THE FIDUCIARY DUTIES OF THE BOARD OF DIRECTORS: CYBERSECURITY POTENTIAL LIABILITY AND PREVENTATIVE ACTIONS

Brennan Ackerman [*]

ABSTRACT

Cyber breaches are an increasingly serious threat faced by corporations. Following a cyber breach, stockholders of a corporation can, in theory, sue the corporation's board of directors for a breach of fiduciary duties. In Delaware, plaintiffs must meet a high threshold to prevail in such suits. At the same time, the duty of a board of directors in relation to cybersecurity is a relatively new and untested area of the law. Courts have yet to set forth a clear safe harbor from liability.

To date, case law suggests that courts expect the board of directors to be informed of and involved in the corporation's cybersecurity framework. Courts have failed to specify how frequently a board must take cybersecurity into consideration. However, dicta suggest it is necessary that cyber breaches be discussed by the full board of directors. Periodic updates to a board regarding the state of a corporation's cybersecurity framework as well as any new risks may be also required.

Courts appear to show deference to directors in judging the adequacy of the actions taken by them to prevent a cybersecurity breach when the corporation has a clearly defined plan and reporting chain for cyber breaches.[1] A reporting system should clearly define the different levels of reporting and the specific information which will be alerted to each level of the chain. A board of directors should conduct discussions with individuals within the corporation whom are tasked with overseeing the corporation's cybersecurity framework. While there are many actions which could be taken by the board in an effort to advance the corporation's cybersecurity framework, no specific action will completely shield the

* Brennan Ackerman is a graduate of Wayne State University Law School. He currently practices as an associate attorney in business contracts, municipal, and school law at Thrun Law Firm.

[1] Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014); *In re* Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016).

board from liability. According to experts, factors that courts will consider when assessing a board's liability include organizational structure, budgetary review, board education and third-party audits.

INTRODUCTION

Cybersecurity has become a prominent issue for corporations with the increasing number of cybersecurity attacks. According to former FBI Director James Comey, "[t]here are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked…"[2] Given the importance of this issue, boards of directors have a significant role to play. Former Commissioner of the U.S. Securities and Exchange Commission ("SEC"), Luis Aguilar, noted in a 2014 speech addressed to the New York Stock Exchange that "[b]oard oversight of cyber risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks."[3] The purpose of this article is to address the cybersecurity-related duties and responsibilities of individuals who serve on boards of directors for Delaware corporations.

During the last five years, there has been five lawsuits filed against the boards of publicly traded corporations following cyber breaches; these corporations include: Wyndham Hotels, Target, Wendy's, Yahoo and Home Depot.[4] As claimed in the lawsuits to date, members of the board of directors may be liable to shareholders for violating their fiduciary duties following a cyber breach. Shareholder lawsuits are typically filed after a regulatory investigation or class action claim from customers or employees and come in one of two forms: on behalf of themselves (direct) or on behalf of the company (derivative). Derivative suits allege that under the board's supervision the corporation failed to take reasonable steps to prevent a data breach. In *Tooley v. Donaldson*, the Delaware Supreme Court stated that to determine whether a lawsuit is direct or derivative, the court must determine "who suffered the alleged harm (the corporation or the suing stock-holders,

---

[2] James Cook, *FBI Director: China Has Hacked Every Big US Company*, BUS. INSIDER (Oct. 6, 2014, 6:24 AM), http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10.

[3] Luis Aguilar, Comm'r, Sec. and Exch. Comm'n, Address at the New York Stock Exchange: Cyber Risks and the Boardroom (June 10, 2014), https://www.sec.gov/news/speech/2014-spch061014laa.

[4] Joseph Crace Jr. & Virgina Yetter, *When Does Data Breach Liability Extend to the Boardroom*?, LAW360 (April 3, 2017, 12:43 PM), https://www.law360.com/articles/907786.

individually), and who would receive the benefit of any recovery or other remedy (the corporation or the stock-holders, individually)?"[5] To maintain a direct claim, "[t]he stockholder's…injury must be independent of any alleged injury to the corporation. The stockholder must demonstrate that the duty breached was owed to the stockholder and that he or she can prevail without showing an injury to the corporation."[6] Therefore, in cyber breaches, stockholders would not be able to file a direct lawsuit based on a drop in the price of the company's stock, but could potentially sue derivatively on behalf of the corporation arguing that the entity's stock or assets were diminished as a result of the interruption of business, legal costs, reputational damages, etc.[7]

Under Delaware's corporate law, boards of directors owe two fiduciary duties to the corporations they serve: duty of care and duty of loyalty.[8] Other duties sometimes referenced in the cybersecurity context, such as the duty of disclosure, are derived from the duties of care and loyalty.[9]

In evaluating whether directors have met their duties, Delaware courts have shown deference to boards resulting in a high bar for plaintiffs to demonstrate that board members breached either their duty of care or duty of loyalty.[10] In regard to cybersecurity, this has continued to hold true. For instance, courts do not expect a board of directors to take actions to completely eliminate the risk of a cyber breach taking place.[11] To date, no courts have found a director to have breached his or her fiduciary duties following the occurrence of a cyberattack.

