U.C. Berkeley School of Law: Berkeley Center for Law, Business & the Economy

Current Trends in Cybersecurity: Board Liability & Best Practices

Richard Hardack
Samuel N. Weinstein

(Working Draft – 4/21/17)

This White Paper addresses legal standards governing Board of Director ("Board") personal liability for cybersecurity issues, best practices for managing cyber threats, and Corporate Social Responsibility ("CSR") aspects of cybersecurity. It does not discuss broader issues of corporate performance or business strategy, reputation, or general liability. The paper focuses on shareholder derivative (rather than class action) lawsuits because they can target Board members for personal liability.

I. Background:

A. A Growing Threat

Cyber-attacks are a growing threat. In a recent survey of nearly a thousand top executives (including chief executive officers, chief information officers, chief technology officers and chief operating officers), "63 percent said their companies were under daily or weekly attack."[1] Many enterprises that handle sensitive information—particularly those operating in the financial, healthcare and large-scale retail sectors—are subject to even more frequent and serious cyber-attacks.[2] But any entity that stores or transmits financial or sensitive information can be a tempting target for data-thieves: as of 2015, for example, "[a]ccording to some analysts, 80% of the top law firms have been hacked at least once in the last five years."[3] If your corporation hasn't been hacked, it likely means you have exceptional security measures in place or your business isn't worth breaching.

B. Boards Slow to Adapt

For years, many Boards were not paying sufficient attention to cybersecurity threats, and taking woefully inadequate preventive measures to address them:

---

1 Katy Barnato, *Most firms face 'significant' daily or weekly cyberattacks: Report*, CNBC, July 29, 2015, http://www.cnbc.com/2015/07/29/most-firms-face-significant-daily-or-weekly-cyberattacks-accenture.html.
2 *See, e.g.*, Scott J. Shackelford et al., *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995, 2004 (2016). (citations omitted) (noting that "Certain industries, including those related to "critical infrastructure," seem to be particularly at risk of cyber attacks . . .. There are, however, some inconsistencies between reports. For example, according to Verizon's recent Data Breach Investigation Report, the hospitality and retail industries were the most at risk of a data breach").
3 Litigation Committee, Association of Corporate Counsel, *Law Firm Cybersecurity, Questionnaire and Guide,* http://webcasts.acc.com/handouts/Microsoft_Word_-_Law_Firm_Cybersecurity_rev6.docx_-_loader.cfm.pdf.

> A recent Thompson Reuters survey, for example, found that half the boards it surveyed did not use a secure form of data portal or secure file transfer system. Meanwhile, more than half relied on printed rather than encrypted data and had no system to determine how those documents were secured, tracked, archived, and disposed of. And the majority of board members surveyed used personal mobile and computing devices and commercial email accounts to access company data, making it all the more difficult to secure and monitor access to such information adequately.[4]

For roughly the past decade, surveys revealed similarly alarming statistics that highlighted the divergence in sensibility between Boards and cybersecurity experts, and between the level of threat and the level of response. The survey of top executives cited above that said that 63 percent of companies were under daily or weekly attack also revealed that only 9 percent "said their companies ran dummy attacks to test their systems on a regular basis."[5] Further, "in a recent survey, nearly 80 percent of the more than 1,000 information technology leaders surveyed had not briefed their board of directors on cybersecurity in the last 12 months."[6] The level of preparedness remains surprisingly low in some critical areas:

> According to the Georgia Tech [Information Security Center 2015 Report on Governance of Cybersecurity: How Boards & Senior Executives Are Managing Cyber Risks ("Georgia Tech Report")], 63 percent of respondent boards are actively addressing and governing computer and information security, including reviewing security budgets, designating roles and responsibilities for the management of privacy and security, developing and reviewing top-level policies, receiving regular reports on security risks and incidents, reviewing annual risk assessments of the security program and reviewing cyber-incident response plans. . . . The Security Survey found that 45 percent of boards participate in overall security strategy and 37 percent participate regarding security technologies. . .. 82 percent of boards regularly or occasionally received reports from senior management regarding privacy and IT security risks. . .. 47 percent of respondents said their board regularly or occasionally reviewed and approved roles and responsibilities of personnel responsible for privacy and security risks. . .. 32 percent of boards review security and privacy risks and 35 percent of security leaders deliver information security risk updates to the board at least four times a year.[7]

---

4 Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 626–27 (2015) (citation omitted).

