case, the shareholders claimed that data security experts warned Target directors as early as 2007 about point-of-sale breaches.[56] The shareholders use this and Target's alleged inaction as evidence of inadequate monitoring.[57] However, as stated above, the very employment of data security experts and continuous presentations to the board demonstrate that internal

---

[53] *Id.*
[54] *Palkon*, 2014 WL 5341880, at n.1.
[55] *Id.*
[56] *Kulla*, 2014 WL 2116594.
[57] *Id.*

controls existed. If the directors failed to act in the face of numerous warnings, this could still be protected by the business judgment rule. As long as the directors used a reasonable and prudent process to make a decision, the content of the decision is a business judgment that courts will not second guess.[58] For example, Target directors could concede that they were warned in 2007 and made the decision to move forward without fortifying security systems because such upgrades would be too costly, or that the possibility of a breach was too remote. Even if Target's directors didn't make a conscious decision, the fact that they considered the information is probably adequate because they can credibly argue that they prioritized other business decisions.

As a subset of the duty of care, directors' oversight decisions are protected by the deferential business judgment rule.[59] Moreover, even if plaintiffs could prove that no internal controls existed, *Caremark*'s doctrinal development has incorporated bad faith by requiring plaintiffs to prove that directors intentionally and consciously disregarded their duties.[60] From a practical and evidentiary standpoint, this requirement makes it even more difficult, if not impossible, for plaintiffs to win a duty to monitor claim.

Even in the unlikely event that shareholders make it past the dismissal stage and prevail on the merits of a duty to monitor claim, directors are not personally liable for damages. DGCL section 102(b)(7) allows Delaware corporations to exculpate directors from personal liability.[61] Minnesota's Business Corporations Code section 302A.251 also enables director exculpation.[62] Both Wyndham and Target have exculpation provisions in their charters, which act as shields against director liability.[63] In sum, shareholder litigation in this area will almost always fail, and even if it succeeds, directors will not be personally liable for damages arising from a shareholder derivative suit.

In light of these facts, why do directors still believe, and scholars still argue, that there is a real duty to monitor under *Caremark*? One explanation is that the import of *Caremark*'s language has been overstated and taken out of context. The *Caremark* court merely suggested that director liability *could* arise from failure to monitor the corporation's compliance with law, which departed

---

[58] *See* Aronson v. Lewis, 473 A.2d 805, 812 (1984) (overruled on other grounds by Brehm v. Eisner, 746 A.2d 244 (2000)) (defining the business judgment rule).

[59] *See* Nees, *supra* note 28 at 206.

[60] In re Walt Disney Co. Litig., 906 A.2d 27, 64 (2006).

[61] DEL. CODE ANN. tit. 8, § 102(b)(7) (West)

[62] MINN. STAT. ANN. § 302A.251.

[63] *See* Restated Certificate Of Incorporation of Wyndham Worldwide Corporation 4, *available at* http://wyndhamworldwide.com/sites/default/files/investordocs/Restated%20Certificate%20of%20Incorporation.pdf (last visited Apr. 1, 2015); Articles of Amendment Adopting Amended and Restated Articles of Incorporation of Target Corporation Article IV, June 10, 2010.

from precedent and caused directors to panic.[64] Immediately following *Caremark*, scholars argued that directors in regulated industries should be especially vigilant since Caremark International violated pharmaceutical regulations.[65] Additionally, before the Delaware Supreme Court handed down *Disney* and *Stone*, it is arguable that a decade-long period of uncertainty as to the contours of the duty to monitor, especially in relation to the duty of good faith, resulted in speculation and overly cautious recommendations from the academy and corporate counsel.

Despite these concerns, one scholar has aptly summarized the state of oversight liability, writing that it "is skewed so far towards director authority that it is an eviscerated and meaningless tool of accountability."66 Even if shareholder litigation in this area will almost always fail, directors still have an interest in preventing such litigation and to improve cybersecurity risk management for practical reasons outlined in Part II.