DUTY OF CARE

[5] Tooley v. Donaldson, 845 A.2d 1031, 1033 (Del. 2004).
[6] *Id.* at 1039.
[7] Pate v. Elloway, No. 01-03-00187-CV, 2003 WL 22682422, at *2 (Tex. App. Nov. 13, 2003) (stating "[t]o have standing to assert a direct or individual claim, a stockholder must allege an injury that is separate and distinct from other stockholders . . .") (applying Delaware law).
[8] *See* Stone v. Ritter, 911 A.2d 362, 369-70 (Del. 2006).
[9] *See* William M. Lafferty et al., *A Brief Introduction to the Fiduciary Duties of Directors Under Delaware Law*, 166 PENN ST. L. REV. 837 (2012).
[10] *Id.*
[11] Michael R. Overly & Chanley T. Howell, *Common Cybersecurity Myths Debunked*, CSO (June 25, 2015), http://www.csoonline.com/article/2939517/data-protection/common-cybersecurity-myths-debunked.html (discussing how studies show that businesses would need to increase their overall security budget nine-fold to address 95% of the cyber threats they face).

A director's fiduciary duty of care involves exercising reasonable business judgment and using ordinary care and prudence in the fulfillment of his or her duties. The fiduciary duty of care is examined under the "business judgment rule."[12]

BUSINESS JUDGMENT RULE

The business judgment rule is derived from section 141(a) of the Delaware General Corporation Laws ("DGCL"), which states the "business and affairs of every corporation organized under this chapter shall be managed by or under the direction of a board of directors."[13] Accordingly, Delaware courts have consistently given deference to the decisions made by a board of directors, respecting its' right to govern a corporation independently from the stockholders. The Delaware Supreme Court held the business judgment rule "is a presumption that in making a business decision the directors of a corporation acted on an informed basis, in good faith and in the honest belief that the action was taken in the best interests of the company."[14] In applying this rule, courts defer to the business judgment of the directors, unless the court finds the board member acted in reckless indifference or deliberate disregard of the stockholders or took actions which are outside the bounds of reason.[15] Effectively, this amounts to a gross negligence standard.[16]

EXCULPATORY PROVISION

Delaware allows for an exculpatory provision to be included in a corporation's charter. This clause nearly eliminates any personal liability which directors owe to shareholders under the fiduciary duty of care.[17] Exculpatory clauses are authorized under Section 102(b)(7) of the DGCL.[18] If a complaint alleges only a breach of the duty of care, it can be dismissed if the directors are protected by an exculpatory clause.[19] Recent Delaware

---

[12] Lafferty et al., *supra* n.9, at 841-42.
[13] 8 Del. C. §141(a).
[14] Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984); Kaplan v. Centex Corp., 284 A.2d 119, 124 (Del. Ch. 1971); Robinson v. Pittsburgh Oil Refinery Corp., 126 A. 46 (Del. Ch. 1924).
[15] Gesoff v. IIC Indus., Inc., 902 A.2d 1130 (Del. Ch. 2006).
[16] Smith v. Van Gorkom, 488 A.2d 858, 874 (Del. 1985).
[17] Rodriguez v. Loudeye Corp., 189 P.3d 168 (Wash. Ct. App. 2008) (stating that an exculpatory clause only applies to the duty of care … [and thus] does not affect a duty of loyalty claim) (applying Delaware law).
[18] 8 Del. C. § 102(b)(7).
[19] Smith, 488 A.2d at 874.

court decisions have steered exculpatory clauses along a course that is increasingly favorable to directors.[20] A shareholder-plaintiff must demonstrate that a director committed an "intentional dereliction of duty" or "a conscious disregard for one's responsibilities" in the pre-discovery phase to overcome an exculpatory clause, which falls under the duty of loyalty.[21]

DUTY OF DISCLOSURE

The duty of care also encompasses a board's duty to disclose information.[22] Therefore, a claim that a board failed to adequately disclose cybersecurity risks in the appropriate documentation, pursuant to U.S. SEC requirements, will fall under the duty of care.[23] In 2011, the SEC advised publicly traded companies to approach cybersecurity as they would any other part of their businesses. In other words, if cybersecurity is a significant factor which makes an investment in the company speculative or risky, then issuers should address it in their risk factor disclosures.[24] Similarly, if a past incident or current risk of cybersecurity is likely to have a material effect on operations or financial statements, then such incident or risk should be included in their Management's Discussion and Analysis of Financial Condition and Results of Operations.[25]

DUTY OF LOYALTY

IN RE CAREMARK STANDARD

In general, the duty of loyalty requires directors to act in good faith to advance the best interests of the corporation and, similarly, to refrain from conduct that injures the corporation. *In re Caremark International Inc. Derivative Litigation* sets the standard for evaluating whether directors have

---

[20] *Id.*
[21] Richard B. Kapnick & Courtney A. Rosen, *The Exculpatory Clause Defense to Shareholder Derivative Claims*, 17 BUS. TORTS J. 2 (2010).
[22] David Rosenberg, *Making Sense of Good Faith in Delaware Corporate Fiduciary Law: A Contractarian Approach*, 29 DEL. J. CORP. L. 491, 504 n.61 (2004).
[23] SEC. AND EXCH. COMM'N, COMMISSION STATEMENT AND GUIDANCE ON PUBLIC COMPANY CYBERSECURITY DISCLOSURES, RELEASE NOS. 33-10459; 34-82746 (2018) (stating that companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements under the Securities Act and the Exchange Act and periodic and current reports under the Exchange Act).
[24] DIV. OF CORP. FIN., SEC. AND EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 - CYBERSECURITY (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[25] Div. of Corp. Fin., Sec. and Exch. Comm'n, *supra* n.24.

met their duty of loyalty regarding oversight.[26] In *Caremark,* the shareholders of Caremark International Inc. brought a suit alleging that the directors failed to put in place adequate internal controls to prevent employees from committing criminal offenses, which resulted in fines and civil penalties for the corporation.[27] The *Caremark* test asks whether: (1) the director knew or should have known of the risk; (2) the director declined to make a good faith effort to prevent the violation; and (3) the lack of action was the proximate cause of damages.[28]