5 Barnato, supra note 1.

6 Michelle A. Reed et al., *Fiduciary Duties of Directors Are Key to Minimizing Cyber Risk* (June 3, 2015), https://www.akingump.com/images/content/3/6/v2/36491/NACD-article.pdf.

7 Melissa J. Krasnow, *Director Cybersecurity Risk Oversight and Actions*, Privacy & Security Law Report, 15 PVLR 64, 1/11/1, http://documents.jdsupra.com/daf8857c-125a-42d5-9354-6ed392998c1c.pdf. For the Georgia Tech report, see https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/governance-of-cybersecurity.

As of roughly 2014, therefore, high percentages of Boards still were not adequately implementing many of the security measures addressed in most surveys and recommended by most experts. However, no doubt in part because of the number of high-profile, high-stakes breaches of corporate cybersecurity in recent years, including the hacks into the Sony Corporation, Target, and the Wyndham Hotel Chain, and the 2015 release of the Panama Papers—which included nearly twelve million documents previously in the possession of the Panamanian law firm Mossack Fonseca—Boards have become increasingly cybersecurity-conscious: "According to a 2013 Risk Management Society Survey, risk professionals ranked cyberrisk as their top risk priority, while senior executives ranked it only twenty-sixth. However, executive perceptions of cyberrisk are changing—a 2014 survey of directors reveals that data security is now the top issue keeping them awake at night."[8]

C. On-Line Gambling:

The frequency and scale of cyber-attacks should remind Boards that they are engaging in high-risk activities—gambling against the odds that they won't be victims of data breaches—if they fail to develop an ongoing, comprehensive approach to their corporation's specific risks. For example, in 2013, 150 million Adobe customers and 70 million Target customers were affected by data breaches; the following year, 76 million accounts at JP Morgan Chase and 56 million accounts at Home Depot were hacked, and eBay advised 145 million users to change their passwords after their personal information had been compromised.[9]

Malware and hacks can function like sleeper cells within corporate networks; they can go undetected for months, slowly siphoning confidential data until they have infiltrated every critical aspect of a firm's electronic infrastructure.[10] In the shareholder derivative suit filed against Home Depot, which named Directors and Officers individually, plaintiffs alleged that the company failed to implement reasonable security measures to safeguard the information of 56 million customers, and that what its own CEO labeled desperately out of date security measures left "in place glaring vulnerabilities that not only allowed hackers to enter the system undetected but permitted them to

---

[8] John E. Black Jr., *Awake at Night: Cyberbreaches and the New Risk to Directors and Officers*, October 2014, https://www.irmi.com/articles/expert-commentary/awake-at-night-cyberbreaches-and-the-new-risk-to-directors-and-officers.

[9] Victoria C. Wong, *Cybersecurity, Risk Management, and How Boards Can Effectively Fulfill Their Monitoring Role*, 15 U.C. DAVIS BUS. L.J. 201, 202 (2015) (citations omitted).

[10] In addressing standing to sue for corporate loss of private data, courts can consider actual injury as well as potential harm when the latter seems likely to occur and is based on existing injury:

> [Clapper v. Amnesty International USA, 133 S.Ct. 1138, 1147 (2013)] stated that "[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." 133 S.Ct. at 1150 n. 5 (2013) (citation omitted). . ..
>
> Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an "objectively reasonable likelihood" that such an injury will occur.

Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692–93, 696 (7th Cir. 2015) (citations omitted).

continue siphoning customer cardholder and personal data for almost five months without detection."[11]

Shareholders can sue corporations, and in some instances Board members, for loss of reputation and a drop in share price—which some studies have shown can be significant[12]—and the real and perceived costs of data-loss. Even if they don't face personal liability, Board members confront a loss of personal reputation, a potential drop in share price, and significant legal costs even when they successfully defend against lawsuits related to data-loss. Target's breach, for example, likely cost the company nearly $1 billion as a result of fraudulent credit card use and hefty fines. Defending the class action lawsuits that are sure to follow such breaches is costly, even if those lawsuits face significant obstacles. Corporations also risk losing proprietary information and the trust and business of customers: "US companies estimated losing $3.3 million in business on average due to data breaches in 2013. . .. [A] recent study found that nearly 60 percent of breach fraud victims 'significantly lost trust' in their retailers and 14 percent avoided their retailer altogether due to the fraud potential."[13] Until a few years ago, an inadequate Board response might have reflected an understandable lack of awareness of the threats at issue; today, it likely would demonstrate a dangerous inability to appreciate both the myriad kinds of cyber-threats corporations face and the multitude of statutes, laws, and regulations that apply across agencies, industries, and continents. The challenges Boards face are practical, legal, financial, and informational.

A Board must navigate a patchwork of regulations that are often industry-specific, sometimes only contextually voluntary, and occasionally vague or broad: in the U.S.,

> the Securities and Exchange Commission ("SEC"), the Department of Justice ("DOJ"), the Department of Homeland Security ("DHS"), the Federal Trade Commission ("FTC"), the Federal Communications Commission ("FCC"), the Financial Industry Regulatory Authority ("FINRA"), and the Consumer Financial Protection Bureau . . . are taking data security seriously and will hold boardrooms accountable. . .. [But t]he U.S. government, for example, has yet to release a cross-agency data security best-practices manual that gives adequate assurance and instruction to board members.[14]

---

[11] Complaint at 2, Bennek v. Ackerman, No. 1:15-cv-2999 (N.D. Ga. Sept. 2, 2015).

[12] *See, e.g.*, Matthew Heller, *Cyber Attacks Can Cause Major Stock Drops*, CFO (April 12, 2017) (citing study by security consultant CGI and Oxford Economics showing "an average decline" in stock prices "of 1.8% on a permanent basis in cases of severe breaches" and noting that "in some cases, breaches have wiped as much as 15% off companies' valuations.") Other studies have shown less significant drops in share price post-breach. *See, e.g.*, Elaine Kvochko & Rajiv Pant, *Why Data Breaches Don't Hurt Stock Prices*, Harvard Business Review (March 31, 2015) ("stock prices during and following the high profile security data breaches . . . in the past several years have decreased slightly or quickly recovered from the breach.")

[13] Black, supra note 8.

[14] Davis et al., 2015 COLUM. BUS. L. REV. at 618, 627. For example, the SEC has "noted that "risk oversight is a key competence of [a] board." Reed et al., supra note 6. Generally, the FTC uses a sliding scale and "a flexible approach to data security to analyze whether companies' practices are reasonable and appropriate in light of the risks and vulnerabilities they face."
https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-comment-fcc-concerning-proposed-cyber-security-certification-program/101013fcccomment.pdf.

Meanwhile, many of the protocols regulatory agencies and private institutes recommend overlap, but they do so imperfectly or vary in details. Boards therefore can try to synthesize best practices; focus on their industry standards; or, to be safest, follow the best practices that apply most widely across industry sectors.

Both regulatory agencies and courts look favorably on systemic approaches that include an overarching framework to address cybersecurity issues throughout an enterprise. The National Association of Corporate Directors ("NACD") published a Cyber-Risk Oversight Handbook proposing that Directors should "set the expectation that management will establish an enterprise-wide cybersecurity risk management framework with adequate staffing and budget."[15] Virtually all research that addresses cybersecurity, such as that published by the National Institute of Standards and Technology ("NIST"), recommends that Directors develop "an organization-wide approach to managing cybersecurity risk."[16]

II. Overview of Board Duties:

What are the duties of Board members in the face of growing cyber threats? Because courts will not "equate a bad outcome with bad faith" on the part of a Board of Directors—i.e., will not assume a breach is itself evidence per se of fault—it is imperative that Board members make and document good faith efforts to secure data.[17] Board members likely will not sustain personal liability for negligent acts in dealing with cybersecurity, only for willful disregard, conscious misrepresentations and bad faith or unreasonable failures to act at all. Paradoxically, Board members can develop a false sense of cybersecurity while having an accurate sense of their immunity from personal liability.