II. REFRAMING THE PROBLEM AS ONE OF CORPORATE BEST PRACTICES

This Part explains why directors should be and are interested in improving corporate governance policies relating to cybersecurity, even when the threat of losing litigation is absent. Recently, shareholders and stakeholders have urged stronger cybersecurity practices. In light of these calls to action, directors have a heightened sense of their own personal interests in board reelection, preventing loss of consumer loyalty, minimizing damage to the bottom line, and preventing shareholder derivative suits in the first instance by having robust internal controls that discourage litigation. Thus, recasting cybersecurity as a corporate governance and best practices issue, rather than a strictly legal or fiduciary duty issue, provides clearer and more well-defined guidance to directors.

A. Reputational Concerns

Directors are still concerned with the duty to monitor and overseeing cybersecurity risk because they want to protect their professional reputations while managing well-respected companies that are not inundated with direct consumer actions or shareholder derivative suits.[67] Heightened oversight, at least in theory, enhances cybersecurity practices and can prevent breaches.

---

[64] H. Lowell Brown, *The Corporate Director's Compliance Oversight Responsibility in the Post Caremark Era*, 26 DEL. J. CORP. L. 1, 16 (2001).

[65] *See id.* at 6.

[66] Nees, *supra* note 28 at 257.

[67] *See generally* Eliezer M. Fich & Anil Shivdasani, *Financial Fraud, Director Reputation, and Shareholder Wealth*, 86 J. FIN. ECON. 306 (2007) (investigating reputational impact of fraud investigations).

In the context of consumer class actions, which are direct suits against the corporation based in tort, directors need not fear personal liability (because they will not be sued in their individual capacities). However, directors still recognize that direct lawsuits deplete corporate resources through legal fees and settlements. Even if the corporation escapes liability from a direct consumer lawsuit, the fact that the corporation is being sued reduces consumer confidence and acts as a "black mark" on corporate reputation.[68]

Directors have a strong incentive to prevent shareholder derivative suits as well, as they signal dissatisfaction with the corporation's management and express disapproval for the directors individually and in their capacity to make good business decisions.[69] James Cox argues that the shareholder suit has an "expressive value" that can "affirm desirable norms in the corporate setting," and suggests ways to enhance the stature and meaning of shareholder suits.[70] Implicit in his argument is that, apart from the plaintiff's desire for compensation to the corporation, these lawsuits communicate something negative to the corporation's directors and society at large.

Even putting aside the financial costs of defending a shareholder derivative suit, they often entail embarrassment to the named directors. Directors do not want to be accused of poor leadership or incompetence. Shareholder derivative litigation against directors can also render directors subject to deposition, or subject their correspondences to discovery.[71] Recently, two scholars have stated that the problem for directors is that, "even if the threat of personal liability is remote, the reputational consequences of embarrassing revelations could be severe."[72]

B. Board Elections as a Corporate Governance Alternative to Lawsuits

At the end of 2013, prominent proxy adviser Institutional Shareholder Services ("ISS") called on Target's shareholders to oust seven out of ten directors for failure to ensure adequate cybersecurity systems.[73] The recommendation focused on board members serving on the audit and corporate responsibility committees, which monitored risk. ISS blamed the board members for "setting

---

[68] *See* Kenneth B. Davis, Jr., The *Forgotten Derivative Suit*, 61 VAND. L. REV. 387, 402 (2008)

[69] *See id*. at 401.

[70] James D. Cox, *The Social Meaning of Shareholder Suits*, 65 BROOK. L. REV. 3, 7 (1999).

[71] Érica Gorga & Michael Halberstam, *Litigation Discovery and Corporate Governance: The Missing Story About the "Genius of American Corporate Law"*, 63 EMORY L.J. 1383, 1398-99 (2014).

[72] *Id*.

