CYBERSECURITY OVERSIGHT: A CAUTIONARY TALE FOR DIRECTORS

Harris Yegelwel[*]

* J.D. 2016, University of Florida Levin College of Law and can be reached at hyegelwel@gmail.com. The author wishes to thank Professor Lyrissa Lidsky, for her faith, interest, and excitement in the topic and helpful comments and critiques of this work. The author also would like to thank his parents, Bruce and Betsy Yegelwel, for their unconditional love, support, and assistance with this work. Finally the author is incredibly grateful to the *Journal of Technology Law & Policy* for selecting his work for publication.

INTRODUCTION

To date, cyberattacks have cost American companies trillions of dollars.[1] The average data breach costs companies nearly $500,000.[2] Cyberattacks are not only disruptive and time-consuming; they can also result in disclosure of corporate strategic planning information, which would otherwise be shielded from the public.[3] Additionally, the nature of hacking has evolved tremendously, even in just the last decade.[4] When hacking first came to the public's attention, hackers and cybercriminals would flaunt their ability to bypass complex codes and encryption designed to safeguard sensitive information.[5] Computer hackers prided themselves on outsmarting any security measure, and identifying themselves as the source of the attack.[6] Cybercriminals grow much more

1. *See* Matt Egan, *Report: Cyber Crime Costs Global Economy Up to $500B a Year*, FOX BUS. (July 22, 2013), http://www.foxbusiness.com/technology/2013/07/22/report-cyber-crime-costs-global-economy-up-to-1-trillion-year (comparing cybercrime to other criminal activities: "global cyber activity costs between $100 billion and $500 billion each year, compared with $600 billion in cost associated with drug trafficking and $1 billion to $16 billion in costs tied to piracy").

2. *Cyberattacks on the Rise: Are Private Companies Doing Enough to Protect Themselves?*, PWC (2014), *available at* http://www.pwc.com/us/en/private-company-services/publications/assets/pwc-gyb-cyber security.pdf [hereinafter *Cyberattacks on the Rise*].

3. *Id.*

4. *Cybercrime: Hearing Before the S. Subcomm. of the Comm. on Appropriations*, 106th Cong. (2000) (statement of Louis J. Freeh, Director, FBI), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-106shrg63940/html/CHRG-106shrg63940.htm.

5. *Id.*

6. S. Krishnan, *Welcome to the Era of Hacking, Total Exposure*, TRAVELING TIME (Aug. 31, 2012), http://krishnan1983.blogspot.com/ 2012/08/hacking-in-todays-world.html.

sophisticated as technological developments continue to advance.[7] Attacks are now more often financially motivated and committed anonymously.[8]

The inability to identify where the source of an attack originates can spark political turmoil[9]—countries are quick to blame one another.[10] It is difficult to combat an enemy without an identity or physical location.[11] Modern cyberattackers are predatory and patient.[12] Hackers install complicated malware that allows them to monitor corporations for months, waiting for the perfect time to strike.[13] Finally, the most troublesome aspect of data breaches and cybersecurity measures is that what may be adequate one day may become obsolete the next day.[14] In response to these daunting developments, cybersecurity defense systems have also evolved.[15] In fact, these new systems identify hackers and target threats that may have only recently gone unnoticed, until it was too late.[16] Although not discussed in depth, some examples are mentioned later in the Note.

This Note seeks to explore the impact of cybersecurity in a particular context: corporate law. Specifically, this Note examines whether a Board of Directors (Board) should be liable for breach of fiduciary duty for failure to take reasonable and prophylactic measures to protect sensitive corporate data. As the magnitude and sophistication of cyberthreats

---

7. THOMAS CALABRESE, INFORMATION SECURITY INTELLIGENCE: CRYPTOGRAPHIC PRINCIPLES AND APPLICATION 69 (2004).

8. Daniel Sieberg, *Hackers Shift Focus to Financial Gain—Internet Criminal Not Content to Just Wreak Havoc Online*, CNN, http://www.cnn.com/2005/TECH/internet/09/26/identity.hacker/ (last updated Sept. 26, 2005 21:54 GMT); *see also* David E. Sanger, *Pentagon Announces New Strategy for Cyberwarfare*, N.Y. TIMES (Apr. 23, 2015), http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html?smprod=nytcore-ipad&smid=nytcore-ipad-share&_r=0.

9. Sanger, *supra* note 8.

10. Jennifer Steinhauer, *House Passes Cybersecurity Bill After Companies Fall Victim to Data Breaches*, N.Y. TIMES (Apr. 22, 2015), http://www.nytimes.com/2015/04/23/us/politics/computer-attacks-spur-congress-to-act-on-cybersecurity-bill-years-in-making.html?smprod=nytcore-ipad&smid=nytcore-ipad-share ("Mr. Obama Blamed North Korea for the [Sony] attack.").

11. *Id.*

12. *See generally* Jessica Lavery, *Which Is More Dangerous: Cause-Motivated or Financially Motivated Hackers*?, VERACODE (Feb. 27, 2015), http://www.veracode.com/blog/2015/02/which-more-dangerous-cause-motivated-or-financially-motivated-hackers.

13. Sieberg, *supra* note 8; *See also APT1: Exposing One of China's Cyber Espionage Units*, MANDIANT (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

14. *See* Brad Lunn, *Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine*, 4 J.L. & CYBER WARFARE 109, 131 (2014).

15. Tod Newcombe, *The Nation's Evolving Cyber-Security Issue: Are States Shoring up Their Defenses Enough to Protect Critical Data and Computer Infrastructure?*, GOVERNING (Dec. 2010), http://www.governing.com/topics/technology/nations-evolving-cyber-security-issue.html.

16. *See Cyberattacks on the Rise*, *supra* note 2.

advances, the resulting harm to corporations develops as well.[17] Corporations are not implementing enough cybersecurity measures to protect their data and sensitive information, and existing law does not create sufficient incentives for corporations and their Boards to take necessary precautions to protect sensitive information from cyberthreats.[18] To complicate the matter, corporations are reluctant to disclose cyberbreaches because of the impact on their reputation, their profitability, and due to fear of increased liability.[19]

Awareness and concern for data breaches must motivate companies to take action. Corporations need stronger incentives to implement more effective security measures and should be subject to greater resulting penalties for non-compliance.[20] Companies often fail to invest in cybersecurity because it is viewed as discretionary spending instead of a business imperative.[21] It is critical that Boards begin to treat cybersecurity as they would any other corporate concern. Indeed, a company may actually be thwarting its economic growth by not preparing for an inevitable cyberattack. In fact, a majority of consumers avoid doing business with corporations that fail to protect its cyberinformation.[22] The adverse economic effects of data breaches have not yet motivated the majority of corporations to prioritize prophylactic cybersecurity measures within their corporate governance.

The author asserts that existing legal doctrines can be adapted to address potential data breaches so as to require a Board to properly manage cybersecurity concerns. Moreover, information technology assessment should be incorporated into corporate governance. Modern courts have been reluctant to hold directors liable for a breach of their fiduciary responsibilities for oversight liability and have only recently begun to address cybersecurity issues.

Corporations have escaped liability for negligent data protection for

---

17. *See* BRUCE SCHNEIER, SCHNEIER ON SECURITY 227-30, 253-56 (2008); Steven Overly, *Cyber Attacks Present a Greater Risk to Firms as They Collect More Data about Customers*, WASH. POST (May 11, 2014), http://www.washingtonpost.com/business/capitalbusiness/cyber-attacks-present-a-greater-risk-to-firms-as-they-collect-more-data-about-customers/2014/05/11/ee861a90-d494-11e3-95d3-3bcd77cd4e11_story.html.

18. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1503 (2013); Gerry Smith, *New Law Would Force Companies Like Target to Report Hacks Quickly*, HUFFINGTON POST (Feb. 24, 2014, 5:59 PM), http://www.huffingtonpost.com/2014/02/24/companies-hacked_n_4848160.html.

19. *See* Lunn, *supra* note 14 at 112.

20. *See* Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, WHITE HOUSE BLOG (Aug. 6, 2013, 11:04 AM), http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

21. *Cyberattacks on the Rise*, *supra* note 2.

22. *10 Minutes on Data Privacy*, PwC (2014), *available at* http://www.pwc.com/us/en/10minutes/assets/pwc-data-privacy.pdf.

four reasons. First, chancery judges grant too much deference to the decisions of a corporation's Special Litigation Committee (SLC), often dismissing meritorious derivative claims alleging violations of the duty of care. Second, courts are confused about a Board's fiduciary duties as well as the extent of authority on oversight liability. Third, courts often misapply the Business Judgment Rule (BJR), permitting directors to hide behind lackluster security and risk assessment measures. Finally, courts have not yet had the opportunity to apply the concepts of the duty of good faith and the duty of loyalty to cybersecurity cases because courts have only recently clarified how these duties apply to oversight. The author challenges the chancery court's decision in *Stone v. Ritter*.[23] By framing oversight claims under the duty of loyalty, instead of under the duty of care, the court severely limited the likelihood that cyberoversight claims will succeed in the near future.[24] The author contends that the reason fiduciary oversight liability has failed to expand to the realm of cybersecurity stems from both intellectual dishonesty and from a general lack of cybersecurity understanding.

This Note proposes a reasonable solution to the data breach problem through a combination of enforcement of existing corporate legal principles, and continued shareholder pressure to scrutinize cybersecurity measures taken by a Board. The structure of this Note will first illustrate the intersection between corporate and cyberlaw as it pertains to cybersecurity and director fiduciary duties through the use of a hypothetical corporate Board. The author will then highlight both the negligence of the hypothetical board's response to a cyberattack, and the likely response of courts applying existing legal doctrines as they are currently and erroneously interpreted. The author will conclude with potential solutions through modification of existing law to appropriately address growing concerns, as well as review an appropriate Board response to a cyberbreach and explore lessons that can be learned for the future.

I. CASE STUDY: HYPOTHETICAL CORPORATION XYZ—THE BOARD SHOULD BE HELD LIABLE, BUT ESCAPES LIABILITY DUE TO INADEQUACIES IN THE LAW

XYZ is a successful corporation that owns some of the largest professional sports teams in the nation. The directors are aware of the need for appropriate oversight and the importance of spotting red flags

23. *See* Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362 (Del. 2006); *see also infra* Part III.D (explaining the evolution of the courts treatment of good faith).