A. Board Liability Standards

While corporations face significant exposure and costs in relation to any serious data breach, Board members generally will be protected from personal liability if they take some active and contextually reasonable measures—and not necessarily the most efficient, appropriate or successful ones—to evaluate and meet their corporation's cybersecurity needs.

In one of the most important cases to address Board liability, the court in In re Caremark International stressed that Boards are required to mount some kind of response to legal compliance issues, but will not be held accountable for failing in that response.[18] Caremark did not address cybersecurity issues, but the alleged failure of the Board to investigate whether a company with which Caremark had merged had been paying illegal management fees to physicians in possible exchange for referrals to Medicare and Medicaid services for which Caremark received reimbursements.[19] In light of the record, the court found a very low probability that Caremark's directors

---

By contrast, the FDA issues targeted regulations, for example on certain medical device makers, but can also suggest somewhat vague goals. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm.

15 Krasnow, supra note 7.

16 *The NIST Framework for Improving Critical Infrastructure Cybersecurity*, https://www.nist.gov/programs-projects/cybersecurity-framework, p. 11.

17 Stone v. Ritter, 911 A.2d 362, 373 (Del. 2006).

18 698 A.2d 959, 961 (Del. Ch. 1996).

19 Id. at 962.

> breached any duty to appropriately monitor and supervise the enterprise. Indeed, the record tends to show an active consideration by Caremark management and its Board of the Caremark structures and programs that ultimately led to the company's indictment and to the large financial losses incurred in the settlement of those claims. It does not tend to show knowing or intentional violation of law. Neither the fact that the Board, although advised by lawyers and accountants, did not accurately predict the severe consequences to the company that would ultimately follow from the deployment by the company of the strategies and practices that ultimately led to this liability, nor the scale of the liability, gives rise to an inference of breach of any duty imposed by corporation law upon the directors of Caremark.

1. An Epic Fail Test

Caremark effectively establishes an "epic fail" test regarding Board oversight responsibilities, which can be extended to apply to cybersecurity. In practice, Boards have a duty to monitor security threats, but not necessarily monitor them well or effectively. To incur liability, Board members must knowingly or in bad faith abjectly fail to fulfill their duty of care; courts will not evaluate the success of Board measures, but the reasonableness of Boards' efforts to oversee cybersecurity, and to stay informed about and respond to risks:

> [T]he duty to act in good faith to be informed cannot be thought to require directors to possess detailed information about all aspects of the operation of the enterprise. Such a requirement would simply be inconsistent with the scale and scope of efficient organization size in this technological age. . ..
>
> Generally where a claim of directorial liability for corporate loss is predicated upon ignorance of liability creating activities within the corporation . . . *only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists—will establish the lack of good faith that is a necessary condition to liability*. Such a test of liability—lack of good faith as evidenced by sustained or systematic failure of a director to exercise reasonable oversight—is quite high. . .. .[20]

Such passages in Caremark likely mean that if a Board takes even intermediate and inadequate security measures, it likely would interrupt and neutralize what could otherwise be a "sustained failure" to address cybersecurity.

The Caremark court approved of the timeliness of Board members' responses, their reliance on outside experts, and their informed implementation of updated policies:

> Caremark had an internal audit plan designed to assure compliance with business and ethics policies. . .. [T]he Ethics Committee of Caremark's Board received and reviewed an outside auditor's report by Price Waterhouse . . .

[20] Caremark, 698 A.2d at 971-72 (emphasis added).

