DERIVATIVE LIABILITY IN THE WAKE OF A CYBER ATTACK

Benjamin Dynkin[*] *& Barry Dynkin*[**]

In the age of the data breach, corporations of all sizes and forms face an ever increasing risk of cyber attack. Successful cyber attacks lead to millions of dollars in remediation costs and can create many forms of legal liability for a company. These liabilities and costs can have serious repercussions on the value of a business, which ultimately can negatively affect a stockholder. This harm has invariably led to the rise of derivative liability for a corporation's Board of Directors, which can force them to incur personal damages. This new form of liability will force Directors to actively manage cyber risk, or risk facing a lawsuit.

[*] Benjamin Dynkin is the Co-Executive Director of the American Cybersecurity Institute and Co-Founder of Atlas Cybersecurity. Prior to that, he was a Senior Forensic Analyst at Law & Forensics and the Managing Editor of the Journal of Law and Cyber Warfare. He has authored and contributed to articles in the fields of cybersecurity, cyber warfare, digital forensics, and e-discovery. He can be reached at Ben@americancyberinstitute.org.

[**] Barry Dynkin is the Co-Executive Director of the American Cybersecurity Institute and Co-Founder of Atlas Cybersecurity. He was a legal researcher on the Tallinn Manual on Cyber Warfare 2.0 and a contributing author on Law Firm Cybersecurity, a publication of the ABA, and has widely published numerous papers on a variety of legal, cybersecurity, and cyber warfare related topics. He was staff editor of the Journal of Law and Cyberwarfare. He can be reached at Barry@americancyberinstitute.org.

I. INTRODUCTION

While many things are uncertain in the age of the data breach, it is undeniable that these attacks are here to stay. Companies must continuously focus on implementing and improving effective cybersecurity procedures and policies or risk facing significant liability as a result of their inaction. There has been ample litigation resulting from data breaches, but most such cases focus on corporate wrongdoing, where plaintiffs allege common law (tort and contract) and statutory (consumer privacy laws) causes of action.[1] These cases often settle, but such a settlement represents only a small portion of the overall price that a company will pay as a result of a data breach—the largest portion of which centers around remediation and other secondary costs.[2]

---

[1] *See generally* David Zetoony et al., *2017 Data Breach Litigation Report*, BRYAN CAVE LLP, https://d11m3yrngt251b.cloudfront.net/images/content/9/6/v2/96690/Bryan-Cave-Data-Breach-Litigation-Report-2017-edition.pdf (for data breach litigation trends).

[2] PONEMON INST., 2017 COST OF DATA BREACH STUDY 29 (2017).
Typical activities for the discovery of and the immediate response to the data breach include the following:
□Conducting investigations and forensics to determine the root cause of the data breach
□Determining the probable victims of the data breach
□Organizing the incident response team
□Conducting communication and public relations outreach
□Preparing notice documents and other required disclosures to data breach victims and regulators
□Implementing call center procedures and specialized training
The following are typical activities conducted in the aftermath of discovery:
□Audit and consulting services
□Legal services for defense
□Legal services for compliance
□Free or discounted services offered to victims of the breach
□Identity protection services
□Lost customer business based on calculating customer churn or turnover

The Ponemon Institute released a study on the average cost of a data breach, which found that the average cost for each lost or stolen record containing sensitive and confidential information was $141,[3] but that number can vary greatly depending on the nature and sensitivity of the records compromised. The total average cost paid by organizations was $3.62 million.[4] While this average alone would be substantial enough for a company to pay attention to the risks of a data breach, some of the largest data breaches have posed far more significant costs. For example, Home Depot suffered "$161 million of pretax expenses, net of expected insurance recoveries, in connection with [its 2014] Data Breach."[5]

With the sheer number of data breaches that have occurred in 2017–1,579 as determined by the Identity Theft Resource Center,[6] which resulted in 178,955,069 records being compromised,[7] with a total scale of economic harm in the billions, a company's Board of Directors ("Directors") must be aware, not only of the litigation costs of a data breach, but also the additional risks posed by derivative litigation for improper or non-action on the part of the Directors. The plaintiff's bar has attempted to bring derivative litigation claims based on cyber-related claims, but have thus far been unsuccessful in pursuing their claims, due to a variety of procedural and substantive roadblocks associated with successfully maintaining a derivative action.[8] With the number of data breaches increasing, it is inevitable that circumstances will arise in which the procedural and substantive roadblocks of previous cases will not be present, and a derivative action will be able to proceed on the merits of the claim. Thus, because of the

---

Customer acquisition and loyalty program costs.
Id.

[3] *Id.* at 1.

[4] *Id.*

[5] Home Depot, Annual Report (Form 10-K) (Mar. 23, 2016).

[6] *Data Breach Reports: 2017 End of Year Report*, IDENTITY THEFT RESOURCE CENTER (2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf. "The IRTC defines a data breach as an incident in which an individual name plus a Social Security number, Driver's License number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure." *Data Breaches*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/data-breaches.html.

[7] *Id.*

[8] *See* Kevin M. LaCroix, *Home Depot Data Breach Derivative Lawsuit Dismissed*, THE D&O DIARY (Dec. 1, 2016), https://www.dandodiary.com/2016/12/articles/cyber-liability/home-depot-data-breach-derivative-lawsuit-dismissed/ (mentioning that derivative lawsuits filed against Home Depot, Target, and Wyndham Worldwide were dismissed).

underlying ambiguities in the application of law in this context, Directors must take cyber risk, and its associated potential liabilities very seriously. This Article seeks to survey the current state of data breach related derivative litigation, as well as identify certain areas of focus that boards must address or risk facing liability.