24. *See infra* Part III.D (explaining that by reframing good faith as a duty of loyalty claim the courts limited the possibility of oversight claims).

for compliance issues. Cybersecurity issues, however, are not discussed at directors' meetings. Neither the risk committee nor the Board addressed information technology.

The corporation's network contains sensitive information about the athlete team members, including: credit card numbers, personal addresses, family members' addresses, birth dates and social security numbers. The CEO advised the directors that hackers have accessed the network and stolen confidential data for over 200,000 athlete-members. Further, the CEO noted that the network was also accessed between 5-7 times in the last few years, although nothing was technically stolen during that time period. XYZ never disclosed the previous breaches to the public, nor did the Board address it. When XYZ disclosed the recent attack in a newspaper article, its stock price dropped from $75/share to $40/share, and a number of its members decided to join a rival sports team management corporation, ABC.

Sammy Shareholder, of XYZ, brings a derivative action against XYZ alleging that the Board breached its duty of care and loyalty. Prior to bringing a derivative action, Sammy is required to make a demand on XYZ's SLC. The committee consists of outside directors who have business relationships with the Board. None of the SLC members have a risk management or assessment background. Further, all of the directors, both on the SLC and those that serve on the Board, have a very rudimentary understanding of the Internet, of the need to protect sensitive information, and of the increasing magnitude of data breaches. The SLC rejected Sammy's demand. The SLC determined that it would not be in the best interest of XYZ to sue itself. The SLC concluded that the directors had no reason to monitor intrusions into the network that did not result in any economic damage or harm to an individual.

The claim alleges a breach of fiduciary duty based on the theory that the decrease in share price adversely affected the value of every shareholder's XYZ stock. Sammy asserts that the Board failed to implement adequate security measures to protect the members' sensitive data. Sammy alleges that the company shielded the information from the shareholders and public in order to avoid an inevitable drop in stock price.

A court reviewed the allegations of Sammy's claim and determined that it should be dismissed with prejudice, consistent with the recommendation of the SLC. The judge determined that because no tangible damage occurred to the shareholders during the period prior to the attack, the directors did not act with gross negligence. Therefore, the Board was protected from liability by the BJR.[25] Additionally, the court found that the directors did not act in bad faith, or violate the duty of loyalty because when a data breach actually occurred, the directors

25. *See infra* Part III.C (giving a more in-depth analysis on the business judgment rule).

disclosed the incident, and took measures to handle the matter immediately.

II. CASE STUDY: THE WYNDHAM CORPORATION—A BOARD'S GUIDE TO AVOIDING CYBERSECURITY OVERSIGHT LIABILITY

Between 2008 and 2010, the Wyndham Hotels sustained three cyberattacks resulting in the loss of 600,000 customers' sensitive credit card data and personal information.[26] Prior to filing an action in court, the shareholder lodged a universal demand with the Board, insisting that the company resolve the fallout from the attack and hold those internally responsible for the damages to the corporation. The Federal Trade Commission (FTC) was also investigating the hotel, which successfully survived the effect of the investigation.[27] The SLC determined that the Board responded adequately to the FTC investigation, and when the shareholder made a demand, it recommended Wyndham dismiss the claim.[28] The Board unanimously refused to investigate the shareholders' demand on the SLC.

The plaintiff ultimately filed a derivative action alleging that Wyndham's Board breached the fiduciary duties of care and loyalty. The plaintiff's claim proceeded on two theories: (1) the company failed to implement adequate data security measures to protect customer's sensitive data, and (2) the company failed to disclose the breach and shielded this information from investors.[29] The case was dismissed with prejudice.[30]

The *Palkon* court reasoned that the BJR[31] appropriately shielded the Board from incurring liability from allegedly breaching its duty of care or duty of oversight.[32] The Board discussed the breaches at 14 separate meetings between 2008-2012 and the Audit Committee discussed the breaches in 16 additional meetings during this time period.[33] Additionally, the Board hired a third party technology firm to assess their information security procedures.[34] Further, the court determined that the

---

26. Palkon v. Holmes, No. 14-cv-1234, 2014 WL 5341880, at *1 (D.N.J. Oct. 20, 2014).
27. *Id.*
28. *Id.*
29. *Id.* at *2.
30. *Id.* at *7.
31. *See infra* Part III.C (giving a more in-depth analysis on the business judgment rule).
32. *Palkon*, 2014 WL 5341880, at *7.
33. *Id.* at *2.
34. *See* Goodwin Procter, *Breaches in the Boardroom: What Directors and Officers can do to Reduce the Risk of Personal Liability for Data Security Breaches*, BUS. LITIG. REP. (Feb. 6, 2015), http://www.goodwinprocter.com/Publications/Newsletters/Business-Litigation-Reporter/2015/February-2015-Business-Litigation-Corner.aspx?article=1.

directors did not act in bad faith since security measures existed when the first breach occurred and the Board had addressed data security concerns on numerous occasions.[35]

III. A HISTORY OF FIDUCIARY DUTIES IMPOSED ON A BOARD

There are various duties imposed on a Board to protect the corporation from harm, including: the duty of care, the duty of loyalty, the duty of oversight, and the duty of good faith.[36] While a Board's priorities and loyalties are always to its shareholders, a Board must also integrate social responsibility into its governance model.

Corporate law demands that directors of a corporation always acquire a rudimentary understanding of the business of the corporation.[37] Directors are not expected to be perfect, but they are expected to exercise reasonable care.[38] Board expectations are context-specific. Responsibility varies depending on the size of the corporation, the governance structure, and the type of work the corporation engages in.[39] However, there is one constant obligation imposed on the Board: the obligation to stay informed of the activities of the corporation.[40] Otherwise, a Board is not effectively "participat[ing] in the overall management of corporate affairs."[41]

The Model Business Corporations Act (MBCA) sets forth the appropriate conduct for directors. The MBCA requires that a Board act in the reasonable interests of the corporation, act in good faith, and be informed regarding its appropriate oversight responsibility.[42] Regarding the first requirement, reasonableness is determined by both a subjective and objective analysis.[43] Reasonability depends on what a Board actually believed, and is therefore partially subjective.[44] However, reasonableness is ultimately an objective analysis; the inquiry is: what would a reasonable Board do in a similar situation.[45]

---

35. *See Palkon*, 2014 WL 5341880, at *4.

36. Julian Velasco, *How Many Fiduciary Duties Are There in Corporate Law?*, 83 S. CAL. L. REV. 1231, 1232-33 (2010).

37. Francis v. United Jersey Bank, 432 A.2d 814, 821 (N.J. 1981).

38. *Id.* at 822.

39. *Id.* at 821.

40. *Id.* at 822.

41. *Id.*

42. *See* MODEL BUS. CORP. ACT § 8.30 (2002) (courts essentially holding directors accountable if there is a poor or unreasonable process that went into making a decision under the circumstances at the time of the decision).

43. Lunn, *supra* note 14, at 120.

44. *Id.*

45. *See id.* at 121.

Courts have implied that directors' responsibilities are not stagnant. Instead, they constantly evolve to maximize the best interests of the corporation.[46] Directors have a fiduciary relationship with shareholders.[47] Shareholders not only expect, but also assume that a Board will exercise reasonable supervision over the corporation.

A court will not hold directors personally liable even for violating their fiduciary duties, unless the violation caused harm to the corporation. In *Francis v. United Jersey Bank*, the former CEO's sons assumed responsibility for operating the corporation after the death of their father.[48] The sons borrowed corporate funds for personal use, failed to pay them back, thereby converting corporate funds into their own trust accounts.[49] During the entire time period, their mother, Mrs. Pritchard, was a majority shareholder and member of the Board. She claimed to be absolved from liability for her sons' actions due to her illnesses and old age.[50] The court opined that the Board should not incur liability unless the Board's actions are the proximate cause of the alleged harm.[51] In holding Mrs. Pritchard liable, the New Jersey Supreme Court reasoned that Ms. Pritchard proximately harmed the corporation because her duties "extended beyond mere objection and resignation to reasonable attempts to prevent the misappropriation of the funds."[52] The court identified a problem that plagues the modern corporate world - director nonfeasance presents "a much more difficult causation question" than director misfeasance.[53] Misfeasance is performing a duty in a wrongful manner; nonfeasance implicates the duty to become informed before a Board member takes any action or inaction.[54]

Courts have held directors personally liable in rare situations. For example, the corporate world was rocked by the decision of *Smith v. Van Gorkom*.[55] A shareholder brought a derivative action alleging that the Board failed to sufficiently evaluate the financial benefits of the merger.[56]

---

46. Lutz v. Boas, 171 A.2d 381, 396 (Del. Ch. 1961).
47. Loft, Inc. v. Guth, 2 A.2d 225, 238 (Del. Ch. 1938), *aff'd*, 5 A.2d 503 (Del. 1939).
48. Francis v. United Jersey Bank, 432 A.2d 814, 819 (N.J. 1981
49. *Id.*
50. *Id.* at 819-20.
51. *Id.* at 826.
52. *Id.* at 827.
53. *Id.* at 826.
54. *Id.* (emphasis added).
55. *See* Jacqueline M. Veneziani, Note, *Causation and Injury in Corporate Control Transactions: Cede & Co. v. Technicolor, Inc*., 69 WASH. L. REV. 1167, 1167 (1994); s*ee also Francis,* 432 A.2d at n.3 (stating that "Before Van Gorkom was decided, one commentator had stated that '[t]he search for cases in which directors . . . have been held liable in derivative suits for negligence uncomplicated by self-dealing is a search for a *very small number* of needles in a very large haystack.'" (citation omitted) (emphasis added)).
56. *See* Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. 1985).