[73] *See* Paul Ziobro, *ISS's View on Target Directors Is a Signal on Cybersecurity; Proxy Firm Says the Board Failed to Adequately Manage Risk of a Breach*, WALL ST. J. (May 28, 2014), http://online.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278.

the stage" for the data breach which resulted in significant losses to the company and its shareholders.[74]

Despite ISS's recommendation, Target shareholders reelected the entirety of Target's board in June 2014.[75] However, four out of ten board members received less than 80% of shareholder votes cast, indicating investor discontent as incumbent board members generally receive a vote of 90% or more.[76] Paul Edelman et al. have argued that in the context of Say on Pay, companies receiving negative ISS voting recommendations have increased their responsiveness to shareholder concerns about compensation plans, and that such responsiveness rises with the proportion of negative shareholder votes.[77] This concept should translate to board elections as well because directors are more likely to change certain behaviors (in this case, directors have the incentive to go the extra mile to demonstrate cybersecurity competency) in response to negative shareholder votes. Although ISS was unsuccessful in calling on shareholders to oust the board, investors, at a minimum, expressed dissatisfaction and demonstrated one way that shareholders can call for improved governance by means other than derivative suits.

C. Consumer Reactions to Data Breaches

Consumers have also reacted negatively to cyber attacks, showing that breaches diminish customer trust and loyalty, and can cause reputational harm to the corporation. For example, Target reported that 2013 fourth quarter profits were down 40% from the previous year. The loss was partially attributed to declining retail sales overall. However, it could also be linked to unanticipated expenditures to lure back customers (e.g., a promotion featuring 10% discount in all stores following the breach announcement), establishing lines of communications with customers whose accounts had been compromised, and offering free credit monitoring.[78] The recorded dip in profits did not account for costs related to litigation, fraud claims, and investigative fees.[79] In July 2014, eBay's third quarter sales outlook fell short of estimates following its data

---

[74] *Id.*

[75] Martin Moylan, *Despite Firestorm, Target Board of Directors Re-elected*, MPRNEWS (June 11, 2014), http://www.mprnews.org/story/2014/06/11/target-board-re-election.

[76] *See* Martin Moylan, *Target Shareholders to Board: We Are Not Happy*, MPRNEWS (June 13, 2014), http://www.mprnews.org/story/2014/06/13/target-shareholder-votes.

[77] *See* Paul H. Edelman et al., *Shareholder Voting in an Age of Intermediary Capitalism*, 87 S. CAL. L. REV. 1359, 1429 (2014).

[78] *See* Harris, *supra* note 9.

[79] *Id.*

breach.[80] In addition to competition from other online retailers, eBay faced other challenges in attracting new customers during the quarter, especially following the announcement that a cyber attack required 145 million users to change their passwords.[81]

The takeaways from litigation risk, effects on board reelection, and consumer dissatisfaction are clear. Even without the threat of legal liability, directors should still be concerned with corporate best practices in the realm of cybersecurity. Accordingly, boards should mount an appropriate response to cybersecurity attacks and improve internal controls and corporate practices related to managing cyber risks.

D. Recommendations Moving Forward

Corporate counsel at well-respected law firms have issued client notices advising boards to do the following: (1) inform themselves of cyber risks, (2) increase monitoring over officers responsible for maintaining base level cybersecurity controls, (3) have an incident response and crisis management plan in place, and (4) encourage company-wide security and promote a corporate culture that prioritizes cybersecurity.[82]

First, education and information technology competency are touchstones of many cybersecurity reforms focused on the board. These efforts should be consistent and well-documented in the event of shareholder derivative litigation since such actions could prove that directors prioritized cybersecurity, sufficiently understood cyber risks, and took adequate and reasonable steps to prevent data breaches.