II. DERIVATIVE LITIGATION

A derivative action is defined as "[a] suit by a beneficiary of a fiduciary to enforce a right belonging to the fiduciary."[9] The specific subset of derivative action that will be discussed in this Article is a shareholder derivative action, which is "a suit asserted by a shareholder on the corporation's behalf against a third party (usu[ally] a corporate officer) because of the corporation's failure to take some action against the third party."[10]

A Board of Directors is responsible for the management of the business affairs of a corporation,[11] but that duty generally only extends to "[authorizing] the most significant corporate acts or transactions: mergers, changes in capital structure, fundamental changes in business, appointment and compensation of the CEO, etc."[12] In discharging their responsibilities, "the directors owe fiduciary duties of care and loyalty to the corporation and its shareholders."[13]

A. The Business Judgment Rule

Prior to examining the types of claims that may follow a breach of the duty of care or loyalty, we must preliminarily examine the primary hurdle that stands in the way of many derivative litigation claims, namely the business judgment rule.[14] The

---

[9] *Derivative Action*, *in* BLACK'S LAW DICTIONARY (10th ed., 2014).

[10] *Id.* This paper will focus on shareholder actions on behalf of publicly traded companies, but the fiduciary responsibilities owed by directors does not change if the company is privately held. In fact, there has been a noticeable downturn in the IPO market, which is resulting in many large companies acquiring capital through other routes. *See e.g.*, Seung Lee, *Tech Companies Are Actively Avoiding Going Public in 2016*, NEWSWEEK (Apr. 4, 2016), http://www.newsweek.com/tech-companies-are-actively-avoiding-going-public-2016-443885.

[11] *See, e.g.*, 8 DEL.C. § 141(a) (West, Westlaw through 81 Laws 2018, chs. 200–216) ("The business and affairs of every corporation organized under this chapter shall be managed by or under the direction of a board of directors").

[12] *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959, 968 (Del. Ch. 1996).

[13] *Mills Acquisition Co. v. Macmillan, Inc.*, 559 A.2d 1261, 1280 (Del. 1989).

[14] *See generally* Douglas M. Branson, *The Rule that Isn't a Rule – The Business Judgment Rule,* 36(3) VAL. U. L. REV. 631 (2002) (discussing that there is not a

Business Judgment Rule ensures that good faith decisions made by Directors are protected even though, in retrospect, the decisions prove to be unsound, incorrect, or erroneous.[15] The rationale behind the Business Judgment Rule is that courts should recognize the expertise of a Board, and under certain circumstances, presume the propriety of the decision of the Board, even when the decision ultimately turns out poorly.[16] This deference has several bases including: (1) the mandate given by stockholders to the directors to manage the day-to-day business of the enterprise; (2) the fact that the courts are ill-equipped in terms of substantive knowledge to undertake a meaningful review of "ordinary" business decisions; (3) the need to encourage directors to undertake the risks inherent in running an enterprise; and (4) the fact that corporations will be able to attract and retain competent directors only if their personal financial exposure is minimized.[17] With this background in mind, we turn to examining forms of derivative liability, specifically breaches of the duties of care and loyalty, respectively.

B. The Duty of Care

The essence of the duty of care has two requirements: (1) Directors must exercise the requisite degree of care in the process of reaching an informed decision for the corporation,[18] and (2) directors must exercise due care in discharging their other duties, including delegation of responsibility.[19] While there was, for a

---

single business judgment rule, but rather states tend to adopt different versions of the rule, based on similar policy goals).

[15] Legal Info. Inst., *Business Judgment Rule*, CORNELL U., https://www.law.cornell.edu/wex/business_judgment_rule.

[16] *See, e.g.*, *Zapata Corp. v. Maldonado*, 430 A.2d 779, 782 (Del. 1981) (discussing the deference that should be given to the decision-making of a board); *Aronson v. Lewis*, 473 A.2d 805, 812 (Del. 1984) (discussing the court's decision to respect the decisions of a board).

[17] *See generally* E. Norman Veasey, *Seeking a Safe Harbor from Judicial Scrutiny of Directors' Business Decisions—An Analytical Framework for Litigation Strategy and Counselling Directors*, 37 BUS. LAW. 1247 (1982) (addressing the Courts' reluctance to interfere in this area).

[18] *See, e.g.*, *Smith v. Van Gorkom*, 488 A.2d 858, 873 (Del. 1985) (noting, in the merger context, that directors have a duty to "act in an informed and deliberate manner in determining whether to approve an agreement of merger"); *In re Goldman Sachs Group, Inc. S'holder Litig.*, C.A. No. 5215–VCG, 2011 WL 4826104, at *16 (Del. Ch. Oct. 12, 2011) ("The business judgment rule, however, only requires the board to *reasonably* inform itself; it does not require perfection or the consideration of every conceivable alternative.")

[19] *See Aronson*, 473 A.2d at 813 (1984) ("the board may delegate its managerial

time, debate as to the standard of care required by a Board of Directors, the question has largely been settled, and the standard of gross negligence was widely adopted.[20] Gross negligence is defined as "reckless indifference to or a deliberate disregard of the whole body of stockholders or actions which are without the bounds of reason."[21] This is a high burden for a plaintiff to meet, which limits the efficacy of a duty of care claim.[22]

The duty of care requires that the board's judgment be informed and based on an "inquiry directed to the material or advice the board had available to it and whether it had sufficient opportunity to acquire knowledge concerning the problem before acting."[23] In order to be able to sustain a cause of action against a board for a breach of this duty, plaintiffs must prove the board "acted so far without information that they can be said to have passed an unintelligent and unadvised judgment."[24]

C. Duty of Loyalty

The duty of loyalty is a much broader form of liability, covering a variety of possible circumstances, all of which can be derived from the principle that forbids directors to "stand on both sides" of a transaction and prohibits them from deriving "any personal benefit through self-dealing."[25] Essentially, this means that for Directors to abide by the duty of loyalty, they must act only in the

---

authority to a committee of independent disinterested directors").

[20] *See, e.g.*, *Stone v. Ritter*, 911 A.2d 362, 369 (Del. 2006) (discussing "the cond uct giving rise to a violation of the fiduciary duty of care (i.e., gross negligence)"); *Brehm v. Eisner*, 746 A.2d 244, 259 (Del. 2000); *Aronson*, 473 A.2d at 812.