The Board approved an offer with a three-day time limit for a cash-out triangular merger by a subsidiary corporation owned by the Pritzker Family.[57] The parent company would purchase all of Trans Union's shares at $55 a share.[58] The CEO chose this price without consulting outside market experts.[59] The market price per share at the time of the offer was $38.[60] The Trans Union shareholders favored the offer because it represented a premium of nearly $17.[61] Hence, an overwhelming majority of shareholders approved the merger.[62] The court found that the shareholders' approval did not justify the directors' breach because the shareholders were not informed of the facts regarding the directors' decision to approve a $55 buyout.[63]

The court concluded that the directors breached their fiduciary duties. The Board's actions were not made with "an informed basis, in good faith, and in the honest belief," that the merger was in the corporation's best interests.[64] The court reasoned that the directors failed to "inform themselves of all information reasonably available to them and relevant to their decision to recommend the Pritzker merger" and "disclose all material information that a reasonable stockholder would consider important in deciding whether to approve the merger."[65] The court made the following findings regarding the Board's behavior: it possessed a general lack of valuation information; the Board misled and mischaracterized a report by a financial expert who inflated the true cost of the shares, and finally, the Board failed to disclose to the shareholders that Van Gorkom chose the $55 price because it best suited his financial situation, which was not in the best interests of Trans Union's shareholders.[66] The decision is all the more stunning because it came from the Delaware Supreme Court, the leader of American corporate law.[67] The notion of a director incurring personal liability for monetary

57. *See id.* at 867.
58. *See id.* at 866.
59. *Id.*
60. *Id.* at 867.
61. *Id.* at 897.
62. *See Van Gorkom*, 488 A.2d at 897.
63. *See id.* at 868.
64. *Id.* at 872.
65. *Id.* at 872, 893.
66. *Id.* at 890-91.
67. Because most corporations are incorporated in Delaware, and its decisions are so powerfully influential in the realm of corporate governance, the author predominantly will focus on Delaware law. *See* Sean O'Sullivan, *Del. Courts Celebrated for Corporate Influence: Magazine Notes Chancery, Supreme Courts' Impact*, DELAWAREONLINE (Oct. 24, 2011, 12:03 AM), http://www.delawareonline.com/article/20111024/NEWS/110240330/Del-courts-celebrated-for-corporateinfluence?odyssey=tab%7Cmostpopular%7Ctext%7CFRONTPAGE ("No other state court impacts business law to such a profound degree.").

damages was a bombshell on corporations.[68]

A. *Doctrinal Flaw #1—Most SLC's Lack Cybersecurity Awareness, and Courts Provide too much Deference to Boards, Thereby Improperly Dismissing Necessary Derivative Actions*

A derivative action is a suit brought by a shareholder on behalf of the corporation for corporate recovery of damages or equitable relief arising from allegedly unlawful or improper conduct by directors, officers, or control persons acting under such authority.[69] The corporation is an indispensable party and is nominally served as the defendant to assure its appearance.[70] The corporation is the real party in interest and the shareholder is only a nominal plaintiff.[71] In a derivative action, the damages are recovered on behalf of the corporation. In effect, a shareholder brings suit on behalf of the corporation because the corporation refuses to bring the action against itself.[72]

The derivative action allows shareholders to protect corporate interests when the directors refuse to take corrective action.[73] A shareholder cannot bring a derivative proceeding unless it will promote justice and be in the best interests of the corporation.[74] As a matter of policy, however, there are many reasons why a corporation would not want to proceed with a derivative action. First, litigation is time-consuming and disruptive. Second, the resources a corporation expends on litigation are wasted if the case is likely to be dismissed. Finally, a derivative action may require that a corporation divulge confidential business information in open court that has been intentionally shielded from the public. While derivative actions serve an important role for corporate governance accountability, elucidating corporate wrongdoing, the downside of derivative actions is that they can be frivolous nuisance suits.

In addition, there are a number of procedural safeguards that a plaintiff must overcome in order to bring a derivative action.[75] First, a plaintiff must be a shareholder at the time when the allegedly damaging

---

68. Bayless Manning, *Reflections and Practical Tips on Life in the Boardroom After Van Gorkom*, 41 BUS. LAW. 1, 1 (1985).

69. 13 WILLIAM MEADE FLETCHER, FLETCHER CYCLOPEDIA OF THE LAW OF PRIVATE CORPORATIONS § 5939 (perm. ed., rev. vol. 2014).

70. *See id.* § 5941.10.

71. *See id.*

72. *See id.* § 5940.

73. *See id.* § 5949.

74. *See id.*

75. Mark J. Loewenstein, *The Quiet Transformation of Corporate Law*, 57 SMU. L. REV. 353, 362 (2004) ("[D]erivative actions are fraught with difficulties.").

transaction occurred.[76] Second, in a majority of jurisdictions complaints must make a universal demand, that is, the complaint must be verified by the court,[77] and allege with particularity the demand to a Board.[78] This requirement is designed to strike a fair balance between a shareholder's rights to assert a claim against a Board who fails to uphold its fiduciary duties and the corporation's right to appoint a Board to manage the critical decisions for the corporation.[79] A Board must decide whether to invest corporate resources in pursuit of a shareholder's allegation of corporate wrongdoing.[80] Thereafter, a Board has a reasonable time to respond, often 90 days, unless the corporation rejects the demand or the corporation will suffer irreparable injury if action is not taken swiftly.[81] Most claims rarely survive the demand stage.[82]

However, before a complaint reaches a court, a Board may consider forming a SLC to evaluate causes of action against the corporation.[83] These committees are made up of independent[84] and disinterested directors.[85] The SLC determines whether the lawsuit is in the "corporation's best interests."[86] The level of deference a court grants a corporation's SLC varies by jurisdiction. For example, courts in certain jurisdictions provide tremendous deference to the decision of the SLC; in other jurisdictions, the court independently scrutinizes the merits of the derivative action.[87] Most courts provide too much deference to the SLC's

---

76. *See* FLETCHER, *supra* note 69, § 5972.

77. Meaning a shareholder must demonstrate that he exhausted all the means within his reach to obtain redress of his grievances within the corporation itself.

78. *See id.* § 5963. *See also* MODEL BUS. CORP. ACT § 7.42 (2014).

79. *See* FLETCHER, *supra* note 69, § 5963.

80. *See id.*

81. *See id.* § 5967.

82. *See generally* Ann Scarlett, *Confusion and Unpredictability in Shareholder Derivative Litigation: The Delaware Courts' Response to Recent Corporate Scandals*, 60 FLA. L. REV. 589, 597-98 (2008). *See also* STEPHEN M. BAINBRIDGE, CORPORATION LAW AND ECONOMICS 362 (2002).

83. *See* Scarlett, *supra* note 82, at 598-99.

84. Legislatures typically fail to define the word "independent" in their corporate statutes.

85. *Id.* at 598.

86. Douglas M. Branson, *The Rule That Isn't a Rule—The Business Judgment Rule*, 36 VAL. U. L. REV. 631, 647–48 (2002) (dismissing a derivative action might increase stock price).

87. In New York, the plaintiff bears the burden of rebutting the deferential presumption of respect the SLC's, and judicial inquiry is limited. *See* Auerbach v. Bennett, 393 N.E.2d 994, 996, 1001 (N.Y. 1979). Some states also give deferential protection to an SLC recommendation but reverse the burden from plaintiff to defendant. *See, e.g.*, Hasan v. CleveTrust Realty Investors, 729 F.2d 372, 378–79 (6th Cir. 1984) (stating that a court should dismiss a derivative action upon an SLC's recommendation if the defendants show that they reasonably investigated, were independent, and acted in good faith); Lewis *ex. rel.* Citizens Sav. Bank & Trust Co., 838 S.W.2d 215, 224 (Tenn. Ct. App. 1992) (stating that a derivative action should be dismissed only after the court (1) finds that the committee was independent and (2) critically reviews the committee's findings to determine whether they are made in good faith, supported by the record of the

decision, resulting in dismissal of "the vast majority of cases."[88]

The first doctrinal problem in the hypothetical corporation is the composition of the SLC, and the court's improper analysis of the cybersecurity issues. Post Enron and Sarbanes-Oxley, it is poor corporate governance to not have a risk management or assessment team.[89] Moreover, in this age of technology, a corporation that handles sensitive information, such as XYZ from the hypothetical above, needs to have a Board with at least a basic understanding of data protection.[90] Many Board members and chancery judges grew up in a pre-digital era. If a Board lacks expertise in cybersecurity matters, then to remedy the information technology gap a Board should outsource these issues to a private data security firm or to attorneys with data breach compliance expertise. Following the bare minimum requirements is no longer acceptable corporate policy. Information technology is becoming increasingly embedded in overall corporate strategy. In order to bridge the information technology gap, affirmative efforts must be taken to become knowledgeable about cybersecurity.

Within a few years, a lack of Internet access and technology ignorance will doom those who "lament[ing] the decline of print media, longing for the good old days."[91] Many Baby Boomers are not comfortable with or proficient at using new computer technology. These typical Board members do not understand the importance of data encryption, cybersecurity, or firewalls. Cyberlaw represents a foreign environment for individuals who are trying to learn new languages of communication and understand the importance of cybereducation.[92]

Growth in the usage of the Internet and associated technology is continuously evolving; accessing the "Internet of Things" has transitioned from desktops to mobile devices.[93] However, Baby Boomers, who comprise most Boards, are reluctant to embrace technology. In contrast, Millennials consider technology to be an integral function of society. Almost 60% of Baby Boomers do not use a cell phone

---

investigation, and are consistent with the best interests of the corporation). In Delaware, by contrast, the defendant bears the burden, and the court may apply its own business judgment as to whether the case should be dismissed. Zapata Corp. v. Maldonado, 430 A.2d 779, 787–89 (Del. 1981).

88. Carol B. Swanson, *Juggling Shareholder Rights and Strike Suits in Derivative Litigation: The ALI Drops the Ball*, 77 MINN. L. REV. 1339, 1356–58 (1993).

89. *See* Lunn, *supra* note 14, at 114.

90. *See* Francis v. United Jersey Bank, 432 A.2d 814, 822 (N.J. 1981).

91. Ira Wolfe, *A Digital Divide Grows Between Baby Boomers . . . and Other Boomers?*, HUFF. POST TECH. (Sept. 11, 2012, 5:15 AM), http://www.huffingtonpost.com/ira-wolfe/baby-boomers-technology_b_1663751.html.

92. *Id.*

93. John Greenough, *The Internet of Everything: 2015*, BUS. INSIDER (Apr. 8, 2015, 5:01 PM), http://www.businessinsider.com/i nternet-of-everything-2015-bi-2014-12.

password.[94] Nearly 20% of those who use a password report that they fail to protect it.[95] The digital divide between Baby Boomers and Millennials may account for the absence of adequate corporate cybersecurity protection.

Additionally, the primary reason corporations create a SLC is to provide a gate keeping function. The SLCs prevent nuisance suits and wasting of corporate funds. However, most of the concerns the SLC is designed to prevent are absent from the hypothetical. Sammy Shareholder's allegations do not lack merit. In fact, the stock price dropped significantly when the company disclosed the hack that resulted in stolen information. Had the company taken adequate measures to disclose the cyberintrusions earlier or taken proactive measures to remedy the situation, a derivative action could have been avoided. Indeed, the ultimate drop in stock price would not have been so catastrophic.