In applying the *Caremark* test, liability can arise in one of two circumstances: (1) the board failed to implement any reporting, information system or internal controls, allowing a situation to develop or continue, which caused the corporation to suffer a loss; or (2) the board failed to consciously monitor or oversee the operation of the systems that were put in place.[29] For a board to meet its duty of loyalty under the *Caremark* test, it must adequately monitor the operations of an enterprise.[30] The board should consider taking three steps: (1) recognizing the magnitude of the risk brought about by the issue; (2) putting a robust reporting system in place and monitoring its operation; and (3) having in depth discussions on the implementation of potential safeguards. It must be noted that under the *Caremark* standard, the court has established a high bar for plaintiffs to prove that sufficient internal controls do not exist.[31] At the same time, by its nature, the *Caremark* standard is fact specific, and there is no safe harbor for a board member to avoid liability.

APPLICATION TO CYBER BREACHES

WYNDHAM WORLDWIDE

Courts applying Delaware law have only ruled on two derivative

---

[26] *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996) (discussing that under Delaware law, a board's duty of loyalty addresses a director's responsibilities for exercising oversight over the corporation).
[27] *Id.*
[28] *Id.* at 971.
[29] Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006) (interpreting Caremark 698 A.2d 959 (Del. Ch. 1996)).
[30] Stephen M. Honig, *Cyber Security: Ugly Gorillas and the Fiduciary Board*, IDAHO BUS. REV. (Aug. 6, 2014), http://idahobusinessreview.com/2014/08/06/cyber-security-ugly-gorillas-and-the-fiduciary-board/.
[31] *In re* Citigroup Inc. S'holder Derivative Litig., 2009 U.S. Dist. LEXIS 75564, at *19 (S.D.N.Y. Aug. 25, 2009).

lawsuits against boards of directors for the occurrence of cyber breaches.[32] In *Palkon ex rel. Wyndham Worldwide Corp. v. Holmes,* the Delaware incorporated hotel chain ("Wyndham") suffered three data breaches in a less than two-year period between April 2008 and January 2010.[33] The breaches resulted in the theft of credit card information of over 600,000 customers.[34]

Following these breaches, shareholder Palkon sent a letter to the Wyndham board demanding that the company "investigate, address and promptly remedy the harm inflicted" on the company and bring a lawsuit against the responsible personnel.[35] The Wyndham board unanimously refused the demand.[36] Subsequently, Palkon brought forth his claim on the basis that Wyndham had failed to implement the necessary cybersecurity protections to prevent a data breach from occurring.[37] In response to the motion to dismiss, Palkon asserted that the Wyndham board had wrongfully refused his demand by relying on an investigation dominated by conflicted counsel, had failed to institute reasonable security protections, and had caused damage to the corporation because of the related U.S. Federal Trade Commission investigation.[38] The court dismissed the action with prejudice based on the board's discretion to not pursue Palkon's lawsuit, the lack of bad faith present in the board's decision, and the adequacy of the internal investigation following the shareholder demand.[39]

The court applied the business judgment rule to the board's decision to not pursue Palkon's lawsuit, stating, "[i]f a board of directors refuses to pursue a shareholder's demand, that decision falls under the purview of the 'business judgment rule.'"[40] The plaintiff must raise a "reasonable doubt that the refusal was a business judgment, which requires pleading with particularity that the decision was either 'made in bad faith' or 'based on an unreasonable investigation.'"[41]

---

[32] Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014); *In re* Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016).
[33] *Palkon,* No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799, at *3.
[34] David Barres, *D&O Liability for Data Breaches After Palkon v. Holmes*, LAW360 (Nov. 3, 2014) https://www.law360.com/articles/592481/d-o-liability-for-data-breaches-after-palkon-v-holmes.
[35] *Palkon,*No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799, at *4.
[36] *Id.* at *4.
[37] *Id.* at *5.
[38] *Id.* at *6.
[39] *Id.* at *9-17.
[40] *Id.* at *7.
[41] *Id.* at *8 (citing *In re* Merrill Lynch & Co., 773 F. Supp. 2d 330, 351 (S.D.N.Y. 2011)).

The court also held that the plaintiff failed to show that there was bad faith, as conflicted legal counsel did not influence the board's refusal.[42] The court found that the counsel did not have conflicted duties representing the company in the simultaneous case with the FTC, stating that the outside firm's interest remained the same in continuing "to act in WWC's best interest."[43] The plaintiff further claimed that Wyndham's General Counsel's advice to the board constituted a conflict of interest.[44] However, the court found that there was not a conflict of interest because the General Counsel was not included as a responsible party and was not directly associated with Wyndham's cybersecurity program.[45] The court continued that had the General Counsel been involved with the cybersecurity program, he would still have been allowed to advise the board on their decision, because the fear of personal liability does not render a corporate director conflicted.[46]

Lastly, the court held that the board's investigation was not predetermined or unreasonable.[47] In response to this claim, the court examined whether the board's investigation suggested gross negligence because "the board acted with so little information that their decision was unintelligent and unadvised."[48] The court found the board's familiarity with the factual underpinnings of the plaintiff's demands began prior to the arrival of the demand, noting that the board had discussed the cyberattacks at fourteen meetings between October 2008 and August 2012.[49] Furthermore, "at every quarterly meeting the General Counsel gave a presentation regarding the [b]reaches and/or WWC's data-security generally," and the audit committee also discussed the subject matter in sixteen meetings during the same period.[50] Additionally, the audit committee reviewed the demand at multiple meetings before discussing it with the entire board; thus, the court held the board had enough information when it assessed the plaintiff's claim.[51]