> Despite the[ir] positive findings . . . the Audit & Ethics Committee adopted a new internal audit charter requiring a comprehensive review of compliance policies and the compilation of an employee ethics handbook concerning such policies.
>
> The Board appears to have been informed about this project and other efforts to assure compliance with the law. . .. Caremark continued these policies in subsequent years, causing employees to be given revised versions of the ethics manual and requiring them to participate in training sessions concerning compliance with the law. . ..
>
> Caremark took several additional steps which appear to have been aimed at increasing management supervision,

including requiring local managers to certify compliance with the corporation's ethics program; appointing the CFO to serve as its compliance officer; and publishing a fifth revised Internal Guide to Contractual relationships.[21]

Shareholders sued Caremark nonetheless, claiming, among other things, that the Board failed to supervise employee conduct or implement sufficient corrective measures: their complaint

> charge[d] the director defendants with breach of their duty of attention or care in connection with the on-going operation of the corporation's business. The claim is that the directors allowed a situation to develop and continue which exposed the corporation to enormous legal liability and that in so doing they violated a duty to be active monitors of corporate performance. . .. The theory here advanced is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment.[22]

On the grounds of both precedent and policy, the court articulated a very low standard for Boards and a very high hurdle for plaintiffs.

2. Board Liability Attaches Only for Doing Virtually Nothing

The court invoked two theories under which Board members still might be held liable for breaches, but validated only one that would apply in the context of a typical cyber-breach: liability could follow from a loss that arose from a putatively negligent Board decision or from an "unconsidered failure" to act in ways that might have prevented the loss.[23]

The first class of liability, for making bad decisions in good faith, is subject to the business judgment rule and generally will not apply to a Board in the context of cybersecurity measures: courts will review only a failure to act reasonably. Caremark indicates that courts will not second-guess Board decisions under the business judgment rule when they do apply that standard: "[W]hether a judge or jury considering the matter after the fact, believes a decision

---

[21] Caremark, 698 A.2d at 963.
[22] Caremark, 698 A.2d at 964, 967.
[23] Caremark, 698 A.2d at 967.

substantively wrong, or degrees of wrong extending through 'stupid' to 'egregious' or 'irrational,' provides no ground for director liability, so long as the court determines that the process employed was either rational or employed in a good faith effort to advance corporate interests."[24]

Caremark then discussed the theory for potential Board liability that more likely would pertain to data breaches—a knowing *failure* to take any measures to address cybersecurity issues: "The second class of cases in which director liability for inattention is theoretically possible entail circumstances in which a loss eventuates not from a decision but, from unconsidered inaction."[25] The court affirmed that a "director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards."[26] In practice, however, in the Board liability context, courts likely will not evaluate the sufficiency of efforts to defend against cybersecurity threats, only their existence:

> [T]he fact that the Caremark Board already has a functioning committee charged with overseeing corporate compliance, the changes in corporate practice that are presented as consideration for the settlement do not impress one as very significant. Nonetheless, that consideration appears fully adequate to support dismissal of the derivative claims of director fault asserted, because those claims find no substantial evidentiary support in the record and quite likely were susceptible to a motion to dismiss in all events.

[27]A court might yet find that a Board's false belief its corporate data was secure was unreasonable and therefore culpable, but so far courts have clearly distinguished false belief from actual knowledge, and any form of bad decision from bad faith.

Other cases reinforce this lenient standard. Addressing its state's corporate law, in Stone v. Ritter the Delaware Supreme Court held that

> Caremark articulates the necessary conditions predicate for director oversight liability: (a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention. In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations.[28]

---

[24] Caremark, 698 A.2d at 967-68.

[25] Caremark, 698 A.2d at 968-69.
[26] Id. at 970.
[27] Id. at 970-71.
[28] Stone, 911 A.2d at 370.

We might call this the ostrich or see no evil theory of liability; Board members risk personal exposure only if they knowingly, and probably ardently, pretend not to know what they know and respond accordingly by doing virtually nothing.

At issue in Stone was AmSouth's payment of $50 million in fines and penalties to resolve government and regulatory inquiries into bank employees' failure to file "Suspicious Activity Reports" required under the federal Bank Secrecy Act and other anti-money-laundering [AML] regulations.[29] The Financial Crimes Enforcement Network, a bureau of the Department of the Treasury, had determined that the bank's AML compliance "program lacked adequate board and management oversight," and that "reporting to management for the purposes of monitoring and oversight of compliance activities was materially deficient."[30]