Second, directors should increase oversight of executives tasked with protecting the corporation's information technology infrastructure, and require internal audits to provide annual reports on the firm's cybersecurity efforts.[83] There should be a dedicated executive information security officer who regularly reports to the board to keep directors apprised of information security projects, strategies, and issues affecting the corporation. This is especially true for large corporations. Directors would be in the best position to monitor executives responsible for information safety by having dedicated cybersecurity executives

---

[80] Brian Womack, *EBay Forecasts Sales Short of Estimates After User Data Breach*, BLOOMBERG (July 17, 2014), http://www.bloomberg.com/news/2014-07-16/ebay-forecasts-revenue-short-of-estimates-as-amazon-surges-ahead.html.

[81] *Id.*

[82] *See* Edward Gallardo & Andrew Kaplan, *Board of Directors Duty of Oversight and Cybersecurity*, DEL. BUS. CT. INSIDER 2 (Aug. 20, 2014), http://www.gibsondunn.com/publications/Documents/GallardoKaplan—Board-of-Directors-Duty-of-Oversight-Aug2014.pdf.

[83] *Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition*, NAT'L ASS'N. CORP. DIRECTORS (June 10, 2014), *available at* http://www.nacdonline.org/Cyber.

who could work in tandem with a separate enterprise risk committee with cybersecurity proficiency. An annual independent audit of the corporation's cybersecurity processes and systems would provide more information to the board, as well as an additional check on the adequacy of internal controls.

Third, directors are ultimately responsible for incident response and crisis management plans, which are essential to minimize reputational harm and consumer loyalty loss after a data breach. An effective crisis management plan requires that internal controls detect the data breach in a timely fashion. Timely detection should trigger an internal incident response and investigation, reporting to law enforcement, customer notification, containment and remediation, and a response to the ensuing publicity.[84]

Critics have noted that Target's reaction to its data breach was exceptionally poor.[85] It took the company almost a week to announce that its payment system had been compromised, which added to consumer outrage.[86] Moreover, rather than reissuing its branded "Red" debit and credit cards to accountholders, Target imposed spending limits on those cards, sometimes without informing customers. Customers learned of this limit when their purchases were declined at other retail establishments during the busy holiday season.[87] Target's failure to timely and effectively respond to its massive data breach demonstrates how ineffective crisis management can exacerbate reputational damage in the eyes of consumers and cause investor dissatisfaction.

Fourth, the board is the catalyst of cultural change in any corporation[88] The Institute of Internal Auditors Research Foundation sponsored a report that said, "In most organizations, the higher you are in the hierarchy of management, the more impact you can have on implementing policies and enabling culture change. Cybersecurity should be no different."[89] Cultural and material changes, such as prioritizing education not only for the board but for employees across the firm, is one way to raise cybersecurity awareness. Employees should be alert of cyber risks and be encouraged to be proactive in raising concerns with supervisors. A firm that prioritizes cybersecurity should remind employees to

---

[84] *Cyber Security Crisis Management: A Bold Approach to a Shadowy Nemesis*, PRICEWATERHOUSECOOPERS 4 (Aug. 2011), http://www.pwc.com/en_CA/ca/technology-consulting/security/publications/pwc-cyber-security-crisis-management-2013-05-en.pdf.

[85] Paula Rosenblum, *Home Depot Data Breach: Banks' Response Is Critical To Consumer Reaction*, FORBES (Sept. 19, 2014), http://www.forbes.com/sites/paularosenblum/2014/09/19/home-depot-data-breach-banks-response-is-critical-to-consumer-reaction.

[86] *Id.*

[87] *Id.*

[88] *See* Thomas C. Baxter, Jr. & Chester B. Feldberg, *Crisis Avoidance, Containment and Control: A Report from the Financial Services Front*, 117 BANKING L.J. 291, 317 (2000).