---

[42] *Id.* at *8-9 (citing *In re* Tower Air, Inc., 416 F.3d 229, 238 (3rd Cir. 2005)).
[43] *Id.* at *10.
[44] *Id.*
[45] *Id.* at *10-12.
[46] *Id.* at *12 (citing Halpert Enters., No. 06 Civ. 2331(HB), 2007 WL 486561, at *6 (S.D.N.Y. Feb. 14, 2007)).
[47] *Id.* at *15.
[48] *Id.* at *12 (citing *In re* Gen. Motors Class E Stock Buyout Sec. Litig., 694 F. Supp. 1119, 1133 (D.Del. 1998)).
[49] *Id.* at *13.
[50] *Id.*
[51] *Id.*

Palkon was decided for the defendant before the court reached the merits of the claim related to the *Caremark* theory; however, in a footnote, the court discussed the application of the *Caremark* standard to the cyber breach.[52] The court clarified that the plaintiff failed to satisfy the high bar that was necessary to prove that the directors violated their duty of loyalty under *Caremark*.[53]

Quoting *Stone v. Ritter*, the court stated "*Caremark* requires that a corporation's 'directors utterly failed to implement any reporting or information system . . . [or] consciously failed to monitor or oversee its' operations thus disabling themselves from being informed.'"[54] The plaintiff's claim was weak because the company had installed cybersecurity measures before the first data breach, and the board had discussed the cyber breach and the risk of future breaches.[55] These discussion and actions included the following: conducting fourteen quarterly meetings in which it discussed the cyberattacks, company security policies and proposed security enhancements; appointing the board's audit committee to investigate the breaches, with the committee meeting at least sixteen times to review cybersecurity; and hiring a technology firm to recommend security enhancements, which the company had begun to implement.[56]

APPLICATION OF WYNDHAM WORLDWIDE

Palkon stands for the proposition that a board may dismiss a shareholder's demands related to a cybersecurity breach under the business judgment rule, unless the plaintiff pleads with particularity that the decision was made in bad faith or upon an unreasonable investigation. Specifically, the plaintiff must claim that the board members either predetermined the results of the investigation in the interest of protecting themselves, or that they failed to undertake a reasonable investigation that would make them aware of the necessary facts surrounding the incident.

Based on *Palkon*, a board of directors should document all discussions taken in anticipation of and response to a cyber breach to show that they properly weighed the cybersecurity risks of the corporation. Furthermore, a board should have a robust reporting system. Like Wyndham, a board should be notified of each cyber breach and be made

---

[52] *Id*. at *15 n.1.
[53] *Id*.
[54] *Id*.
[55] *Id*. at *5.
[56] *Id*.

aware of the results of the investigations regarding the breaches. A board should also discuss the implementation of safeguards. For instance, the Wyndham board's discussions led to the decision to contract outside consultants to identify weaknesses and recommend improvements for the company's cybersecurity system. One of the most obvious safeguards a board can implement is a budget review, which can result in increased funds being directed towards cybersecurity.[57] Other safeguards include, but are not limited to, stress tests, the implementation of measures to create a business culture that prioritizes cybersecurity, and the disposal of unnecessary records.[58]

IN RE HOME DEPOT

In *In re* Home Depot Shareholder Derivative Litigation, the home improvement supply store suffered multiple data breaches between April and September 2014.[59] The breaches resulted in the theft of the financial records for 56,000,000 customers, which cost an estimated $10 billion in damages.[60]

The shareholders' derivative suit alleged that: (1) the board breached its duty of loyalty through the failure to institute internal controls; (2) the board wasted corporate assets; and (3) the board of directors violated section 14(a) of the Securities Exchange Act in the corporation's 2014 and 2015 proxy filings.[61]

Following the breaches, the shareholders made no demands on the board of directors as is required by Delaware law.[62] In Delaware, aggrieved shareholders must demand that the board take the desired action unless the demand would be futile.[63] Although the court acknowledged that the

---

[57] Stephen L. Caponi, *Cybersecurity and the Board of Directors: Avoiding Personal Liability – Part III of III: Policies and Procedures,* REUTERS (Aug. 8, 2013), http://blogs.reuters.com/financial-regulatory-forum/2013/08/08/cybersecurity-and-the-board-avoiding-personal-liability-part-iii-of-iii-policies-and-procedures/.

[58] Bruce A. Radke & John C. Cleary, *Lessons from Dismissal of Wyndham Shareholders Derivative Action*, THE NAT'L. L. REV. (2014), https://www.natlawreview.com/article/lessons-dismissal-wyndham-shareholders-derivative-action.

[59] *In re* Home Depot S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1321 (N.D. Ga. 2016).

[60] *Id*. at 1321.

[61] *Id*. at 1325.

[62] *Id*. at 1324.

[63] *Id*. (citing Stepak v. Addison, 20 F.3d 398, 402 (11th Cir. 1994)).

majority of the directors were named as defendants, it noted that "derivative action plaintiffs do not ring the futility bell merely by including a majority of the directors as defendants."[64] Delaware law instead requires a plaintiff to show that a director's conduct is "so egregious on its face that board approval cannot meet the test of business judgment, and a *substantial likelihood* of director liability therefore exists." [65]

The plaintiffs' primary claim was that the directors breached their duty of loyalty to the corporation.[66] Specifically, the plaintiffs claimed that the board consciously disregarded its duty when the directors failed to designate the responsibility of overseeing data security, thereby leaving the company without a reporting system.[67] Prior to the breach, Home Depot's infrastructure committee, which had managed cybersecurity, was disbanded and the audit committee, which was supposed to assume those responsibilities, had not amended its charter accordingly.[68] The court saw past this formalism, explaining that "the [a]udit [c]ommittee received regular reports from management on the state of Home Depot's data security, and the [b]oard in turn received briefings from both management and the [a]udit [c]ommittee."[69]