Evidencing Caremark's continuing influence, and the lenient approach of courts relative to some regulatory agencies, the Stone court affirmed the dismissal of all claims against the Board; it emphasized that Board members could face liability for such compliance failures only if they had acted, or more likely not acted at all, in a manner that could be labeled as being in bad faith.[31] To succeed in a derivative suit, shareholders must "plead the existence of "red flags"—"facts showing that the board ever was aware that [a corporation's] internal controls were inadequate, that these inadequacies would result in illegal activity, and that the board chose to do *nothing* about problems it allegedly knew existed."[32] This is a high bar. Indeed, despite the escalating number of cyber-breaches, "no derivative action brought by a shareholder against a Board for breach of cyberfiduciary duty has succeeded" or even survived a motion to dismiss.[33]

Courts apply a similar standard when evaluating a Board's response to shareholder demands to file a derivative suit. That the Wyndham Board took "numerous steps" to familiarize itself with the subject matter of the plaintiffs' demand again demonstrated that it had made a reasonable effort to respond to the issues raised.[34] With regard to shareholder demands after the fact of a data breach, Courts seem to validate even cursory investigations in ways that comport with their validations of good faith efforts to prevent breaches before the fact: "Given the business judgment rule's strong presumption, courts uphold even cursory investigations by boards refusing shareholder demands. See Levine v. Smith, 591 A.2d 194, 199, 214 [(Del. 1991)] (upholding investigation where board merely wrote to plaintiff that it had reviewed the demand and found that pursuing it would not be in the corporate interest)."[35]

---

[29] Id. at 365.
[30] Id. at 366.
[31] Id. at 369-70. Board members generally will face exposure from failing to fulfill their duty of loyalty rather than their duty of care (which would usually cover business decisions): "The typical provision in a company's certificate of incorporation under 8 Del. C. § 102 (b)(7) exculpating directors from monetary damages resulting from conduct amounting to a breach of the duty of care will preclude any attempt to base liability on an alleged failure to exercise due care in overseeing the company's cybersecurity controls and procedures." Timothy A. Miller et al., *Director Liability for Data Breaches: How Real is the Risk?* (July 9, 2015), https://www.skadden.com/sites/default/files/publications/Director_Liability_for_Data_Breaches_How_Real_is_the_Risk.pdf.
[32] Id. at 370 (emphasis added).
[33] Harris Yegelwel, *Cybersecurity Oversight: A Cautionary Tale for Directors*, 20 J. TECH. L. & POL'Y 229, 246 (2015).
[34] Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 WL 5341880, at *5 (D.N.J. Oct. 20, 2014).
[35] Id. at *6.

3. The Enemy Within:

With good reason, Board members likely will first imagine "professional" hackers and outside agents as the primary threats to their corporation's data, but they should also remember to address current and former employees and the opportunistic amateur. While "[a]ccording to the Identity Theft Resource Center, cyberattacks caused more than 25 percent of the data breaches reported in 2013," at least 10% were caused by insider misuse, error or some form of theft.[36] In other words, Boards should not focus entirely on preventing sophisticated hacks, but also take measures to prevent more "basic" threats, such as employee theft and failure to erase and secure mobile devices. However, in the absence of particularized suspicion, Boards likely will not be expected to anticipate that their own corporate employees pose a specific security threat: "absent cause for suspicion there is no duty upon the directors to install and operate a corporate system of espionage to ferret out wrongdoing which they have no reason to suspect exists."[37]

In a discussion relevant to the contemporary form of espionage—data theft—the Caremark Court added that Graham v. Allis-Chalmers Manufacturing Co., 188 A.2d 125 (1963), "can be more narrowly interpreted as standing for the proposition that, absent grounds to suspect deception, neither corporate boards nor senior officers can be charged with wrongdoing simply for assuming the integrity of employees and the honesty of their dealings on the company's behalf."[38] Summarizing the standard of liability regarding a Board's oversight of employees, the Court required plaintiffs to prove that "the Caremark directors breached their duty of care by failing adequately to control Caremark's employees" by showing "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 . . . ."[39]

If Board members have instantiated some kind of system in good faith, courts generally will not second guess their efforts to impose liability, and won't hold them accountable for bad employee behavior of which they were unaware: "In the absence of red flags, good faith in the context of oversight must be measured by the directors' actions 'to assure a reasonable information and reporting system exists' and not by second-guessing after the occurrence of employee conduct that results in an unintended adverse outcome."[40]

In sum, if Boards make a good faith effort to confront and redress cybersecurity issues, members likely will not be held personally liable. Considering the magnitude of cyber-threats, genuinely effective planning that prevents breaches might prove more challenging, however.