Courts must carefully scrutinize a SLC's recommendation with regard to handling a derivative action. A claim alleging a breach of fiduciary duty for inadequate cybersecurity planning will inevitably survive the impenetrable SLC and withstand the procedural hoops of the motion to dismiss. The adverse effects and costs of doing business with a poor cybersecurity infrastructure will need to be internalized. The courts must force corporations to revamp their governance structure to account for information technology security. Furthermore, Boards must adapt and stay ahead of the digital divide by learning about the evolving cyberenvironment in order to prosper and remain competitive.

B. *Doctrinal Flaw #2: What are a Director's Fiduciary Duties Regarding Oversight in the Context of Cybersecurity? The Duties Remain Unclear, Since Courts have Avoided Addressing the Issue*

In Re: Caremark International, Inc. Derivative Litigation was a landmark decision that rejected old case law that shielded directors from personal liability for breaching their fiduciary duty of care. Caremark provided health care services to patients who were referred by physicians.[96] Federal law prevented corporations like Caremark from making referral payment arrangements with physicians.[97] Caremark was indicted for violating this law.[98] However, the court held that the evidence

94. *Baby Boomers Need to Become More Educated About Digital Security*, BUS. WIRE (Oct. 1, 2012, 6:00 AM), http://www.business wire.com/news/home/20121001005449/en/Baby-Boomers-Educated-Digital-Security#.VTfQLxPF9fx.

95. *Id.*

96. *In re* Caremark Int'l Inc., 698 A.2d 959, 962 (Del. Ch. 1996).

97. *Id.*

98. *Id.* at 963. It should be noted that Caremark took several steps upon notice of being

and facts in the record "did not support" the claim that defendants either "lacked good faith" in their oversight responsibilities, or "consciously permitted" the corporation to violate the law.[99] Previous cases protected directors from incurring liability. Boards could intentionally ignore learning about wrongdoing within the corporation.[100] The court engaged in a rhetorical debate that rejected the axiom "hear no evil, see no evil," for future directors seeking to avoid liability, in response to the holding from *Graham*:[101]

> Can it be said today that, absent some ground giving rise to suspicion of violation of law, that corporate directors have no duty to assure that a corporate information gathering and reporting systems exists which represents a good faith attempt to provide senior management and the Board with information respecting material acts, events or conditions within the corporation, including compliance with applicable statutes and regulations? *I certainly do not believe so*.[102]

The court's reasoning reflected a departure from outdated theories of duty of care and introduced the concept of "red flags" and oversight to the duty of care.[103] Although a Board has no duty to install and operate an elaborate system of espionage to ferret out wrongdoing which it has no reason to suspect to exist, "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."[104]

Caremark established the precedent that directors have a legal duty to not only create compliance programs, but also ensure that they are effective. This is particularly significant for directors in large diversified companies. Like the BJR, the duty to monitor is a judicially created standard, not codified in state statutes. For example, a director of a nuclear power corporation should be aware of the impact that dumping

---

investigated by the DOJ in 1992. Caremark essentially restructured its entire corporate policy and maintained both an internal audit and external audit committee. *See id.* Finally, Caremark increased management supervision. *See id.*

99. *Id.* at 972.

100. *Cf.* Graham v. Allis–Chalmers Mfg. Co., 188 A.2d 125 (1963).

101. *Id.* at 126 (holding that the plaintiff failed to show that any director had actual knowledge of anti-trust activities by corporate employees or any actual knowledge of any facts, which should have put them on notice that anti-trust activities were being carried on). The Court reasoned, "in [the] absence of knowledge of suspicious circumstances" the directors were not liable despite failing to take action designed to learn of and prevent the illegal activities). *Id.*

102. *Caremark*, 698 A.2d at 969 (emphasis added).

103. Lunn, *supra* note 14, at 122.

104. *Caremark*, 698 A.2d at 971 (emphasis added).

waste could have on a local river's ecosystem. The BJR will not shield a director who has not investigated or determined whether corrective action is needed when the company violates a chemical dumping law. Moreover, if the director allows this practice to persist for years, then he will not be afforded protection for his behavior. This director could be found liable under a breach of a duty of oversight.

As noted in dicta of Caremark, a claim of inadequate oversight is, "possibly the most difficult theory in corporate law upon which a plaintiff might hope to win a judgment."[105] Despite this reality, the author suggests that the same logic for director oversight can easily be extended to cybersecurity violations. With the frequency and magnitude of data breaches, it has become necessary for Boards to establish a risk management assessment procedure to help identify cyberattacks.

Identifying the doctrinal flaw from the hypothetical XYZ Corporation is a misunderstanding of the duty of care by both the Board and the court. Whether due to fear of litigation or because it is required by law, Boards will encounter growing cybersecurity threats. Legal responses to cybersecurity allegations should take the form of increased cybersecurity-oversight duties and the associated threat of potential liability. Compliance professionals should inform directors of the necessary steps to take to protect the company and its shareholders.

In view of the extensive damage that recent attacks have caused to major companies, a Board will no longer be able to hide behind its own ignorance. For example, in 2008 Heartland Payment Systems' (Heartland) was hacked, resulting in the loss of over 100 million individuals credit card and personal information, marking one of the largest data breaches in U.S. history.[106] Heartland paid legal fees owed to over 650 financial institutions including MasterCard, Discover and Visa, as well as costs related to the data breach, ultimately losing nearly $140 million.[107] Also, in 2011, Sony was the victim of a cyberattack. The Sony breach generated negative publicity for the company and illuminated the

105. *Id.* at 967.

106. Norah C. Avellan, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 200 (2014); *see also* Juliet M. Moringiello, *Warranting Data Security*, 5 BROOK. J. CORP. FIN. & COM. L. 63, 67-68 (2010); Rachael King, *Lessons from the Data Breach at Heartland*, BLOOMBERG (July 6, 2009), http://www.businessweek.com/stories/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice; Brian Krebs, *Payment Processor Breach May Be Largest Ever*, WASH. POST (Jan. 20, 2009, 1:30 PM), http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html (the Heartland Payment Systems breach, though immense, was not the first of its kind).

107. *See* Moringiello, *supra* note 106, at 68; Jessica Silver-Greenberg & Nelson D. Schwartz, *MasterCard and Visa Investigate Data Breach*, N.Y. TIMES (Mar. 30, 2012), http://www.nytimes.com/2012/03/31/business/mastercard-and-visa-look-into-possible-attack.html.

global impact of hacking.[108] The attack resulted in the loss of 77 million Sony customers' personal information internationally.[109] By failing to encrypt this information, Sony was a ripe target for an inevitable cyberattack.[110] Sony did not announce the breach immediately to its customers and shareholders.[111] Sony's stock value dropped a total of 7% following public disclosure of the magnitude and impact of the event.[112] Experts estimate that between the litigation-related expenses, the damage caused by the attack, and the necessary implementation of an identity theft program to prevent future attacks, it will ultimately cost Sony an estimated $10 billion.[113]

Finally, the most recent Target Corporation data breach highlights another important lesson for Boards and companies. Where Sony was unprepared for a cyberattack, lacking any type of security measures, Target allegedly had protections in place, but simply failed to react appropriately to the breach.[114] The breach not only resulted in lawsuits brought by customers and shareholders, but it also led to the resignation of Target's CEO.[115] The hackers remotely installed malware that targeted the processing system for Target's credit cards.[116] Although Target had

---

108. Lance Bonner, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 258 (2012).

109. *See* Nick Caplin, *PlayStation Network and Qriocity Outage FAQ*, PLAYSTATION BLOG (Apr. 28, 2011, 2:28 AM), http://blog.eu.play station.com/2011/04/28/playstation-network-and-qriocity-outage-faq/.

110. *See* Hunton & Williams LLP, *Gaming Security Breach: "Only on PlayStation*?," PRIVACY & INFO. SECURITY L. BLOG (Apr. 28, 2011), https://www.huntonprivacy blog.com/2011/04/articles/gaming-security-breach-only-on-playstation/.

111. Martyn Williams, *PlayStation Network Hack Timeline*, PCWORLD (May 1, 2011, 7:30 AM), http://www.pcworld.com/article/ 226802/playstation_network_hack_timeline.html; Dan Mitchell, *Yet Another Hack, Yet Another Delay in Reporting it*, FORTUNE (June 9, 2011, 7:57 PM), http://fortune.com/2011/06/09/yet-another-hack-yet-another-delay-in-reporting-it/ (noting that Sony and Citigroup both stalled for more than a week before formally disclosing to the public cyberincidents affecting their corporations); *see also* Patrick Seybold, *Update on PSN Service Outages*, PLAYSTATION BLOG (Apr. 20, 2011), http://blog.us.playstation.com/2011/04/20/ update-on-psn-service-outages-2/ (noting that Sony stated that it was "aware" its systems were offline, but did not offer its users a reason).

112. Avellan, *supra* note 106, at 201.

113. *See* Richard J. Bortnick, *"Anonymous" Hacks PlayStation Network and Sony Feels the Pain*, CYBER INQUIRER (May 6, 2011, 6:09 PM), http://cyberinquirer.com/2011/05/06/ "anonymous"-hacks-playstation-network-and-sony-feels-the-pain/.

114. *See* Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUSINESSWEEK: TECH. (Mar. 13, 2014), http://www.business week.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

115. Privacy Rights Clearinghouse, *Target Corp.*, PRIVACY RIGHTS CLEARINGHOUSE (Dec. 13, 2013), http://www.privacyrights.org/data-breach-asc?title=target+corp (last visited Oct. 25, 2014).

116. Andrea Peterson, *Secret Service Estimates Type of Malware that Led to Target Breach is Affecting 1,000 U.S. Businesses*, WASH. POST (Aug. 22, 2014), http://www.washingtonpost.

employed a cybersecurity firm that alerted Target to the presence of a potential and likely breach, Target failed to react swiftly and appropriately.[117] Between 70 and 100 million customers were affected by this breach.[118] Target's stock value decreased over 9% as a result of this breach.[119]

Despite the proliferation of cyberattacks, no derivative action brought by a shareholder against a Board for breach of cyberfiduciary duty has succeeded. In fact, no derivative actions or securities related data breach actions in the context of cybersecurity have survived a motion to dismiss.[120]

Current technology mandates that directors focus on the steps they take to ensure the protection of sensitive corporate data. The XYZ Board had no policy regarding cybersecurity risk management, and barely possessed a rudimentary understanding of technology, let alone data protection. Further, the XYZ Board had actual knowledge that its sensitive data may have been compromised, even if nothing was technically stolen. The failure by the Board to disclose this type of information to shareholders qualifies as a material misrepresentation.[121] The material misrepresentation standard asks "whether a reasonable investor [or shareholder in this case], in the exercise of due care, would have been misled by [the misrepresentation]."[122]

Cyberattacks are now a corporate reality. A Board should assume that data is being or will be compromised, and improve their security measures accordingly. A Board's lack of expertise on cybersecurity matters will soon no longer shield it from the requirement to implement a competent monitoring system. "Just as financial controls were not universally understood by directors, pre Sarbanes-Oxley and Enron, that

---

com/blogs/the-switch/wp/2014/08/22/secret-service-estimates-type-of-malware-that-led-to-target-breach-is-affecting-over-1000-u-s-businesses/.