[21] *Tomczak v. Morton Thiokol, Inc.,* C.A. No. 7861, 1990 WL 42607, at *12 (Del. Ch. Apr. 5, 1990) (internal quotations omitted).

[22] Stuart R. Cohn, *Demise of the Director's Duty of Care: Judicial Avoidance of Standards and Sanctions Through the Business Judgment Rule*, 62(4) TEX. L. REV. 591, 591 (1983) ("Duty of care litigation against corporate directors gen erates an abundance of commentary despite a scarcity of successful results. Cases that assess damages against negligent management are rare to the point of becoming an endangered species.").

[23] *Moran v. Household Int'l Inc.*, 490 A.2d 1054, 1075 (Del. Ch. 1985), *aff'd*, 500 A.2d 1346 (Del. 1985).

[24] *Gimbel v. Signal Cos.,* 316 A.2d 599, 615 (Del. Ch. 1974) (quoting *Mitchell v. Highland-Western Glass Co.*, 19 Del. Ch. 326, 330 (Del. Ch. 1933)).

[25] *Anadarko Petroleum Corp. v. Panhandle Eastern Corp.*, 545 A.2d 1171, 1174 (Del. 1988); *see also QC Communications Inc. v. Quartarone*, C.A. No. 8218–VCG, 2014 WL 3974525, at *11 (Del. Ch. Aug. 15, 2014) ("As a fiduciary, Quartarone owed a duty of loyalty to the Company, which he breached in the most funda mental way possible when diverting revenues owed to QC to his own company, Q Media.").

best interest of the corporation and its stockholders.[26] Generally, these aspects of the duty of loyalty are not in question with respect to derivative liability in the wake of a data breach, due to the fact that there is generally no situation where a Director has interest conflicting with those of the company. What is of particular interest within the broader context of the duty of loyalty is the duty of oversight. The duty of oversight is a subset of the broader duty of loyalty, which holds that boards may be liable for a breach of their duty of loyalty to the corporation if they do not take adequate steps to ensure the proper management of the corporation's affairs, even if there is no claim that they had conflicting interests.[27]

Traditionally, a claim based on a theory of the breach of the duty of oversight is referred to as a "*Caremark* claim" in reference to the seminal case *In re Caremark*,[28] wherein Plaintiffs alleged before the Court of Chancery that Directors, by not creating a corporate information and reporting system for monitoring Medicaid kickbacks, breached their duty of care to their stockholders.[29] In defining this cause of action, the Court handed down the following factors:

In order to Show that the Caremark directors breached their duty of care by failing adequately to control [the company's] employees, plaintiffs would have to show either (1) that the directors knew or (2) should have known that violations of law were occurring and, in either event, (3) that the directors took no steps in a good faith effort to prevent or remedy that situation, and (4) that such failure proximately resulted in the losses complained of.[30]

A later court, in elaborating on the scope of *Caremark* liability, summed up the root of the cause of action is that "the directors were conscious of the fact that they were not doing their jobs."[31]

---

[26] *Revlon, Inc. v. MacAndrews & Forbes Holdings, Inc.*, 506 A.2d 173, 182 (Del. 1986); *Guth v. Loft, Inc.*, 5 A.2d 503, 510 (Del. 1939) ("The rule that requires an undivided and unselfish loyalty to the corporation demands that there shall be no conflict between duty and self-interest.").

[27] *Mills Acquisition Co. v. Macmillan, Inc.*, 559 A.2d 1261, 1281 (Del. 1989) ("While a board of directors may rely in good faith upon information, opinions, re ports or statements presented by corporate officers, employees and experts selected with reasonable care [. . .] it may not avoid its active and direct duty of oversight") (internal quotations omitted).

[28] 698 A.2d 959.

[29] *Id.* at 960, 962–63.

[30] *Id.* at 971.

[31] *Guttman v. Huang*, 823 A.2d 492, 506 (Del. Ch. 2003).

Of particular relevance in the data breach context, the Delaware Court of Chancery, in *Yu Kwai Chong*,[32] recently held that "[w]hen faced with knowledge that the company controls are inadequate, the directors must *act*, i.e., they must prevent further wrongdoing from occurring."[33] While that case dealt with an illicit money transfer scheme, the Court maintained that a *Caremark* claim can be sustained when "directors are aware of pervasive, fundamental weaknesses in [the company's] controls and knowingly failed to stop further problems from occurring."[34]

D. Demand on the Board of Directors

In order for a shareholder to be able to bring a derivative suit, they must first demand that the directors bring the suit on behalf of the corporation, unless such a demand would be futile.[35] This is a critical hurdle for plaintiffs to meet, since, in cases where demand is not futile, it gives broad powers to the Directors to determine whether to bring the suit. If the Directors choose not to pursue the claim, their decision is entitled to the protection of the Business Judgment Rule.[36] As has been established earlier, the Business Judgment Rule is a near fatal obstacle in pursuing claims, so plaintiffs have flocked to demand futility as a refuge for their claims.

The Delaware Supreme Court established the following standard in determining demand futility: "[W]hether, under the particularized facts alleged, a reasonable doubt is created that: (1) the directors are disinterested and independent and (2) the challenged transaction was otherwise the product of a valid exercise of business judgment."[37] While there are two prongs for this test, a plaintiff need only meet one of the prongs: "A director will be considered unable to act objectively with respect to a presuit demand if he or she is interested in the outcome of the litigation *or* is otherwise not independent."[38]

---

[32] 66 A.3d 963 (Del. Ch. 2013).

[33] *Id.* at 984.

[34] *Id*. at 971, 984.

[35] *In re eBay, Inc. S'holder Litig.*, C.A. No. 19988–NC, 2004 WL 253521, at *2 (Del. Ch. Jan. 23, 2004, *revised* Feb. 11, 2004). If shareholders believe that dem and would be futile, they must allege the reasons for this belief in their complaint. FED. R. CIV. P. 23.1.