The plaintiffs also argued that the board "failed to ensure that a plan was in place to *immediately* remedy the deficiency [in Home Depot's data security]."[70] The court noted that the plaintiffs repeatedly acknowledged that there was a plan, only arguing that the plan moved too slowly.[71] The limited plan was enough to satisfy the board's duty of loyalty. Delaware courts have held that "[b]ad faith cannot be shown by merely showing that the directors failed to do all they should have done under the circumstances."[72] The court stated that "while the board probably should have done more, '[s]imply alleging that a board incorrectly exercised its business judgment and made a 'wrong' decision in response to red flags...is not enough to plead bad faith.'"[73]

The shareholders also alleged that the directors wasted corporate

---

[64] *Id*.
[65] *Id*. at *1324-25.
[66] *Id*. at *1325.
[67] *Id*. at 1325-26.
[68] *Id*.
[69] *Id*. at 1326.
[70] *Id*.
[71] *Id*.
[72] *Id*.
[73] *Id*. at 1327.

assets.[74] Under *Aronson*, the demand futility test requires the plaintiffs to "provide particularized factual allegations that raise a reasonable doubt that '(1) the directors are disinterested and independent [or] (2) the challenged transaction was otherwise the product of a valid exercise of business judgment.'"[75] The plaintiffs challenged the board under the second prong of *Aronson*, stating that the "board's insufficient reaction to the threat posed by the holes in Home Depot's data security caused significant losses to the [c]ompany, which they claim is a waste of Home Depot's assets."[76] The court continued, stating that "the [p]laintiffs are asking the Court to conclude from the presence of these 'red flags' is that the [d]irectors failed to see the extent of Home Depot's security risk and therefore made a 'wrong' business decision by allowing Home Depot to be exposed to the threat of a security breach."[77] Thus, this decision fell under the protection of the business judgment rule.[78]

The shareholders lastly asserted that the directors violated section 14(a) of the Securities Exchange Act when they issued their 2014 and 2015 proxy statements.[79] The court found that the plaintiffs failed to specify which statements in the 2014 and 2015 proxy statements were rendered misleading or false by omissions, failed to show the materiality of the Audit Committee's failure to report that its charter had not been amended, and failed to show that the alleged omissions caused the alleged losses.[80]

The shareholders appealed the decision after the case was dismissed. Before the pending appeal was considered, the case was settled. The settlement agreement set forth corporate governance reforms, which required Home Depot to: (1) document the duties and responsibilities of the Chief Information Security Officer; (2) periodically conduct tabletop cyber exercises; (3) monitor and periodically assess key indicators of compromise on network endpoints; (4) maintain and periodically assess the company's partnership with a dark web mining service to search for confidential Home Depot information; (5) maintain an executive-level committee focused on the company's data security; (6) receive periodic reports from management

---

[74] *Id*.
[75] *Id*. (citing Brehm v. Eisner, 746 A.2d 244, 254 (Del. 2000)).
[76] *Id*.
[77] *Id*. at 1328.
[78] *Id*. The plaintiffs also tried to argue that the board wasted corporate assets with M. Carey's compensation package. This argument was made in the Resp. to the Def. The court stated that a "plaintiff cannot amend the complaint by arguments of counsel made in opposition to a motion to dismiss." The court also dismissed the claim on its merits.
[79] *Id*. at 1329.
[80] *Id*. at 1331.

regarding the amount of the company's IT budget and what percentage of the IT budget is spent on cybersecurity measures; (7) maintain an Incident Response Team and an Incident Response Plan; (8) maintain membership in at least one Information Sharing and Analysis Center ("ISAC"); (9) join and comply with ISAC or Information Sharing and Analysis Organization ("ISAO"); and (10) retain their own IT, data, and security experts and consultants as they deemed necessary.[81]

APPLICATION OF IN RE HOME DEPOT

In re Home Depot demonstrates that shareholders must show "particularized facts beyond a reasonable doubt that a majority of the [b]oard faced substantial liability because it consciously failed to act in the face of a known duty to act" in order to satisfy the demand futility for duty of loyalty claims.[82] This high standard must be satisfied by shareholders in to bring forth a claim.

Based on *In re* Home Depot, a board may fulfill its duty of loyalty by assigning the oversight of cybersecurity to a subcommittee. A subcommittee of the board does not need to have explicit authority for cybersecurity oversight through a company's bylaws or the committee's charter. The court will recognize that a subcommittee, such as an audit or risk committee, has practical authority if the committee addresses and discusses the issue on multiple occasions. Courts will also likely give deference to any cybersecurity breach response plan a corporation has in place because the business judgment rule protects a flawed and slowly implemented response plan.

The fiduciary law is still unsettled for the board of directors in the instance of a cyber breach. The *In re* Home Depot settlement may have been motivated by that legal uncertainty. Thus, corporations should have in-depth discussions on cybersecurity oversight and address the potential issues with a robust reporting system and safeguards. Following the rulings in cases like *Palkon* and *In re* Home Depot, the implementation of such precautions would likely guarantee that a court would find for the corporation.

---

[81] Plaintiffs' Unopposed Mot. for Prelim. Approval of S'holder Derivative Settlement and Mem. of Law in Supp. at 2, *In re* Home Depot S'holder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016) (No. 1:15-CV-2999 TWT).

[82] *In re* Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1325 (N.D. Ga. 2016).