117. *See* Riley et al., *supra* note 114.

118. Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES (Jan. 20, 2014), http://www.nytimes.com/ 2014/01/11/business/target-breach-affected-70-million-customers.html.

119. Dhanya Skariachan & Jim Finkle, *Target Shares Recover After Reassurance on Data Breach Impact*, REUTERS (Feb. 26, 2014, 1:52 PM), http://www.reuters.com/article/2014/02/26/us-target-results-idUSBREA1P0WC20140226.

120. *See In re* Heartland Payment Sys., Inc. Sec. Litig., No. 09-1043, 2009 WL 4798148 (D.N.J. Dec. 7, 2009); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942 (S.D. Cal. 2012); Miele v. Carr, No. 309-cv-04687, 2009 WL 5864279, at *1 (D.N.J. 2009); In re Target Corporate S'holder Derivative Litig., No. 14-cv-00203 (D. Minn. Jan. 21, 2014); Matrixx Initiatives, Inc. v. Siracusano, 131 S. Ct. 1309, 1317-18 (2011); Janus Capital Grp., Inc. v. First Derivative Traders, 131 S. Ct. 2296, 2301-03 (2011); Greenberg v. Crossroads Sys., Inc., 364 F.3d 657, 663-65 (5th Cir. 2004); *In re* Novatel Wireless Sec. Litig., 830 F. Supp. 2d 996, 1019 (S.D. Cal. 2011).

121. SEC v. Texas Gulf Sulphur Co., 401 F.2d 833, 862 (2d Cir. 1968).

122. *Id.* at 863.

lack of a firm grasp of financial controls did not mean that oversight was not required, but rather that the oversight lacked attention and expertise, which was later addressed through *regulation and litigation*."[123] Whereas a Board is not required to act perfectly, it must act reasonably under the circumstances. XYZ's Board did not act reasonably, and breached its fiduciary duty of care due to its failure to implement adequate cybersecurity measures.

C. *Doctrinal Flaw #3: Misunderstanding the BJR*

Investing in a corporation carries a number of assumed risks. Corporate law seeks to stimulate risk-taking, innovation, and entrepreneurship among Boards.[124] Shareholders expect that a Board will make sound business judgments in the best financial interests of the corporation. At the same time, scholars recognize the fundamental unfairness in praising a Board for favorable results, but criticizing a Board merely because their decisions led to undesirable results.[125]

The BJR creates a presumption that directors have acted in good faith.[126] It protects directors from liability for violating good faith, unless a plaintiff shareholder is able to overcome the presumption of good faith by proof of: conflict of interest, illegality, fraud, or bad faith.[127] Consequently, the plaintiff bears a heavy burden of proof to overcome the presumption.[128] Courts have found that a plaintiff overcomes the BJR only when gross negligence or other highly improper conduct by a Board can be proven.[129]

The BJR is *not* the rule of conduct; it is only a presumption of good faith, and not a presumption of compliance with the duty of care.[130] The

---

123. Lunn, *supra* note 14, at 114.

124. Experimental Economics Center, *Decision-Making Under Uncertainty—Basic Concepts*, ECONPORT, http://www.econport.org/econport/request?page=man_ru_basics4 (last visited Mar. 5, 2015); *see also*, Manuel Nunez Nickel & Manuel Cano Rodriguez, *A Review of Research on the Negative Accounting Relationship Between Risk and Return: Bowman's Paradox*, 30 OMEGA 1, 1 (2002), *available at* http://www.sciencedirect.com/science/article/pii/S030504830100055X.

125. Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984), *overruled by* Brehm v. Eisner, 746 A.2d 244 (Del. 2000) (indicating that it is a presumption that in making a business decision the directors act on an informed basis in good faith and in the honest belief that the action was in the best interests of the company).

126. *Eisner*, 746 A.2d at 261.

127. *See* Lori McMillan, *The Business Judgment Rule as an Immunity Doctrine*, 4 WM. & MARY BUS. L. REV. 521, 525 (2013).

128. Cede & Co. v. Technicolor Inc. (*Cede II*), 634 A.2d 345,361 (Del. 1993), *modified on other grounds*, 636 A.2d 956 (Del. 1994).

129. *Cede II*, 634 A.2d at 361

130. MELVIN EISENBERG, CORPORATIONS AND OTHER BUSINESS ORGANIZATIONS: CASES AND MATERIALS 544-49 (8th ed. 2000) (emphasis added).

rule of conduct that a Board must comply with is the duty of care. Although it would seem unlikely that a Board could have acted in good faith and failed their duty of care, the BJR does not protect against liability under duty of loyalty grounds.[131] The predicate for the BJR to apply is that the directors must make an informed business judgment.[132] A Board cannot hide behind the heavy presumption of the BJR if its directors do not make a rational business decision.[133]

Yet, why should a Board be entitled to such broad deference and a presumption that it acted properly? Judge Ralph Winter of the Second Circuit Court of Appeals defended the policy underlying the BJR in the acclaimed case of *Joy v. North*. First, Judge Winter reasoned that shareholders *voluntarily undertake the risk* of bad judgment, as they have chosen to invest in a company partly on the basis of its management.[134] Second, courts recognize that *after-the-fact litigation is an imperfect device* to evaluate corporate business decisions.[135] Finally, because potential profit often corresponds to the potential risk, overly cautious corporate decisions may ultimately harm shareholders.[136]

The proper application of the BJR remains misunderstood.[137] There is often a lack of consensus among the courts on the correct application of this rule.[138] As the nature and complexity of both corporate transactions and technology evolve, it will become more difficult to apply the BJR.[139] Finally, this rule touches at the heart of corporate governance - attempting to strike the ideal balance between directors' legal authority to manage the corporation and shareholders' right to hold a Board accountable for its actions.[140]

---

131. Stephen M. Bainbridge, *The Business Judgment Rule as Abstention Doctrine*, 57 VAND. L. REV. 83, 90 (2004).

132. *See Eisner*, 746 A.2d at 258; In re Caremark Int'l Inc., 698 A.2d 959, 968 (Del. Ch. 1996).

133. *See* Singer v. Magnavox Co., 380 A.2d 969, 975 (Del. 1977).

134. Joy v. North, 692 F.2d 880, 885 (2d Cir. 1982) (emphasis added).

135. *Id.* at 886; *see also* Bainbridge, *supra* note 131, at 114-15

> [T]here is a substantial risk that suing shareholders and reviewing judges will be unable to distinguish between competent and negligent management because bad outcomes often will be regarded, ex post, as having been foreseeable and, therefore, preventable ex ante. If liability from bad outcomes, without regard to the ex-ante quality of the decision or the decision-making process, however, managers will be discouraged from taking risks.

Id.

136. *North*, 692 F.2d at 886.

137. McMillan, *supra* note 127, at 526.

138. *Id.*

139. *See id.*

140. *Id.*

The third doctrinal problem identified in the hypothetical XYZ Corporation is a very common misapplication of the BJR. The XYZ Board cannot hide behind the favorable presumption that it acted in the best interest of the corporation. The Board failed to make an informed business decision, let alone a rational one. "Data security and information governance are increasingly part of the board-level communications as the centrality of information to enterprises continues to grow."[141] Cybersecurity is becoming ubiquitous in the United States, paired with abounding opportunities to incur potential liability.[142] XYZ's Board lacked a comprehensive cybersecurity risk management assessment procedure. The absence of these programs constitutes an egregious violation of its fiduciary duties, rising to the level of gross negligence. The author also contends that courts should presumptively find that a Board operated in bad faith for ignoring the practical realities of data breaches and cybersecurity.

Additionally, even if the judge in the hypothetical found that XYZ did not violate its duty of care, the judge allowed the BJR to subsume the duty of loyalty. The BJR only grants a presumption against breaching the duty of care and provides no protection for a Board that acts in bad faith. The judge's error closely resembles that of the court in *Shlensky v. Wrigley.*

In *Shlensky*, a shareholder brought a derivative action against the Wrigley Family's corporation, which owned the Chicago Cubs.[143] The shareholder alleged that the Cubs were losing profits because of a lack of stadium lighting, preventing the Cubs from playing night games.[144] The shareholder's theory alleged that this failure by the Board breached the duty of care.[145] The appellate court erred in affirming the lower court's denial of the motion to dismiss. "We are not satisfied that the motives assigned to [Wrigley] and through him to the other directors, are contrary to the best interests of the corporation and the stockholders."[146] "The decision is one properly before directors and the motives alleged in the amended complaint showed no fraud, illegality or conflict of interest in their making of that decision."[147]

The court in *Shlensky*, like the judge in the XYZ Corporation hypothetical, ignored the company's duty of care, and justified the Board's action based on the BJR. The rule is not a presumption against fraud, illegality, conflict of interest, or bad faith. It cannot be applied if

141. *See* Procter, *supra* note 34.
142. *Id.*
143. Shlensky v. Wrigley, 237 N.E.2d 776, 777 (Ill. App. Ct. 1968).
144. *See id.* at 776-77.
145. *See id.*
146. *Id.* at 780.
147. *Id.*

the directors do not properly make a decision with facts in front of them. Unlike the shareholder in *Shlensky*, Sammy alleged both a breach of duty of loyalty and breach of duty of care.