[36] *Oliveira v. Sugarman*, 130 A.3d 1085, 1094–95 (Md. Ct. Spec. App. 2016).

[37] *Aronson*, 473 A.2d at 814.

[38] *Beam v. Stewart*, 845 A.2d 1040, 1049 (Del. 2004) (emphasis added).

The standard contained in *Aronson*[39] only deals with actions undertaken by a board of directors, but demand futility can extend to matters where directors have not taken any action, which is the foundation of a *Caremark* claim. The Delaware Supreme Court applied the *Aronson* standard to Director inaction in *Rales*,[40] where it held that

whether or not the particularized factual allegations of a derivative stockholder complaint create a reasonable doubt that, as of the time the complaint was filed, the board of directors could have properly exercised its independent and disinterested business judgment in responding to a demand. If the derivative plaintiff satisfies this burden, then demand will be excused as futile.[41]

This standard was applied to a case, *White v. Panic*,[42] where plaintiffs alleged a failure to monitor and attempted to claim demand futility.[43] The Court in confronting this question stated that "[d]emand is not excused [. . .] because the allegations of the complaint show that the board has *responded* to this perceived threat, not because the threat does not exist."[44] This will play a critical role in analyzing possible data breach-related *Caremark* claims because the board's knowledge will become critically important.

While the above analysis was not directly related to data breaches, it represents an introduction to the complicated and nuanced world of derivative litigation, the rules of which will be critical in shaping the way shareholders might bring a data breach-related claim, regarding either a Director's breach of their duty of care or duty of loyalty.

III. DATA BREACHES

It is truly the age of the cyber attack; one can no longer pick up a copy of a newspaper without seeing some mention of a data breach, cyber attack, or a variety of other cyber hostilities. In fact, there are so many data breaches that consumers are beginning to report "data breach fatigue."[45] Moreover, these are only the cases

---

[39] *Aronson*, 473 A.2d at 805.
[40] *Rales v. Blasband*, 634 A.2d 927 (Del. 1993).
[41] *Id.* at 934.
[42] 793 A.2d 356 (Del. Ch. 2000).
[43] *Id.* at 359.
[44] *Id.* at 371.
[45] *See* PONEMON INST., THE AFTERMATH OF A DATA BREACH: CONSUMER

that are successful, many companies face daily cyber attacks, any one of which can be the one that breaks through and causes significant harm, or massive data breaches.[46] Before delving into whether companies are prepared, and boards are informed, it is necessary to understand the types of threat that companies are facing.

A. What is a cyber attack

A cyber attack is a "deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft."[47] In more concrete terms, cyber attacks have three primary attack vectors with respect to a system's data: (1) Confidentiality, (2) Availability, and (3) Integrity.[48] These terms, while generally known in the cybersecurity industry, are also federally defined:

- **Confidentiality:** "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information . . . "[49] A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** "guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity . . . "[50] A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** "ensuring timely and reliable access to and use of information . . . "[51] A loss of availability is the disruption of access to or use of information or an information system.

Cyber attacks can take a variety of modalities in order to

SENTIMENT 5 (2014) ("The most frequent [consumer] response to a [data breach] notification is to ignore it and do nothing (32 percent of respondents)").

[46] *See* ROGER OSTVOLD & BRIAN WALKER, BUSINESS RESILIENCE IN THE FACE OF CYBER RISK 2 (Accenture Strategy 2015) ("Two-thirds of executives surveyed . . . said that their organizations experience significant attacks that test the resilience of their IT systems on a daily or weekly basis.").

[47] *Cyberattack*, TECHOPEDIA, https://www.techopedia.com/definition/24748/cyberattack.

[48] *See CIA Triad of Information Security,* TECHOPEDIA, https://www.techopedia.com/definition/25830/cia-triad-of-information-security. In the cybersecurity community, these vectors are commonly referred to as the "CIA triad."

[49] 44 U.S.C.A. § 3552 (West, Westlaw through P.L. 115-140 approved 03/20/18).

[50] *Id.*

[51] *Id.*

compromise any of the above three vectors, but the most common are: (1) Device Compromise, (2) Service Disruption, (3) Data Exfiltration, (4) Bad Data Injection, (5) Advanced Persistent Threat (APT).[52] Cyber attacks are a constantly evolving threat, which require the constant efforts of diligent IT and Information Security departments, both of which require the expenditure of resources which must ultimately be sanctioned by corporate executives and the board of directors.

B. Are Companies and Boards Prepared?

In a study by Accenture, two-thirds of 900 corporate executives surveyed disclosed that their organizations experienced "significant attacks that test[ed] the resilience of their IT systems on a daily or weekly basis. Operational technology systems [were] subjected to cyber attacks nearly every day."[53] Other key findings from the Accenture report were that:

- Nine percent of executives surveyed stated that they proactively run inward-directed attacks and intentional failures to test their systems on a continuous basis.[54]
- Twenty-five percent of executives surveyed stated that they consistently design resilience parameters into their operating model and technology architectures.[55]
- Fifty-three percent have a continuity plan that is refreshed as needed.[56]
- Forty-five percent have produced threat models to existing and planned business operations.[57]

Needless to say, these numbers do not inspire great confidence in the ability or willingness of a company to defend itself, but that is ultimately not the focus of this Article's analysis. What is interesting from the derivative liability perspective is that if executives are in fact aware of the cyber threats their companies face, then Directors too must be similarly aware of these threats. In not taking proper precautionary steps, directors may be opening themselves up to the types of derivative claims discussed above,

---

[52] Miao Lu & Jason Reeves, *Types of Cyber Attacks*, TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID (Sept. 12, 2014), https://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf.

[53] OSTVOLD & WALKER, *supra* note 46, at 2.

[54] *Id*. at 4.

[55] *Id*.

[56] *Id*. at 5.

[57] *Id*.

namely duty of care or failure to monitor claims.