III. Best Practices

Despite the high bar for personal Board liability, general counsels and board members should adopt best practices to protect companies from reputational damage and class-action law suits, and because that bar could fall as cybersecurity protocols increasingly become standardized and adopted.

---

[36] Black, supra note 8, citing the *2014 Verizon Data Breach Investigations Report*.
[37] Caremark, 698 A.2d at 969 (citation omitted).
[38] Id.
[39] Id. at 971.
[40] Stone v. Ritter, 911 A.2d 362, 373 (Del. 2006).

A. A Tangled Web of Laws and Standards

Almost all complaints against corporations for data breaches are likely to invoke multiple state and often federal laws.[41] To obtain a comprehensive overview of potential liability, relevant laws, and disparate requirements, it will be necessary to conduct a jurisdictional review of the laws in all the states and circuits in which a corporation does business. For a wealth of information on integrating and synthesizing the numerous standards, best practices and controls that government agencies and NGOs recommend, see the Center for Internet Security's Critical Security Controls for Effective Cyber Defense.[42] Given the uncertainty in the regulatory arena, the safest approach is to adopt the most rigorous protocols available across jurisdictions. SEC Commissioner Aguilar warned in 2014 that "boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."[43]

Boards should initiate entirely separate reviews if the corporation conducts business abroad. For example, one international industry standard is provided under the ISO/IEC 27001:2013 (Information technology – Security techniques – Information security management systems – Requirements), which offers voluntary cybersecurity standards and checklists for corporations operating worldwide (as well as certification).[44]

In terms of enforcement, "The Council of Europe Convention on Cybercrime, which has been signed by 54 countries and ratified by 47 (including the U.S.), holds companies civilly, administratively, or criminally liable for cybercrimes that benefit the company and were made possible due to the lack of supervision or control by someone in a senior management position, such as an officer or director."[45] In part because "European regulators struck down the longstanding international Safe Harbor agreement, which had enabled American companies working in the European Union to transfer data painlessly," the regulatory framework remains inchoate, and could get more complex and fragmented after Britain leaves the European Union.[46]

---

41 For example, Plaintiffs' Complaint raised seven claims in the Target case: "Count One contend[ed] that Target violated the consumer protection laws of 49 states (all states save Alaska) and the District of Columbia. Count Two allege[d] a similar violation with respect to the data breach statutes of 38 states. Count III assert[ed] that Target was negligent in failing to safeguard its customers' data." In re Target Corp., 66 F. Supp. 3d 1154, 1158.

42 Available at https://www.cisecurity.org/critical-controls/Library.cfm.

43 Black, supra note 8.

44 See https://www.iso.org/isoiec-27001-information-security.html. Board members should keep in mind, however, that though some "EU jurisdictions have codified the business judgment rule, or something similar, many others have not." Edward T. Paulis III, *Preparing Your Board Before Litigation: A Primer on Defending Board Actions, Preserving Confidential Information, and Managing Risk*, http://www.accdocket.com/articles/resource.cfm?show=1429218.

45 Georgia Tech Report, supra, note 7.

46 Association of Corporate Counsel ("ACC") Foundation, *ACC Foundation: State Of Cybersecurity Report In-House Counsel Perspectives*, http://webcasts.acc.com/handouts/Key-Findings-from-the-ACC-Foundation-the-State-of-Cybersecurity-Report.pdf. Cybersecurity law for U.S. corporations doing business in the European Union remains un-unified: in October, 2015, the Court of Justice of the European Union issued its

> final ruling in Schrems v. Data Protection Commissioner (Case C-362/14), [and] invalidated the Safe Harbour arrangement, which governs data transfers between the

B. Key Measures

Boards should engage in a conscious, well-informed evaluation to consider best practices that will reduce the risk of data breaches, and to prepare mitigation measures to remediate specific and predictable kinds of breaches. They should focus on industry and corporation-specific measures that are tailored to their particular exposures; to identify and implement such measures shows on its face that Boards have not simply adopted random or generic protections, but made a good faith effort to conduct reasonable reviews of cybersecurity issues.