[89] *Cybersecurity: What the Board of Directors Needs to Ask*, INST. INTERNAL AUDITORS RESEARCH FOUND. 13 (2014), https://na.theiia.org/special-promotion/PublicDocuments/GRC-Cybersecurity-Research-Report.pdf.

keep a "clean machine" and avoid installing outside programs on work computers, follow good password practices, encourage deletion and reporting of suspicious emails and attachments to avoid phishing and spearphishing scams, and backing up employee work in reliable storage systems.[90] Commentators have noted that cybersecurity is something that the corporation must affirmatively and continuously *do*, rather than a rote exercise in ticking checkmarks off a list that lulls directors and management into a false sense of security once establishing some base level of risk management.[91]

Some may argue that the cost of implementing these recommendations is too high when balanced against the risk that directors will be held liable for a breach of fiduciary duty. However, as discussed in Part II.c, loss of consumer loyalty and goodwill negatively impacts a corporation's bottom line.[92] Moreover, consumer lawsuits, such as class actions, are costly to settle or defend for any firm.[93]

Accordingly, corporations have increased spending on cybersecurity, both for prevention and to enhance corporate reputation following a breach. For example, after its summer 2014 data breach, JPMorgan Chase announced that it will double its spending on cybersecurity in the next five years.[94] Target accelerated a $100 million program to adopt the use of chip-enabled smart cards in Target stores, a method that makes stolen information more difficult for hackers to use.[95] These corporate actions demonstrate the understanding that cyber attacks and data breaches are harmful to the corporation even absent the risk of losing fiduciary duty lawsuits.

Ultimately, these recommendations are steps in the right direction for directors who are concerned not only about their own personal liability, but are unsure of how to effectively fulfill their roles as the ultimate managers of the

---

[90] *Creating a Culture of Awareness*, NAT'L CYBER SECURITY ALLIANCE, http://staysafeonline.org/re-cyber/creating-a-culture-of-awareness (last visited Nov. 17, 2014 10:10 AM).

[91] *See* Jeffrey Man, *Cybersecurity Is About Attitude, Culture—Not Strictly Compliance*, TENABLE NETWORK SECURITY (Apr. 10, 2014), http://www.tenable.com/blog/cybersecurity-is-about-attitude-culture-not-strictly-compliance.

[92] *See supra* Part II.C. Consumer Reactions to Data Breaches.

[93] *See e.g.*, Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L. 313, 334 (2011) (providing as an example the class action lawsuit arising from a data breach against TJX, the parent company of TJ Maxx and other retailers, where TJX spent over $12 million in one quarter for investigation and containment costs, improvements to their computer security and systems, and legal fees).

[94] Emily Glazer, *J.P. Morgan CEO: Cybersecurity Spending to Double*, WALL ST. J. (Oct. 10, 2014), http://online.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976.

[95] Dhanya Skariachan & Phil Wahba, *U.S. Retailers Face Pressure to Raise Cybersecurity Spending*, REUTERS (Feb. 5, 2014), http://www.reuters.com/article/2014/02/05/us-usa-retailers-cybersecurity-idUSBREA1409H20140205.

corporation. A practical and beneficial effect of formal, robust internal controls is that some shareholder suits will be prevented in the first instance. Even if such claims are filed, they are more likely to be dismissed if the corporation can show at the outset that adequate cybersecurity measures have been taken and that the board and top executives are informed of such risks. Aside from litigation considerations, directors would simultaneously address several concerns arising from data breaches, such as loss of consumer loyalty and resultant impact on the bottom line, investor satisfaction, and board reelection.

CONCLUSION

Cybersecurity attacks on major U.S. corporations are now ubiquitous and inevitable. Some commentators have questioned the effect of cybersecurity on directors' duty to monitor. These concerns are largely overblown. The case law addressing the duty to monitor demonstrates that the bar for plaintiff success in fiduciary duty violation cases is exceedingly high, as plaintiffs are essentially required to show that *no* internal controls existed. Although directors need not fear liability stemming from shareholder derivative suits, there are practical reasons that corporate governance policies relating to cybersecurity should continuously be examined and improved. These reasons include director reelection to the board, customer loyalty, protecting the corporation's bottom line, and discouraging shareholder litigation in the first place. Practically, directors should educate themselves, increase oversight over processes and management dedicated to cybersecurity, develop and update crisis management plans, and promote corporate culture prioritizing cybersecurity.