C. A Case Study in Data Breaches: Equifax

On September 7, 2017, Equifax publicly disclosed a series of data breaches that resulted in 143 million consumer records, including Social Security numbers, birth dates, addresses and some driver's license numbers.[58] Additionally, "credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed."[59] While not the largest documented data breach,[60] it is one of the largest breaches, and involves a critical link in the chain of consumer and commercial finance. In using the parlance discussed above, the Equifax data breach can be understood as a cyber attack targeting the confidentiality of data using data exfiltration as its primary modality.[61] How did these cyber criminals successfully breach one of the largest credit agencies in the United States? By exploiting a known vulnerability in a tool used in Web development called Apache Struts.[62] The vulnerability was first discovered by the United States Computer Emergency Readiness Team, who released a notice on March 8, 2017, that Apache, the company in charge of maintaining Apache Struts, had released a patch to the vulnerability.[63]

It is important to understand that a patch, while critically important to updating and securing systems,[64] also provides a

---

[58] *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sept. 7, 2017) https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[59] *Id*.

[60] That honor belongs to two Yahoo! data breaches that resulted in 1.5 million records being compromised. *See World's Biggest Data Breaches,* INFORMATION IS BEAUTIFUL, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (for updated breach figures).

[61] *See supra* Section III.A for further discussion of cyber attacks.

[62] *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes,* EQUIFAX (Sept. 15, 2017), https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

[63] *Apache Software Foundation Releases Security Updates*, UNITED STATES COMPUT. EMERGENCY READINESS TEAM (Mar. 8, 2017), https://www.us-cert.gov/ncas/current-activity/2017/03/08/Apache-Software-Foundation-Releases-Security-Updates.

[64] *See* Andra Zaharia, *15+ Experts Explain Why Software Patching is Key for Your Online Security*, HEIMDAL SEC. (Apr. 6, 2016), https://heimdalsecurity.com/blog/expert-roundup-software-patching/ (explaining that software patching is overlooked by most Internet users but key to maintaining security).

blueprint for cyber criminals to exploit now known and publicly disclosed computer vulnerabilities.[65] Thus, it is imperative that companies actively manage their systems, and apply patches in a timely manner; otherwise they risk falling victim to even unsophisticated criminals that leverage work done by others.[66]

In the case of Equifax, the company did not properly implement the Apache Struts patch, and by May 13, 2017, criminals had successfully exploited the vulnerability and gained control of Equifax systems.[67] From May 13 to July 30, 2017, criminals, acting undetected, exfiltrated approximately 143 million personal records.[68] From July 30, 2017, until disclosing the breach on September 7, 2017, Equifax conducted an internal forensic investigation, and attempted to prepare for the fallout that would result from the public disclosure.[69]

After the breach was disclosed, Equifax, in a matter of days, lost one-third of its market capitalization, and now faces a wide variety of liabilities, including a Department of Justice Investigation,[70] a Federal Trade Commission Investigation,[71] state regulatory actions for improper breach notification practices,[72] private causes

---

[65] *See* Gregg Keizer, *Hackers Now Crave Patches, and Microsoft's Giving Them Just What They Want*, COMPUTERWORLD (May 11, 2014), https://www.computerworld.com/article/2489256/malware-vulnerabilities/hackers-now-crave-patches--and-microsoft-s-giving-them-just-what-they-want.html. ("By conducting before- and after-patch code comparisons, attackers may be able to figure out where a vulnerability lies in Windows 7").

[66] "Script kiddy" is a derogatory term used to refer to individuals that take the work of sophisticated cyber criminals and use preprogrammed scripts to compromise systems. Margaret Rouse, *Script Kiddy (or Script Kiddie)*, TECH TARGET, http://searchmidmarketsecurity.techtarget.com/definition/script-kiddy.

[67] *Equifax Announces Cybersecurity Incident*, *supra* note 58.

[68] *Id.*

[69] *Id.*

[70] Tom McKay, *Equifax's Troubles Grow with News of Prior Breach, DOJ Investigation into Stock Trades*, GIZMODO (Sept. 18, 2017), http://gizmodo.com/equifaxs-troubles-grow-with-news-of-prior-breach-doj-i-1818529191

[71] Brian Fung & Hamza Shaban, *The FTC is Investigating the Equifax Breach. Here's Why That's a Big Deal.*, THE WASHINGTON POST (Sept. 14, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/14/the-ftc-confirms-its-investigating-the-equifax-breach-adding-to-a-chorus-of-official-criticism/?utm_term=.0b090b9d6df4.

[72] *See, e.g.*, *In Wake of Major Equifax Data Breach, AG Healey Launches Investigation and Urges Consumers to Protect Themselves from Identity Theft*, MASS.GOV (Sept. 8, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-09-08-equifax-data-breach.html; Jim Ross, *Attorney General's Office Monitoring Equifax Data Breach*, THE EXPONENT TELEGRAM (Sept. 18, 2017), https://www.wvnews.com/theet/news/local/attorney-general-s-office-monitoring-equifax-data-breach/article_04e7093e-358c-5cac-b4f2-567830a1a1c5.html; Francine McKenna, *Equifax Faces its Biggest Litigation Threat from State*

of actions, such as a data breach class-action lawsuits,[73] and derivative actions.[74] This list is not exhaustive, nor does it include the remediation costs Equifax has already suffered, and will likely continue to pay as the investigation continues.[75] In sum, Equifax may pay out close to or over $1 billion dollars[76] in addition to the multibillion dollar hit to its market capitalization.

While there are certainly many idiosyncrasies to the Equifax data breach—as there are in every data breach—there are certain key lessons that can, and in fact must, be learned for directors across the nation. First and foremost should be the reinforcement that cyber attacks are a serious and real threat that must get consideration from boards. Second, even though there is no way to eliminate the risk of a cyber attack,[77] companies must ensure that they are not making the job easy for cyber criminals by not following basic protocols, such as patch management. Third, incident response must be a critical piece of an organization's cybersecurity posture, otherwise, they risk botching the response and leading to new forms of liability, such as state data breach notification violations.[78] Failing to take these steps into consideration will result in serious liability for the company, and in turn there may be serious liability for directors, personally, through derivative actions.