DUTY OF LOYALTY

RECOGNITION OF THE MAGNITUDE OF THE RISK

If a plaintiff in a derivative suit is successful in surviving a motion to dismiss, the critical question will likely become whether the director violated his or her duty of loyalty based on the *Caremark* standard. In an attempt to satisfy the *Caremark* standard, the board should engage in discussions and actions that are commensurate with the magnitude of the risk facing the company. In terms of cybersecurity, directors should understand their company's cybersecurity risk profile, which is a combination of how likely it is a company will suffer a cyberattack combined with the severity of the consequences that may flow from an attack.[83] To understand the level of risk that the issue presents, the board should review the reporting systems and safeguards related to cybersecurity that the corporation already implemented. The audit should identify the weaknesses within the framework and judge the relevant threats accordingly.[84]

To accomplish this review, it may be necessary for the board to consult outside studies and statistics.[85] Corporations may also choose to contract a third party to conduct a review. Courts may show deference to corporations that have invited third parties to conduct cybersecurity system audits.[86] According to *Caremark*, the board will not have to consider taking actions in the aim of protecting the corporation from cyber breaches if the risk is only negligible.[87] However, based on the highly publicized recent cases of major cyberattacks against corporations, it can be predicted that

---

[83] *See* Kobi Kastiel, *Cyber Governance: What Every Director Needs to Know*, HARV. L. SCH. F. ON CORP. GOVERNANCE AND FIN. REG. (June 5, 2014), https://corpgov.law.harvard.edu/2014/06/05/cyber-governance-what-every-director-needs-to-know/.

[84] *See* Victoria C. Wong, *Cybersecurity, Risk Management, and How Boards Can Effectively Fulfill Their Monitoring Role*, 15 U.C. DAVIS BUS. L.J. 201, 214-215 (2015).

[85] *See id*.

[86] Jan P. Levine et al., *Wyndham Decision Provides Guidance to Corporate Directors and Officers in Responding to a Data Breach*, PEPPER HAMILTON LLP (Nov. 13, 2014), https://www.pepperlaw.com/resource/135/27F3, *available in* the Jan. 7, 2015 issue of Cyber Risk Network *under the title* "D&O's Best Defense Against Shareholder Demands Over Cybersecurity."

[87] 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/.

courts will expect the matter be given serious consideration.[88]

Many industries are facing issues of cybersecurity, but the automotive industry in particular is especially susceptible to cyber breaches. The increasing data gathering functions within automobiles has made it foreseeable for potential claims to arise against an automobile manufacturer or supplier not only at the enterprise level breach, but also for breaches related to vehicle hacks.[89] Large scale breaches of consumer data will be possible if a corporation receives or stores the data from vehicles. Current vehicles use about one hundred million lines of software code, with the average of fifteen potential entry points every thousand lines.[90] The number of line codes is expected to increase to three hundred million lines per vehicle in the near future, increasing the potential for hacks.[91]

An automobile's susceptibility to be hacked has recently been showcased by Charlie Miller and Charlie Valasek, who were able to hack into and take control of a 2014 Jeep Cherokee.[92] The parties completed the hacking using a cellular-based hacking device to take control of the vehicle. Similar automobile hacking devices are available online, with some of the devices selling for prices below $100.[93] With cars continuously storing more internal data, it is possible that hacking devices could compromise data specific to the user such as geo-location, biometrics, and driver behavior.[94] A number of individual data breaches could result in a class

---

[88] Steven L. Caponi, *Cybersecurity and the Board of Directors: Avoiding Personal Liability – Part II of III*, REUTERS, (Aug. 6, 2013), http://blogs.reuters.com/financial-regulatory-forum/2013/08/06/cybersecurity-and-the-board-of-directors-avoiding-personal-liability-part-ii-of-iii/.

[89] *See generally* Daniel A. Crane et al., *A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles*, 23 MICH. TELECOMM. & TECH. L. REV. 191 (2017).

[90] David Gelles et al., *Complex Car Software Becomes the Weak Spot Under the Hood*, N.Y. TIMES (Sep. 26, 2015), https://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html.

[91] Robert N. Charette, *This Car Runs on Code*, IEEE SPECTRUM (Feb. 1, 2009, 5:00 PM), http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code.

[92] John Villasenor, *Five Lessons on the 'Security of Things' From the Jeep Cherokee Hack*, FORBES (July 27, 2015, 1:31 PM), https://www.forbes.com/sites/johnvillasenor/2015/07/27/five-lessons-on-the-security-of-things-from-the-jeep-cherokee-hack/.

[93] Darlene Storm, *$60 DIY Car Hacking Device is an Inexpensive and Easy Way to Hack Cars*, COMPUTERWORLD (Mar. 30, 2015, 7:43 AM), https://www.computerworld.com/article/2903714/60-diy-car-hacking-device-is-an-inexpensive-and-easy-way-to-hack-cars.html.

[94] Ryan Beene & Gabe Nelson, *Automakers Adopt Protocols to Handle, Protect Consumer Data in Connected Car Era*, AUTOMOTIVE NEWS (Nov. 13, 2014, 12:00

action and subsequently a derivative action could be filed.

A cyber breach resulting in data being compromised could have a number of negative effects upon a corporation. The possible risks include the loss of customer confidence, harm to the company's reputation, impact on the stock price, potential regulatory action, potential litigation, and an interruption to the course of business.[95] According to a recent study by Ponemon Institute, an organization that conducts research on data protection and emerging information technologies, the average monetary loss incurred by a corporation as a result of a cyber breach is $3.62 million.[96] The average cost paid for each lost or stolen record containing sensitive and confidential information is $141.[97]

IMPLEMENTATION OF A REPORTING SYSTEM

The most essential component of satisfying the *Caremark* test, pursuant to *Stone v. Ritter*, is that a board implement a reporting system, and continue to properly oversee or monitor its operations.[98] Courts may expect for a process to be in place where the board of directors continues to be informed of the company's cybersecurity framework, as well as ongoing developments related to the company's cybersecurity. The specifics of what should be reported and how much detail should be included in the reports has not been specified by the courts.