D. *Doctrinal Flaw #4: Misunderstanding of the Duty of Good Faith and Duty of Loyalty in the Context of Oversight Liability*

1. Duty of Loyalty

Another judicially created doctrine that underpins the confusion in resolving derivative actions is the duty of loyalty. The duty of loyalty, like the BJR, is not codified in any statute, but evolved from trust law.[148] The duty of loyalty is essentially a "boy scout oath" for a Board. Directors and officers are charged with the fiduciary duty to act in the best interests of the corporation at all times and not for their personal wealth.[149] This duty includes safely managing the corporation's assets on behalf of the shareholders.[150] It is critical to understand that the BJR does not protect a Board when a shareholder alleges a violation of the duty of loyalty.[151]

2. Duty of Good Faith

The Delaware Supreme Court attempted to clarify the confusion surrounding the various duties of a Board with respect to corporate governance. In *In Re Walt Disney Co. Derivative Litigation* (*Disney*), the court explored the uncharted waters of good faith and how it should be assessed in the context of a Board's other fiduciary duties. The court clarified that while gross negligence (including a failure to be properly informed of all available material facts) can establish a breach of duty of care, without additional wrongful conduct, gross negligence cannot constitute bad faith.[152] Although philosophically the concept of good faith overlaps with due care, these are two distinct legal duties in corporate law.[153]

The *Disney* court justified distinguishing a breach of fiduciary duty of care and bad faith by showing how merging good faith into the duty of care would undermine legislative intent. As a matter of good public policy and fairness, no corporate statute allows exculpatory provisions

148. *See generally* Guth v. Loft, Inc., 5 A.2d 503, 510 (Del. 1939).

149. Historically, the duty of loyalty was associated with situations involving a Boards' conflict of interest and the corporate opportunity doctrine.

150. *Id.*

151. *See, e.g.*, Brehm v. Eisner, 746 A.2d 244, 264 n.66 (Del. 2000). The business judgment rule only insulates a Board decision from judicial scrutiny as long as, a Board acts in good faith.

152. *In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 65 (Del. 2006).

153. *Id.*

for conduct that is exercised in bad faith.[154] However, exculpatory provisions do provide significant protection to directors for monetary liability arising from breach of the duty of care.[155] By converting bad faith into all violations of duty of care, exculpatory provisions would provide no protection and the BJR would be fruitless.[156] Therefore, the court ruled that bad faith is not gross negligence.[157] Acting in bad faith does not violate the duty of care.[158] The court articulated many scenarios that would constitute bad faith:

> A failure to act in good faith may be shown, for instance, where the director intentionally acts with a purpose contrary to advancing the best interests of the corporation, acts with the intent to violate the law, or intentionally fails to act in the face of a known duty to act, consciously disregarding his duties.[159]

However, the court did not discuss oversight liability.

IV. CURRENT STATE OF CORPORATE FIDUCIARY DUTIES

The Delaware Supreme Court in *Stone v. Ritter* confronted the difficult question *Disney* avoided addressing—whether a violation of the duty to act in good faith is a basis for the direct imposition of liability. The majority concluded that bad faith is a condition for director oversight liability.[160] The court reaffirmed *Disney*, but simultaneously clarified the conflict between the duties of care, good faith, and loyalty effectively overruling *Caremark*. The court held that because good faith is a "subsidiary element" of the duty of loyalty, the fiduciary duty violated by acting in bad faith is the duty of loyalty.[161]

Stone had a major impact on the corporate world. First, it reiterated the notion that the duties of good faith, loyalty, and care do not operate as a "triad of fiduciary duties." The obligation to act in good faith is not an independent fiduciary duty.[162] Second, the court greatly expanded the notion of the duty of loyalty beyond simply financial or personal conflict

---

154. DGCL § 102(b)(7) does not permit eliminating personal liability for breaches of the duty of care if the underlying acts or omissions were not in good faith. DEL. CODE ANN., tit. 8, § 102(b)(7)(ii)(2015).

155. *See generally id.*

156. *Disney*, 906 A.2d at 66-67.

157. *Id.* at 64-66.

158. *Id.* at 64.

159. *Id.* at 67.

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

161. *Id.* at 370.

162. *Id.*

of interest transactions and simultaneously limited oversight. The duty of loyalty now encompasses all cases, including allegations of oversight, where a Board acts in bad faith.[163] The decision implicitly challenged all Boards to restructure their corporate governance. Directors should no longer operate passively, waiting for red flags to arise. Directors should actively engage in information-gathering techniques to discover problems before they arise and implement preventive solutions.

There are now two bases upon which a plaintiff shareholder can bring an oversight claim.[164] First, by showing that a Board completely failed to establish an information or reporting system.[165] Second, by demonstrating that a Board consciously failed to oversee or enforce such a system.[166] For both scenarios, a plaintiff must prove that the directors were aware that they failed their fiduciary duties in order for a court to hold them liable.[167]

The doctrinal flaw reflected in the XYZ hypothetical demonstrates an application of bad faith. Despite the *Stone* ruling above, the author contends that whether an individual brings an oversight claim under breach of duty of care or duty of loyalty should be irrelevant to the analysis of the merits of a derivative cybersecurity claim against a Board. Today, systematic lack of data breach detection and prevention is bad faith in the cybersecurity context. Courts must not become consumed by form, but should instead focus on the substance of a claim. Boards like that of XYZ can no longer hide behind the BJR for such a conscious disregard of the best interests of the corporation. Boards now must take an active role in corporate information technology governance.

The XYZ Board erred in its disregard for the potential breaches. With the magnitude of cyberattacks and the fallout that results, defending on the grounds that no financial harm actually occurred is insufficient. Victims may not immediately feel intangible harm from the disclosure of sensitive material, such as credit card or social security information. However, the effects are devastating when analyzing the impact on the financial lives of the sports team members. The burden placed on the members includes dealing with the ramifications of identity theft. It may take years to clean up their credit history. Moreover, unlike a credit card, a victim of a stolen social security number cannot simply cancel their number and order a new social security card. The theft of a social security number by a hacker can carry grave repercussions.[168]

---

163. *Id.*

164. Rich *ex rel.* Fuqi Intern., Inc. v. Yu Kwai Chong, 66 A.3d 963, 981 (Del. Ch. 2013).

165. *Id.*

166. *Id.*

167. *Id.*

168. *See generally* Amber Newby, *The Consequences of Your Social Security Number Being Stolen*, BESTTIDTHEFTCOMPANYS.COM (Feb. 28, 2014), http://bestidtheftcompanys.com/2014/

Courts have tremendous influence over prevailing corporate governance practices.[169] Judges' opinions and commentary from scholars evaluating those opinions help shape norms and practices that ultimately influence Board behavior.[170] As courts continue to decide data breach cases, and as legal scholars assess the impact of these decisions, there will be a corporate governance cybersecurity metamorphosis. Only when judges begin speaking out about the importance of a Board's duty to monitor will the rest of society push to expand the scope of the duty to monitor.[171]

A. *Doctrinal Solution #1: Boards must Become Educated on Cybermatters, and Courts must Independently Scrutinize Derivative Actions and not Blindly Accept all SLC Recommendations*

In *Palkon*, Judge Chesler properly evaluated the Wyndham SLC's position that the shareholder derivative action be dismissed.[172] Unlike the judge in the XYZ Corporation hypothetical, Judge Chesler did not blindly adopt the SLC's findings. Instead, he opined that the committee's investigation had a predetermined conclusion,[173] specifically noting the numerous steps the Wyndham Board took to familiarize itself with the data breaches by discussing cybersecurity and risk assessment at numerous meetings.[174]

Due to the frequency of data breach stories in the news, directors will not be able to claim that they were "unaware of the risks posed to their [corporations] by cyberattacks."[175] Because of the limelight that

---

the-consequences-of-your-social-security-number-being-stolen.

169. Eric J. Pan, *A Board's Duty to Monitor*, 54 N.Y.L. SCH. L. REV. 717, 740 (2010).

170. *Id.*; *see, e.g.*, Myron T. Steele & J.W. Verret, *Delaware's Guidance: Ensuring Equity for the Modern Witenagemot*, 2 VA. L. & BUS. REV. 189 (2007) (highlighting the influence of Delaware judges' extrajudicial activities on corporate law and norms); E. Norman Veasey & Christine T. Di Guglielmo, *What Happened in Delaware Corporate Law and Governance from 1992-2004? A Retrospective of Some Key Developments*, 153 U. PA. L. REV. 1399, 1404-07 (2005) (arguing that "judges have had a substantial role in shaping best practices in corporate governance" and "speeches and articles by Delaware judges are often helpful in guiding boards and their counsel in the direction of best practices").

171. Pan, *supra* note 169, at 741.

172. *See generally* Palkon v. Holmes, No. 14-cv-01234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

173. *Id.* at *2

174. *Id.*

175. Steven L. Caponi, *Cybersecurity and the Board of Directors: Avoiding Personal Liability--Part I of III*, REUTERS (July 25, 2013), http://blogs.reuters.com/financial-regulatory-forum/2013/07/25/cybersecurity-and-the-board-of-directors-avoiding-personal-liability-part-i-of-iii/; Paul A. Ferrillo, *Cyber Governance: What Every Director Needs to Know*, HARV. LAW SCH. FORUM ON CORP. GOVERNANCE & FIN. REG. (June 5, 2014, 9:23 AM), http://blogs.law.harvard.edu/corpgov/2014/06/05/cyber-governance-what-every-director-needs-t o-know/.

cybersecurity is currently receiving, Boards should not be able to claim that an attack and the resulting harm was unknown.[176] The global state of cybersecurity now classifies corporations into two categories: "those who have been hacked, and those that don't know they've been hacked."[177]

In responding to a data breach or cyberattack, corporate officers and directors can learn a number of important lessons from the *Palkon* dismissal. The law places an affirmative obligation of oversight on directors to manage significant risks looming over a corporation's sensitive data.[178] A reasonable Board will hold meetings to address breaches or attacks on their sensitive data.[179] Boards that are unfamiliar with cybersecurity or data breaches would be wise to employ outside counsel for advice on limiting legal liability.[180] Finally, it is critical that a Board take necessary remedial measures to address a breach and minimize the harm that can result from exposure.[181] In light of the likelihood of a cyberattack, the appropriate time to address a cyberattack is before it occurs.[182] Boards can mitigate liability by having robust preventative policies and a response team in place in case a breach does occur.[183]

B. *Potential Solutions to Doctrinal Flaws #2, #3, and #4: Corporations Must Revamp Their Governance Structure to Account for Cybersecurity Concerns*

The tort law case *T.J. Hooper* demonstrates the reasoning directors should employ to implement protective measures to avoid incurring liability for data breaches.[184] In that case, a tugboat was caught in a vicious storm, which caused it to sink.[185] Although radio systems on boats were a recent technological development in the 1930s, radios were both relatively inexpensive and available.[186] Had the tugboat been equipped with a radio, the boat would have easily been able to receive warnings

176. Caponi, *supra* note 175.

177. *See* Nicole Perlroth, *Cybercriminals Zero in on a Lucrative New Target: Hedge Funds*, N.Y.TIMES (June 19, 2014, 5:16 PM), http://bits.blogs.nytimes.com/2014/06/19/cybercriminals-zero-in-on-a-lucrative-new-target-hedge-funds/?_php=true&_type=blogs &_r=0.