Attorneys General, MARTKETWATCH (Sept. 15, 2017), http://www.marketwatch.com/story/equifax-faces-its-biggest-litigation-threat-from-state-attorneys-general-2017-09-15 ("Several state attorneys general, including from Illinois, Massachusetts, New York and Pennsylvania, have already contacted Equifax in response to the announcement by the company on Sept. 7").

[73] Polly Mosendz, *Equifax Faces Multibillion-Dollar Lawsuit Over Hack*, BLOOMBERG (Sept. 8, 2017) https://www.bloomberg.com/news/articles/2017-09-08/equifax-sued-over-massive-hack-in-multibillion-dollar-lawsuit

[74] Meena Yoo, *Director Liability in a Data Breach Era,* FORDHAM J. OF CORP. & FIN. L. (Nov. 6, 2017), https://news.law.fordham.edu/jcfl/2017/11/06/director-liability-in-a-data-breach-era/.

[75] *See Equifax Releases Details on Cybersecurity Incident*, *supra* note 62 ("With respect to the company's security posture, Equifax has taken short-term remediation steps, and Equifax continues to implement and accelerate long-term security improvements.").

[76] *See* Mosendz, *supra* note 73. One class action suit seeks as much as $70 billion nationally—a number that is comically disproportionate to the harm suffered but nonetheless highlights the extent of the potential legal liability).

[77] *See You Can't Prevent Every Cyber Attack*, FIREEYE, https://www.fireeye.com/solutions/cyber-security-reimagined.html (advertising cybersecurity services such as crisis response).

[78] *See Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (for citations to state laws on point).

IV. REGULATORY ACTIONS FOR DATA BREACHES

As a practical matter, derivative litigation is almost never initiated *sua sponte* by shareholders, rather they act as parallel proceedings to civil or regulatory actions.[79] While data breach litigation arising in the civil context is generally based on a breach of contract or statutory violation claim,[80] there is no clear statutory provision that empowers agencies to enforce data security.[81] This lack of statutory guidance has allowed the Federal Trade Commission ("FTC") to attempt to fill the regulatory void.[82] The FTC's mission statement is "to protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity."[83] Missing in this description is any reference to data privacy or security. Thus, any reference promulgated cybersecurity regulations must arise under unfair or deceptive business practices. Because federal agencies can conduct their investigations without having to survive a motion to dismiss, their work can be instrumental in aiding shareholders in preparing and pursuing their claims, as was the case in *Wyndham*.

One of the first high profile matter where the FTC brought an action in the wake of a data breach was *FTC v. Wyndham*.[84] In the case, *Wyndham's* property management systems were hacked multiple times, which left 619,000 consumers' private data in the hands of hackers.[85] The FTC filed an action against Wyndham, claiming that Wyndham's data security practices violated §5 of the

---

[79] Jim Ducayet & Nilofer Umar, *Shareholder Derivative Litigation and Parallel Proceedings: Practical and Strategic Implications, Part I*, BUREAU OF NAT'L AFF. (Aug. 25, 2014), http://www.sidley.com/~/media/files/publications/2014/08/shareholder-derivative-litigation-and-parallel-p__/files/view-article/fileattachment/82514-bna-securities-regulation-and-law-report.pdf.

[80] Wayne M. Alder, *Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend a Claim*, BECKER & POLIAKOFF, http://beckerlawyers.com/wp-content/uploads/2018/02/20151001_alder_data_breaches.pdf.

[81] *CFPB Initiates its First Data Security Action*, BALLARD SPAHR LLP (Mar. 3, 2016), http://www.ballardspahr.com/alertspublications/legalalerts/2016-03-03-cfpb-initiates-its-first-data-security-enforcement-action.aspx.

[82] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602, 607 (D.N.J. 2014) [hereinafter *Wyndham* (D.N.J.)]; *LabMD, Inc. v. FTC*, 776 F.3d 1275, 1277 (11th Cir. 2015) (providing recent examples of the FTC using its power to enforce data security).

[83] *About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc.

[84] 799 F.3d 236 (3d Cir. 2015) [hereinafter *Wyndham*].

[85] *Id.* at 241–42.

FTCA,[86] which provides the FTC with the power to "to prevent . . . corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[87]

At the district level, Wyndham raised two objections to the FTC's attempt to bring this type of action under §5: (1) the FTC's lack of authority to assert an unfairness claim in the data-security context, and (2) the FTC must formally promulgate regulations before bringing its unfairness claim.[88] Ultimately, both the district and circuit court disagreed with Wyndham, and held that the FTC had the authority to pursue data security claims under §5.[89] This is a critical expansion for the purposes of derivative litigation because ultimately directors will be forced into exposing themselves to liability in an entirely new realm: namely administrative actions. Quite importantly, if the FTC has this power, companies will be unable to avoid liability if they can disprove harm to the consumer,[90] because the FTC is regulating the practice itself, and not any harm that is fundamental to the issue of standing in civil data breach cases.[91] Additionally, directors may be put into the difficult position of cooperating with government regulators attempting to catch and punish the cyber criminals who perpetrated the attack, and at the same time risking increased exposure to regulators that are investigating claims against them. In sum, even though there are serious questions about the FTC's ability to bring these claims, it is clear that for the moment they are sanctioned, and directors should be on notice for what that means regarding their company's liability, as well as their personal liability.

V. THE CURRENT STATE OF DATA BREACH DERIVATIVE

---

[86] *Wyndham* (D.N.J.), 10 F. Supp. 3d at 607.

[87] 15 U.S.C.A. § 45 (a)(2) (Supp. 2010).

[88] *Wyndham* (D.N.J.), 10 F. Supp. 3d. at 607

[89] *Wyndham*, 799 F.3d at 240; *Wyndham* (D.N.J.), 10 F.Supp.3d at 602.