According to some experts, an ideal reporting system would consist of the board receiving regular briefings from the CIO and a yearly internal report on the cybersecurity program.[99] The cybersecurity updates should examine existing risks, reassess the magnitude of those risks, and note any

---

AM), http:/www.autonews.com/article/20141113/OEM11/141119926/automakers-adopt-protocols-to-handle-protect-consumer-data-inopt-protocols-to-handle-protect-consumer-data-in-connected-car-era.

[95] Paul Ferillo, *Cyber Security, Cyber Governance, and Cyber Security*, HARV. L. SCH. F. ON CORP. GOVERNANCE AND FIN. REG. (Nov. 13, 2014), https://corpgov.law.harvard.edu/2014/11/13/cyber-security-cyber-governance-and-cyber-insurance/.

[96] PONEMON INST., 2017 COST OF DATA BREACH STUDY: GLOBAL OVERVIEW 1 (2017), https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/security-ibm-security-services-se-research-report-sel03130wwen-20180122.pdf.

[97] *Id*. at 5.

[98] Stone v. Ritter, 911 A.2d 362, 369 (Del. 2006).

[99] *See* Interview with Robyn Bew, Dir. of Research, Nat'l Ass'n of Corp. Dirs. (NACD) (Aug. 14, 2014, 6:38PM), http://ccbjournal.com/articles/29597/cybersecurity-and-national-association-corporate-directors.

legislative or regulatory changes that have taken place.[100] The board of directors may consider appointing a committee that would solely address cybersecurity threats facing the corporation. As stated above, courts may still find it sufficient for an audit or risk committee to address the issue.[101] The committee should schedule time for the periodic review of risk management in addition to its role of reviewing financial statements and accounting compliance. All discussions should be documented.[102] The committee should work closely with the executives charged with cybersecurity.[103] *In re* Home Depot demonstrates that a board committee does not have to have formal oversight over cybersecurity. In *In re* Home Depot, oversight responsibility had been transferred to the audit committee, but the committee's charter did not reflect the change.[104] Despite this omission, the court found it sufficient that the audit committee received regular cybersecurity reports and briefed the board.[105]

Additionally, the board of directors is expected to spend time discussing cybersecurity after receiving reports or updates. In *Palkon* the court found that Wyndham's board of directors had an adequate reporting system for cybersecurity because the subject matter was discussed at fourteen 14 quarterly meetings.[106] Discussions should focus on the organization's security framework, top security threats (external and internal) facing the organization, employee awareness regarding cybersecurity, the performance of the individuals charged with maintaining the cybersecurity framework, and the response plan for a breach.

DISCUSSION OF POTENTIAL SAFEGUARDS

The third part of the *Caremark* test is whether the board conducted discussions regarding the implementation of safeguards. Internal controls which are implemented to prevent cyber breaches should be discussed in

---

[100] Martin Lipton et al., *Risk Management and the Board of Directors*, HARV. L. SCH. F. ON CORP. GOVERNANCE AND FIN. REG. (July 18, 2015), https://corpgov.law.harvard.edu/2015/07/28/risk-management-and-the-board-of-directors-3/.
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *In re* Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1322 (N.D. Ga. 2016).
[105] *Id.* at 1326.
[106] Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799, at *13-14 (D.N.J. Oct. 20, 2014).

order to address the magnitude of the risk of a cyber breach.[107] The most obvious way to show that the implementation of internal controls received adequate consideration is for the board to actually implement the controls.

While there is no clear guidance as to the appropriate amount of internal controls, boards are not required to guarantee complete security.[108] Corporations should look to the safeguards and reporting systems of companies with similar risk profiles.[109] The board may engage management by discussions concerning whether specific cybersecurity insurance is required and whether this insurance is adequate in relation to the costs that a company would incur from a cyber breach. Regular commercial insurance policies may not cover damage associated with data theft, destruction or compromise or other harms from cybersecurity breaches.[110]

Compliance with recognized industry standards may also be a way to demonstrate appropriate safeguards.[111] The National Institute of Standard and Technology ("NIST") standard may provide some objective evidence of the steps that should be taken by a corporation and may be used as the minimum standard in cases. NIST's "Framework for Improving Critical Infrastructure Cybersecurity" was used in the FTC's recent lawsuit against Wyndham but that was not a case involving a board of directors.[112] Other well-known cybersecurity standards include the "Control Objectives for Information and Related Technology" ("CoBIT"), and the International Standards of Organization's cybersecurity standard ("ISO/IEC 27002").[113]

---

[107] Jon Talotta et. al., *Data Breaches Hit the Board Room: How to Address Claims Against Directors and Officers*, CHRON. OF DATA PROTECTION: PRIVACY & INFO. SEC. NEWS & TRENDS (Jan. 23, 2015), http://www.hldataprotection.com/2015/01/articles/cybersecurity-data-breaches/data-breaches-hit-the-board-room/.

[108] *See* Palkon, No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799.

[109] Caponi, s*upra* n.57.

[110] *See* Stephen Gandel, *Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year*, FORTUNE (Jan. 23, 2015), http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.

[111] NAT'L INST. OF STANDARDS AND TECHNOLOGY, U.S. DEP'T OF COMMERCE, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[112] FTC v. Wyndham Worldwide Corp, 799 F.3d 236, 246 (3d Cir. 2015) (discussing how the FTC alleged that the company failed to follow proper incident response procedures, including failing to monitor its computer network for malware used in a previous intrusion pursuant to the NIST framework).