178. *Id.*

179. Jan P. Levine et al., *D&O's Best Defense Against Shareholder Demands Over Cybersecurity*, ADVISEN (Jan. 7, 2015), http://www.cyberrisknetwork.com/2015/01/07/dos-best-defense-shareholder-demands-cybersecurity/.

180. *Id.*

181. *Id.*

182. *Id.*

183. *Id.*

184. Lunn, *supra* note 14, at 118.

185. *See generally* T.J. Hooper v. N. Barge Corp., 60 F.2d 737 (2d Cir. 1932).

186. *Radio in the 1930s*, PBS.ORG, http://www.pbs.org/opb/historydetectives/feature/radio-in-the-1930s/ (last visited Nov. 23, 2015).

about the storm and avoid it.[187] The operator of the boat argued that he should not be liable because it was not industry standard to equip boats with radios at the time.[188] Judge Learned Hand rejected his argument, reasoning that any objectively reasonable tugboat operator would have a radio to receive weather reports.[189] Objective reasonableness of industry practices changes quicker than industry standards when a given industry is exposed to new technology because companies are opposed to higher costs, unbeknownst that a court will deem those costs reasonable.

The lesson from *T.J. Hooper* can be analogized to the world of cyberlaw and director oversight, because the technologies and risks associated with breach-related issues continue to evolve. Judge Learned Hand applied his famous formulation to determine what is reasonable in light of breach. If the burden (B) necessary to prevent a negative result is less than the probability of harm (P) multiplied by the likelihood (L) or gravity of harm, then the actions taken are not reasonable.[190] While no federal law currently penalizes a Board for the failure to implement cybersecurity measures (similar to the tugboat operator in *T.J. Hooper*), this fact should not relieve a Board from potential liability when it suffers a data breach.

Although not a "cybercase," a recent decision from the Third Circuit Court of Appeals provides a cautionary regulatory tale for Boards.[191] *Lemington* sets forth a warning for all fiduciaries that recognize governmental and organizational risks but fail to address them adequately.[192] In *Lemington*, a non-profit nursing home sought bankruptcy protection and closed because of service deficiencies and financial troubles.[193] A committee of unsecured creditors filed an action against the directors claiming breaches of fiduciary duties of loyalty and care.[194] The Third Circuit found that the directors and officers failed to exercise reasonable care in allowing the fiduciaries to remain in office after their mismanagement became clear.[195]

The court was particularly perturbed by the fact that the Board sought and obtained a $178,000 grant to replace the current administrator and despite repeated knowledge of the administrator's poor performance the

187. *See generally Hooper*, 60 F.2d at 737.

188. *See id.* at 739.

189. *Id.* at 740.

190. United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

191. *See generally In re* Lemington Home for the Aged, 777 F.3d 620 (3d Cir. 2015).

192. Richik Sarkar, *A Cautionary Cyber-Liability/Regulatory Tale for Boards, Officers, and Directors*, BUS. ADVOC. (Mar 26, 2015, 12:54 PM), https://businessadvocate.mcdonaldhopkins.com/Data-Privacy-Solutions/2015/03/26/lemington.

193. *Id.*

194. *Id.*

195. *Lemington*, 777 F.3d at 626.

Board simply never utilized the funds for that purpose.[196] Additionally, the directors concealed the Board's decision to deplete the patient census and close the home for over three months.[197] Finally, during the bankruptcy process, the Board "failed to disclose in its monthly operating reports that the Home had received a $1.4 million Nursing Home Assessment Tax Payment . . . [which] damaged the Home's financial viability after it had become insolvent."[198] The court specifically noted, "[t]his [was] not a case where directors, acting in good faith reliance on information and reports prepared by others, made a rational business decision."[199] Rather, the directors had "actual knowledge of mismanagement, yet stuck their heads in the sand in the face of repeated signs that residents were receiving severely deficient care."[200] *Lemington* is an example of the legal analysis that courts must conduct when a valid cybersecurity allegation is brought against a Board for breach of fiduciary duty.[201]

This Note argues that a Board cannot wait to take action until the corporation is attacked, but instead it has an affirmative obligation to stay informed so that it can take preventative measures. The failure to recognize red flags in a corporation's data security measures, such as a potential intrusion, unusual activity, or even a virus, should not *per se* establish a violation of a Board's fiduciary duties. However, a failure to implement a reasonable system to understand the warnings and resolve them in a manner to protect the best interests of the corporation should form the basis for gross negligence and constitute bad faith. A detection system for red flags is only the first step in ensuring good information technology compliance to avoid liability. The risk management system implemented by a Board must be designed with teeth, meaning it is no longer sufficient to just identify potential breaches and disclose them. The lesson from *Palkon* is that despite an increased fear of a flood of cybersecurity oversight liability claims, a Board *can* be hacked and still act reasonably and be entitled to the protections of the BJR, as long as a Board proves it treated cybersecurity as seriously as any other typical issue within corporate governance.[202]

The extent of "reasonable" cybersecurity measures necessary to protect data will depend on the size and value of the data, the financial capabilities of the corporation, and the impact of previous attacks.[203] The

196. *Id.* at 629.
197. *Id.* at 630.
198. *Id.* at 630-31.
199. *Id.* at 629.
200. *Id.* at 630.
201. Sarkar, *supra* note 192.
202. *Id.* (emphasis added).
203. Lunn, *supra* note 14, at 132.

reasonableness of a Board's actions to avoid liability for oversight may change daily in the cybersecurity context;[204] "what is sufficient oversight [one day] may quickly become obsolete [the next]."[205] Therefore, a Board must be proactive in addressing cybersecurity issues.

Despite the seemingly uncontrollable and evolving nature of cybermatters, corporations must begin to recognize that information technology risks are at least as important as any other business risks that a Board may face.[206] A Board can implement a number of measures to help survive a derivative claim brought by a shareholder alleging a breach of fiduciary duty for cybersecurity oversight. Along with preventive measures, Boards must also focus on damage control following an attack. These measures are also consistent with good corporate governance.

First, similar to the formula from *T.J. Hooper*, Boards must apply a general cost benefit analysis to cybersecurity. As previously demonstrated, the probability of a cyberattack is great, and it is accepted that serious harm will result from such an attack. "You can't open a newspaper or visit an online news site these days without some mention of a cyberattack or data breach."[207] Therefore, Boards must implement a risk management component to corporate governance. "If the loss probability multiplied by the loss event value exceeds the burden (mitigation costs) such mitigations should be implemented."[208] A Board's policy must not only be highly responsive to red flags, but must also be so that the directors are constantly educated about cyberbreaches.

Second, if a corporation has previously suffered a cyberattack, directors are not only on notice, but are also expected to be absolutely vigilant in protecting the company in the future. The author acknowledges that after one attack, it may be difficult to thwart another. If an attack is so novel that even computer security experts could not have anticipated it, absent further negligence, a corporation should not be found liable.[209] However, courts should closely scrutinize Board action both prior to and after an attack.

Third, Boards must restructure corporate governance to give cybersecurity the same emphasis as generating profit.[210] Companies should be encouraged to create bylaws or amend current bylaws to outline

---

204. *Id.* at 131.

205. *Id.*

206. Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility For Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L. 313, 317 (2011).

207. Bit9, *Breach Preparation: Plan for the Inevitability of Compromise*, INFO. WK. (Apr. 1, 2015), http://www.informationweek.com/whitepaper/Security/Vulnerabilities-and-Threats/breach-preparation-plan-for-the-inevitability-of-wp1428441540?articleID=200001188.

208. Lunn, *supra* note 14, at 133

209. John A. Fischer, *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215, 231 (2013).

210. Caponi, *supra* note 175.

the scope of a Board's responsibility in relation to cybersecurity. One expert analogized that "[a] robust and resilient cybersecurity system must be regarded similarly to the physical locks on the doors of a brick-and-mortar building."[211] Some technical measures include encrypting confidential information, and creating firewalls or storing the confidential data separately from the rest of the financial systems.[212] As a matter of simple good corporate governance, a Board should encourage regular discussions of and document cybersecurity measures and potential issues that will inevitably arise.[213] Two standards the author suggests are likely to help a Board survive a breach of fiduciary claim are: creating an independent committee composed of outside directors to assess cyberattacks, and outsourcing the management of data protection to a private cybersecurity firm.[214]

V. TRANSFORMING THE SEC DISCLOSURE GUIDANCE INTO FEDERAL LAW AND TRANSFORMING SOCIETAL VIEWS ABOUT CYBERSECURITY

Despite the seriousness and gravity of harm that a cyberattack can exact upon a corporation, the existing SEC rules and regulations do not require disclosure of attacks.[215] Existing law also does not extend liability to directors as a deterrent or provide positive incentives like exemption from liability to force corporations to internalize the cost of doing business.[216] Most commentators and scholars anticipated that the adverse publicity of data breach incidents against large companies would encourage "proactive corporate disclosure [and remedies] for cyberattacks.[217] In a 2009 survey, almost 40% of Fortune 500 companies did not mention cybersecurity in their SEC filings, despite the fact that *90% of companies are breached in a given year*.[218]

Most corporations fail to mention data breaches for fear of reputational damage.[219] The disclosure of data breaches to the public may harm a corporation's future growth capacity, strategic market position, brand, ability to raise capital, and relationship with its customers and

211. Avellan, *supra* note 106, at 225.

212. Pessin Katz Law, *Cybersecurity Breach: Are Board Members at Risk?*, ABOVETHELAW (Apr. 21 2015, 3:27 PM), http://abovethelaw.com/2015/04/cybersecurity-breach-are-board-members-at-risk/.

213. *Id.*

214. *Id.*

215. Sam Young, *Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches*, 38 J. CORP. L. 659, 668 (2013).

216. *Id.* at 676-78.

217. *Id.* at 667.

218. *Id.* (emphasis added).