[90] *See, e.g.*, *In re* LabMD, No. 9357 (F.T.C. Jan. 16, 2014) (order denying respondent LabMD's motion to dismiss) ("[O]ccurrences of actual data security breaches or actual, completed economic harms are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted unfair . . . acts or practices.") (internal citations omitted).

[91] *See generally Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013) (holding the objectively reasonable likelihood that respondents' communications would be acquired under 50 U.S.C. § 1881a at some point in the future was too speculative to establish Article III standing).

LITIGATION

There have been several instances of shareholders bringing a derivative action in the wake of a data breach, but very few have reached a conclusion. The three cases that will be focused on are: (1) Wyndham, (2) Home Depot, and (3) Target. In all of these cases, shareholders brought derivative actions, and in each case the Court dismissed the claims due to procedural rather than substantive hurdles.

A. Wyndham Shareholders File a Derivative Lawsuit

On February 25, 2014, a shareholder of Wyndham Worldwide Corporation, filed a complaint in the District of New Jersey, seeking, *inter alia*, damages incurred by the corporation as a result of the named directors' breaches of fiduciary duty as well as corporate governance reforms to ensure similar cyber attacks would not happen in the future.[92]

The shareholders alleged that "Despite being confronted with the Company's blatantly inadequate security measures, the Individual Defendants failed to implement a system that would provide reasonable and appropriate security for the personal information collected and maintained by [Wyndham]."[93] Interestingly, the shareholders cite several harms to the corporation, and, in addition to the traditional monetary costs, alleged that "[Wyndham's] current and potential customers consider a company's ability to protect their personal and financial information when choosing where to book their travel arrangements. Customers are less likely to book at hotels that cannot be trusted to safeguard their sensitive private information."[94] This theory of harm is generally unavailable for shareholders in other derivative actions because self-interested transactions, for example, have very little effect on consumer perceptions of the company, but data breaches have the potential to be very high profile, and quite damaging, to a company's reputation.

Defendants in this case quickly entered a motion to dismiss, which was ultimately granted by the Court.[95] The bulk of the

---

[92] Verified Shareholder Derivative Complaint at ¶ 1, *Palkon v. Holmes* (D.N.J. 2014) (No. 14CV01234), 2014 WL 11071195.

[93] *Id.* at ¶ 64.

[94] *Id.* at ¶ 68.

[95] *Palkon v. Holmes*, C.A. No. 2:14–CV-01234 (SRC), 2014 WL 5341880, at *1

decision focuses on demand, demand refusal, and the business judgment rule, as well as allegations of bad faith in the demand refusal process. Ultimately, there is minimal discussion on the merits of the shareholder's underlying claims, but the Court explicitly addresses this in a concluding footnote:

Because the law on demand-refusals resolves the motion, the Court need not reach the merits of Plaintiff's underlying claim. It is worth acknowledging, however, that a board considering whether to file suit may consider the merits of the proposed action. Here, Plaintiff's claim rested on a novel theory. *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." *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006). Yet Plaintiff concedes that security measures existed when the first breach occurred, and admits the Board addressed such concerns numerous times.[96]

Essentially, the Court stripped away from these plaintiffs the ability to pursue a *Caremark* claim because they conceded that the directors were conscious of the fact that they were doing their jobs.[97]

Wyndham at its core, demonstrates that directors will not be liable, under a failure to monitor cause of action, for a data breach if they take affirmative steps to ensure some degree of oversight over data security practices. Unfortunately, *Palkon*[98] does not address the duty of care directly.

B. Home Depot Shareholders File a Derivative Action

On August 25, 2015, Home Depot shareholders filed a shareholder complaint against the Board of Directors of Home Depot, alleging breaches of fiduciary duty, and seeking damages incurred by the corporation as a result of the breaches of fiduciary duty, and corporate governance reforms to ensure that similar events would never happen again.[99] The crux of the shareholder's

---

(D.N.J. Oct. 20, 2014).

[96] *Id.* at *6 n.1.

[97] *Guttman*, 823 A.2d at 506.

[98] *Palkon v. Holmes*, C.A. No. 2:14–CV–01234 (SRC), 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

[99] Verified Shareholder Derivative Complaint at ¶ 175, *In re Home Depot S'ho lder Derivative Litig.*, 223 F. Supp. 3d 1317 (N.D. Ga. Aug. 25, 2015) (No. 1:15–CV–2999).

argument was that the Board of Directors of Home Depot "were well-aware that a data security breach such as the one that occurred from April to September 2014 was a substantial 'Risk Factor' for the Company."[100] To evidence this awareness the plaintiffs cite to a litany of various notifications, ranging from payment processing forensic experts, to letters of notice from Visa, to reports issued by security consultants.[101] The plaintiffs in Home Depot cite to data breaches, such as Target and Neiman Marcus, to evidence the climate of corporate data breaches, which Home Depot would be aware of, and consequently be put on greater notice.[102] Essentially, the plaintiffs allege that in the age of the data breach, the duties owed by directors for cyber-related matters may be heightened relative to the panoply of duties owed more generally to the company and its stockholders.[103] While the plaintiff did not press this point beyond a mere paragraph, there may be great force behind that idea.[104]

In an opinion dismissing the case, the Court held that since no demand was made onto the Directors (a fact that was not in contention), the plaintiff needed to show that demand was futile; otherwise the claim would need to be dismissed.[105] The Court engaged in a detailed analysis of the interests of each of the Directors in the case, and ultimately found that demand was not in fact futile.[106] The Plaintiffs appealed the Court's decision, but ultimately the case was settled before a higher court could render judgment.[107]

C. Target Shareholders File a Derivative Action

Arguably one of the most infamous data breaches occurred during the 2013 holiday season, where approximately 40 million

---

[100] *Id.* at ¶ 28.

[101] *Id.* at ¶ 34, 45, 47.

[102] *Id.* at ¶ 48.

[103] *See id.* at ¶ 154 (discussing the directors' failure to act despite knowledge of "the magnitude of damage that a data breach could cause").