[113] *See* Health Information Trust Alliance, *Framework for Reducing Cyber Risks to Critical Infrastructure – Response From The Health Information Trust Alliance (HITRUST)*, HEALTH INFO. TRUST ALL. (2013), https://www.nist.gov/file/368381.

Boards should have the knowledge and expertise to understand the reports they receive on cybersecurity. If the board lacks directors who understand cybersecurity, a court could hold that the board is incapable of properly weighing the magnitude of risks, taking advantage of the reporting system, or putting the necessary controls in place. Thus, the board should receive some level of education on cybersecurity and should consider appointing board members with some IT governance or cybersecurity risk experience.[114] Education programs could include an assessment of the company's risk of a cyber breach, information about the current cybersecurity framework, potential and planned improvements, outside audits, and other information that the cyber security team believes to be of importance in educating the board.[115]

DEVELOPMENT OF A RESPONSE PLAN

Of potential safeguards, courts will show the most deference to cyber breach response plans.[116] An ideal response plan should aim to mitigate potential damages caused by the cyber breach, as well as identify the root cause and source of the breach. The response plan should be a well-developed, deliberate plan consistent with the best practices for a company in the same industry.[117] The response plan may specify who will be notified, within what time frame, what documentation must be kept, who is designated to speak about the incident, and who has authority to make certain decisions about the investigation.[118] Following a cyber breach, a corporation should implement its response plan immediately. Failing to properly carry out the response plan could convey a lack of preparation by

---

[114] Wong, *supra* n.85, at 214.
[115] Brenda Sharpton, *Breaches in the Boardroom: What Directors and Officers Can Do to Reduce the Risk of Personal Liability for Data Security Breaches*, JD SUPRA (2015), https://www.jdsupra.com/legalnews/breaches-in-the-boardroom-what-director-78635/.
[116] *See* Luis A. Aguilar, Comm'r, Sec. and Exch. Comm'n., Address at the New York Stock Exchange Conference: Cyber Risks and the Boardroom (June 10, 2014, https://www.sec.gov/news/speech/2014-spch061014laa.
[117] Eduardo Gallardo & Andrew Kaplan, *Board of Directors Duty of Oversight and Cybersecurity*, DEL. BUS. COURT INSIDER (Aug. 20, 2014), https://www.gibsondunn.com/wp-content/uploads/documents/publications/GallardoKaplan--Board-of-Directors-Duty-of-Oversight-Aug2014.pdf.
[118] Jody R. Westby, *Cybersecurity & Law Firms: A Business Risk*, 39 L. PRAC. MAG. 4 (2013), https://cdn.ymaws.com/www.napaba.org/resource/resmgr/2015_NAPABA_Con/CLE_/SSFs/SSF3_NAPABA2015CLE.pdf.

the board.[119] However, *In re* Home Depot demonstrates that a flawed and slowly implemented response plan may still be sufficient.

The board of directors should also conduct an internal investigation or contract a third party to identify the weakness in the cybersecurity system if a cyber breach occurs, and subsequently, should look to address the problem.[120] Courts normally put greater weight on third party investigations following a breach than those that are conducted in-house. *Palkon* demonstrates that it is not necessary for the investigation to recognize the root cause of the breach for the board's fiduciary duty to be fulfilled. In *Palkon*, the appointment of an audit committee to investigate the breach, which then hired a technology firm to recommend security enhancements, was evidence that the board satisfied its duties.[121]

CONCLUSION

DUTY OF CARE

In the instance that shareholders of a publicly traded Delaware corporation bring a derivative suit based on the duty of care against the board of directors in the event of a cyber breach, the lawsuit will likely fail. Delaware courts give deference to the board's decisions and will only find its members liable in instances of gross negligence or intentional disregard of the risks present based on the business judgment rule. Delaware courts have found that "the mere fact that a company takes on business risk and suffers losses—even catastrophic losses—does not evidence misconduct, and without more, is not a basis for personal director liability."[122] In regards to cybersecurity, the board of directors would have to be grossly negligent by unintentionally failing to acknowledge the issue despite the publicity it has received.

The board is further protected if the company has an exculpatory clause in its charter. Directors must be found to have acted in bad faith by either intentionally violating their duties to act in the company's best interest or completely ignoring their responsibilities. For cybersecurity, the board will be protected from duty of care claims unless it acknowledged the presence of a prevalent risk of the company and made it clear that it would

---

[119] *See* Aguilar, *supra* n.116.
[120] Talotta et. al., s*upra* n.107.
[121] Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 U.S. Dist. LEXIS 148799, at *5 (D.N.J. Oct. 20, 2014).
[122] *In re* Citigroup Inc. S'holder Derivative Litig., 964 A2d 106, 130 (Del. Ch. 2009).

disregard the entirety of the issue.

DUTY OF LOYALTY

In order to meet its duty of loyalty in the context of a cybersecurity issue, a board must discuss relevant risks, implement a reporting system whereby it is informed of important cybersecurity developments, and put in place internal controls. A board may implement safeguards to protect against a cyber breach as well as develop a response plan that would be put in place in the event of a cyber breach. At the same time, the standard of proof that the plaintiff must show to demonstrate that a board member violated the duty of loyalty is high. In *Palkon* and *In re* Home Depot, the court found that the board members did not violate their duty of loyalty despite taking limited actions to prevent cyber breaches.[123]

[123] Note that *Palkon* is fact-specific and there is no safe harbor from liability and *In re* Home Depot was settled following the dismissal.