219. *Id.*

suppliers.[220] Recognizing this growing harm, Senator John D. Rockefeller and other members of Congress wrote a letter to the SEC Chairwoman seeking clarification regarding a corporation's duty to disclose a cyberattack.[221] In October 2011, the SEC responded with disclosure guidelines on obligations that corporations should consider when determining whether to disclose a cybersecurity breach,[222] including: risk factors, management's discussion and analysis of financial condition and results of operations (MD&A), description of business, legal proceedings, financial statement disclosures, and disclosure controls and procedures.[223] Unfortunately, the guidelines are not official "rule[s], regulation[s], or statement[s]" of the SEC.[224]

The author asserts that the primary reason that the SEC has not transformed the guidelines into rules stems from prevailing ignorant views of cybersecurity as an externality. An externality is an outside source that has an external effect on the market.[225] Positive externalities occur when an activity generates external benefits that an actor cannot internalize, such as through prices; "[n]egative externalities occur when one's activity imposes costs on others" that likewise are not transmitted through prices.[226] An externality can thus be viewed as a market failure.[227] The government often responds to a negative externality by discouraging the responsibility through taxation or regulation, whereas the response to a positive externality is to encourage the conduct, often through subsidies.[228]

Cybersecurity is often understood in this context.[229] When a corporation suffers an intrusion, the harm rarely falls directly on the corporation. Instead, the costs are borne by third parties. This in turn represents a negative externality, like pollution. Pollution was ignored as a problem until everyone felt the effects globally. Similar to the effects of pollution, a corporation does not shoulder the costs associated with data breaches and cybersecurity.[230] "What is needed, though, is a cultural

220. *Id.*

221. *Id.* at 667-68

222. *Id.* at 669.

223. *Id.*

224. *Id.*

225. Niva Elkin-Koren & Eli M. Salzberger, *Law and Economics in Cyberspace*, 19 INT'L REV. L. & ECON. 553, 563 (1999).

226. *Id.*

227. Sales, *supra* note 18, at 1520.

228. *Id.*; *see also* Christopher J. Coyne & Peter T. Leeson, *Who's to Protect Cyberspace*?, 1 J.L. ECON. & POL'Y 473, 476 (2005); Paul Rosenzweig, *Cybersecurity and Public Goods: The Public/Private "Partnership*," HOOVER INST. 2 (2011), *available* at http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf.

229. Sales, *supra* note 18, at 1520.

230. Avellan, *supra* note 106, at 215.

shift where those in control of large corporations no longer view cybersecurity as an obligation imposed by the government, and instead as a necessity."[231] Therefore, without some outside force requiring corporations to reduce the incidence of data breaches and improve cybersecurity measures, a corporation simply will not do so.[232]

VI. INFORMATION TECHNOLOGY AND CYBERSECURITY INSURANCE

Cybersecurity liability and privacy insurance are new forms of professional insurance that can cover issues not traditionally resolved by legal principles.[233] The policies are designed to cover the costs of combating first and third party breaches. Coverage includes suits for damages suffered by the company from other third parties like customers for the exposure and loss of sensitive data when hackers infiltrate a company's system and cause significant damage, and the cost of data recovery and restoration (especially when an attack causes system disruption and the losses associated with being offline).[234] While literature abounds regarding cybersecurity insurance, a further discussion of cyberinsurance as the proper the solution to limiting cyberfiduciary liability is beyond the scope of this Note.

VII. A HOPEFUL FUTURE FOR CYBERSECURITY—THE AMERICAN BAR ASSOCIATION (ABA) & CYBERSECURITY INFORMATION AND SHARING ACT (CISA)

The ABA adopted a resolution in 2013 creating sanctions for unauthorized and illegal intrusions into computer networks.[235] The resolution highlighted the increasingly important issue of information security for attorneys.[236] Breaches expose clients to significant economic losses that greatly undermine the legal profession by diminishing the client's confidence in the attorney-client relationship.[237]

In 2015, it was essential that attorneys stay abreast of cybersecurity

---

231. *Id.* at 225.

232. *See generally* Scott H. Segal, *Blowin' in the Wind: Early Indications of a Clinton Climate Policy*, 24 ST. B. TEX. ENVTL. L. J. 43 (1993).

233. Trautman & Altenbaumer-Price, *supra* note 206, at 337.

234. *Id.*

235. *See generally* American Bar Association (ABA), *Resolution*, AMERICAN BAR ASSOCIATION (2013), http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf.

236. *See id.*

237. *See id.*

practices.[238] Continuing Legal Education (CLE) programs on cybersecurity issues have become commonplace. These CLE's provide insight into the most current cybersecurity information and strategies.[239] Like Boards, lawyers who ignore cyberthreats risk millions of dollars for their clients.[240]

While the courts and Boards may be hesitant to take swift action to respond to the growing number of computer security breaches, the Legislature is beginning to take action. In the spring of 2015, the House passed a cybersecurity measure that would encourage companies to share their computer records and network access with the federal government.[241] Paul Kurtz, a cybersecurity and information sharing expert who worked under three presidential administrations stated, "[t]he gravity of the emergency we have in cyberspace is setting in with lawmakers;" corporations can no longer combat cyberattacks individually.[242] The House bill would provide corporations legal liability protection if they participate in the program and share cyberthreat information with the government.[243]

To satisfy First Amendment privacy concerns, and persuade wary corporations, the government provides the liability protection only after the corporation's personal information data is essentially screened out, once by the corporation and then by a government agency before any information is transferred.[244] To stress the gravity of the situation, during the passage of the House Bill, one politician noted, "[w]e are under attack as I speak; [t]o do nothing is not an option."[245]

On October 27, 2015, the Senate finally approved a cybersecurity bill known as CISA.[246] CISA has been described as a "voluntary threat

---

238. Georgetown Law, *Cybersecurity Law Institute*, CONTINUING LEGAL EDUCATION (May 5, 2014, 10:32 AM), https://www.law.georgetown.edu/continuing-legal-education/programs/cle/cybersecurity/.

239. *Id.*

240. *Id.*

241. Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015); *see also* Jennifer Steinhauer, *House Passes Cybersecurity Bill After Companies Fall Victim To Data Breaches*, N.Y. TIMES (Apr. 22, 2015), http://www.nytimes.com/2015/04/23/us/politics/ computer-attacks-spur-congress-to-act-on-cybersecurity-bill-years-in-making.html?smprod=nytcore-ipad&smid=nytcore-ipad-share; Mark S. Nelson, *House Passes First of Two Cybersecurity Bills on Tap this Week*, SEC TODAY, Apr. 23, 2015, at 1.

242. Steinhauer, *supra* note 10.

243. *Id.*

244. *Id.*

245. *Id*.

246. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015); Nicole Perlroth & David E. Sanger, *Senate Approves a Cybersecurity Bill Long in the Works and Largely Dated*, N.Y. TIMES (Oct. 27, 2015), http://www.nytimes.com/2015/10/28/us/ politics/senate-approves-cybersecurity-bill-despite-flaws.html?_r=0; Rajesh De et al., *U.S. Senate Passes Cybersecurity Information Sharing Act*, BNA (Nov. 4, 2015), http://www.bna.com/us-senate-

information-sharing vehicle," by which governmental agencies and companies in the private sector share and exchange information about hackers' methods of attack, as well as provide risk alerts.[247] In theory, CISA seems like a great step in the right direction. However, what is controversial about this bill is that it includes liability protection for private companies who participate, essentially shielding them from lawsuits for sharing their data.[248]

Naturally, there is a support and opposition concerning the implications of CISA. Stakeholders and privacy advocates, including the American Civil Liberties Union (ACLU), fear that the National Security Agency (NSA) will abuse CISA and engage in warrantless searches to obtain information from citizens unconnected to cybersecurity threats.[249] Greg Nojeim, a senior counsel at the Center for Democracy and Technology, believes the bill is a "backdoor wiretap" for the authorization of sharing sensitive data that have nothing to do with cybersecurity.[250] On the other side of the debate are stanch proponents of national security and those who recognize the growing threat of cyberwarfare. Rajesh De, former general counsel of the NSA astutely noted, "[i]f you took the position that no single thing solves the problem, then you would never do anything . . . [y]ou have to start with something."[251]

The author agrees more with the proponents of the bill, but shares some major concerns about its utility and effectiveness. Liability protection could serve an effect opposite of that intended by the drafters and proponents of CISA—it could discourage companies from investing in cybersecurity. It is also possible that CISA could have a negative cascading effect, reducing competition by making business too expensive to conduct for small businesses since they would need to invest money into cybersecurity defense on the same scale as large corporations. Most cybersecurity experts agree that the bill focuses on a diminishing form of defense, collecting and sharing cyberattack signatures.[252] However, the author proposes that CISA's fatal flaw is that it fails to set a threshold requirement for the implementation of cybersecurity standards. Until society forces companies to bolster their cyberdefenses and focus on remedial solutions to hacks rather than emphasizing detection, cybersecurity will continue to be a free rider problem and operate very much like pollution—when society decides to act, it will be too late.

---

passes-n57982063139/.

247. Perlroth & Sanger, *supra* note 246.

248. *Id.*

249. *Id.*

250. *Id.*

251. *Id.*

252. *Id.*

CONCLUSION

A Board has an obligation to fulfill its duties of care and loyalty in good faith and in the best interest of the corporation. It is only a matter of time before corporate directors are held accountable for cybersecurity oversight. The author believes that reasonably well-informed directors recognize cybersecurity risk to corporate value. The author demonstrated that even if the Courts were to properly reframe oversight as a duty of care issue, procedural devices such as demand, the SLC, and the BJR create obstacles to meritorious shareholder derivative cybersecurity oversight claims alleged as violations of the duty of care.

Stone severely curtailed the viability of cybersecurity oversight claims. Through faulty transitive logic—the *Stone* court reasoned that bad faith falls into the duty of loyalty: *Stone* determined that most oversight claims allege bad faith. Therefore, *Stone* held that oversight claims necessarily must be brought as a breach of the duty of loyalty.

A Board should be aware and proactive in oversight, not idle until a corporation suffers a cybercatastrophe. Whether the shareholder claim is classified as duty of care or duty of loyalty should be irrelevant to a court's analysis. If a Board utterly fails to create an information system with respect to cybersecurity or systematically disregards cybersecurity red flags and as a result the corporation suffers, the directors violated their fiduciary duties. Rather than becoming consumed with which fiduciary duty a Board violated, as a matter of policy and fairness, courts should focus on the merits of claims and hold directors who fail to incorporate cybersecurity into corporate governance liable for lackluster cybersecurity measures.