[104] *See infra* VI. for more discussion ("What Should Boards Be Doing to Prepare Themselves and Their Companies?").

[105] *In re Home Depot S'holder Derivative Litig.*, 223 F. Supp. 3d at 1323. "It is undisputed that no demand was made in this instance. The Plaintiff shareholder thus has the burden of demonstrating that demand is excused because it would have been futile."

[106] *Id.* at 1332.

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

Target customers had their payment card records stolen by hackers.[108] This spawned massive litigation, which has ultimately settled with Target paying out over $100 million to various parties.[109] This led to shareholders filing a derivative suit seeking to hold the directors and officers of Target liable for the damages incurred by the company as a result of their alleged breaches of fiduciary duties.[110]

The shareholders focused their allegations on how the board "breached their duty of loyalty by knowingly [. . .]: (i) failing to implement a system of internal controls to protect customers' personal and financial information; (ii) failing to oversee the (inadequate) internal controls that failed to protect customers' personal and financial information . . . "[111] In sum, this meant that their cause of action was of a *Caremark* nature. While a similar underlying cause of action, this case represents a quite different cause of action to the above Home Depot derivative suit. This demonstrates the variety of tools prospective plaintiffs have in their arsenal.

VI. WHAT SHOULD BOARDS BE DOING TO PREPARE THEMSELVES AND THEIR COMPANIES?

Many commentators have begun to realize that in today's legal climate boards that do not take affirmative steps to stay on top of their company's cyber security policies face significant liability from a variety of fronts. One of the biggest proponents of this position is former SEC Commissioner Luis Aguilar, who stated that "boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."[112] Commissioner Aguilar went on to state that "evidence suggests that there may be a gap that exists between the magnitude of the exposure presented by cyber-risks and the steps, or lack thereof, that many corporate boards have taken to address these risks."[113]

---

[108] *Target Investigating Data Breach*, KREBS ON SECURITY (Dec. 19, 2013), http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

[109] Ahiza Garcia, *Target Settles for $39 Million Over Data Breach*, CNN (Dec. 2, 2015), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/.

[110] Verified Consolidated Shareholder Derivative Complaint at ¶ 1, *Davis v. St einhafel*, No. 14-cv-00203-PAM-JJK (D. Minn. July 18, 2014).

[111] *Id.* at ¶ 152.

[112] Luis A. Aguilar, Comm'r, Sec. & Exch. Comm'n, Address at the NYSE "Cyber Risks and the Boardroom" Conference (June 10, 2014).

[113] *Id.*

Suffice it to say that when an SEC Commissioner speaks before a roomful of directors at the New York Stock Exchange, they should be put on notice that they must implement meaningful oversight and focus on cybersecurity issues.

If boards want to follow the advice of people like Commissioner Aguilar and close the gap of cyber risk and response at their company, what steps should they take?

First and foremost, boards must elevate cybersecurity to an "enterprise-level risk management" issue.[114] This means preparing for a breach, as well as preparing meaningful post-breach procedures.[115] This is a cross departmental endeavor that requires meaningful input from technical, legal, and business stakeholders. While these steps are no doubt beneficial to any defenses for claims that may arise in a derivative data breach lawsuit, they are not the only steps that directors can take to limit their liability.

As has been demonstrated above, shareholders have a claim when directors have failed to monitor or breached their duty of care to the shareholder. This means that in order for boards to defend themselves, they must create adequate cybersecurity monitoring procedures, as well as ensure that those procedures are faithfully followed. How can boards do this? There may be a wide variety of ways to answer this question, but one possible way is to create a cybersecurity audit committee, with the resources necessary to retain outside advisors, whose job it is to audit and recommend improvements to the company's cybersecurity policies. This option is particularly appealing because a recurring theme found throughout the above lawsuits was communication between cybersecurity employees and the board. This is a concern that would be effectively resolved by the establishment of a

---

114 Michelle A. Reed et al., *Fiduciary Duties of Directors Are Key to Minimizing Cyber Risk*, NACD DIRECTORSHIP, May/June 2015, at 41.

115 For a compelling breakdown of the cybersecurity steps a board can take, *see* U.S. DEP'T OF COMMERCE: NIST, *Cybersecurity Framework Core*, http://www.nist.gov/cyberframework/upload/framework-for-improving-critical-infrastructure-cybersecurity-core.xlsx. (The Framework Core offers the following breakdown for cybersecurity readiness: Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). Within these subcategories, the Framework Core tracks what regulations can be employed to achieve its goals. While the Framework Core is generally used to secure critical infrastructure, there is nothing that would prevent a private entity from using and learning from the Framework Core, which is one the best cybersecurity frameworks available. *See also* PRICEWATERHOUSECOOPERS, *Why You Should Adopt the NIST Cybersecurity Framework* (May 2014), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf (for further discussion of the Framework).

cybersecurity audit committee. Finally, if companies begin to implement a cybersecurity audit committee, the policy will become an industry standard, which will further reinforce the need to for boards to accept them.

VII. CONCLUSION

As time goes on, data breaches will continue to play a greater role in the corporate world. Courts to date have not yet arrived at the underlying issues of cyber-derivative liability; rather they have centered their analysis on the hurdles discussed earlier. With the ever-rising number of data breaches, it is inevitable that a case will arise in which the Business Judgment Rule and the Demand requirement will not impede a claim, and Directors will be held liable for insufficient or improper action or inaction. This rise, will force boards to confront the issue, or if they continue acting without regard and consideration to cyber risks, they will face increasing personal liability risks. Unlike most derivative contexts, data breaches deal largely with external threats rather than internal controls, which further evinces the need for effective risk management and cyber security practices, and director liability for a lack thereof. This is an issue that is on the minds of regulators, executives, and most importantly consumers. If companies, led by their boards, do not make sufficient progress, they will be forced into the history books, even if stock prices and financial fundamentals don't reflect that risk. Ultimately, data breaches are a problem that will not go away without careful attention and dedication, but boards are uniquely situated to help order the affairs of a company in such a way as to minimize these risks.