As Stone suggests, in reviewing a compliance program, courts will look favorably on corporations that, among other oversight measures and especially in advance of any breach

- Hire a specific cybersecurity officer who either serves on the Board or reports directly and regularly to it;
- Adequately fund and receive regular reports from a compliance department;
- Have a dedicated cybersecurity department, if the scale of the enterprise makes it appropriate;
- Have systems in place to detect breaches; and
- Install and continually update state of the art malware and virus detection software that end-users cannot tamper with or disable.[47]

Many reports advise Board members to appoint a cyber specialist to the Board, and to determine whether the entire Board or dedicated members should stay apprised of detailed cybersecurity issues:[48]

> EU and the US. . .. [The decision] allows each country's national regulators to suspend transfers if the company in the United States does not adequately protect user data. Consequently, US companies are no longer allowed to transfer private data from the EU to the US solely on the basis that they are members of the Safe Harbour scheme.

Marina Škrinjar Vidović: *Schrems v. Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities*, www.cyelp.com/index.php/cyelp/article/download/231/146.

[47] As Victoria C. Wong attests, "The fact that a corporation employs data security employees, has contracts with security vendors, and receives periodic reports about the status of the company's cybersecurity will easily defeat the claim that directors did not take adequate steps to inform themselves of risk." Wong, supra note 9 at 209.

[48] The Global Network of Director Institute, which comprises "16 member director institutes, including NACD in the U.S. and the Institute of Corporate Directors in Canada," issued "Guiding Principles for Cybersecurity Oversight" that recommends "that boards consider adding a member with some knowledge of information technology (including digitalization and cybersecurity). It is interesting to note that legislation was introduced in the U.S. that would require a public company to disclose to the Securities and Exchange Commission (SEC) whether any director has cybersecurity expertise or experience . . .." Krasnow, supra note 7.

> [T]he board may wish to consider moving responsibility for cyberrisk away from the audit committee to a dedicated group such as a risk management committee. Some companies have opted to retain a single board member with cybersecurity expertise in place of a risk management committee. However, this approach risks the board deferring too readily to a single person's expertise. . ..
>
> If the board establishes a committee dedicated to cybersecurity, it may wish to include as an adjunct member a senior cyberrisk officer, such as a chief information officer (CIO) or a chief information security officer (CISO). . ..
>
> [S]ome large organizations are hiring a CISO to have in place an executive whose principal task is information security. . .. Typically, in such an arrangement, the CISO reports to the CIO. However, this practice may also be changing in light of the heightened need for cybersecurity as some companies are choosing to select a CISO as a peer to the CIO.[49]

Board members should consult experts regarding any issues requiring technical expertise, and perhaps appoint a technical specialist to the Board, but they must remain responsible for oversight and executive-level planning; to do so, they need to have an adequate overview of the risks they must evaluate.

As the Georgia Tech Report admonishes, security often has been miscategorized as primarily an Information Technology ("IT") rather than management issue, a misprision that can lead Board members to misdelegate or fail to assert their authority. According to the NACD Cyber-Risk Oversight Handbook, "deferring responsibility to IT inhibits critical analysis and communication about security issues, and hampers the implementation of effective security strategies. . .. [In addition] directors should be mindful there might be an inherent bias on the part of management to downplay the true state of the risk environment. One study found that 60 percent of IT staff do not report cybersecurity risks until they are urgent—and more difficult to mitigate—and acknowledged that they try to filter out negative results."[50]

C. Independent Experts

If a Board reasonably relies on expert reports, it should be able to insulate itself from claims of bad faith and therefore from liability.[51]

---

[49] Black, supra note 8. The Georgia Tech Report determined that "Boards and senior management are improving in establishing key positions for security and risk officers, but lag in establishing privacy positions. The survey results indicate a steady rise in the number of CISOs (73%) at respondents' companies, up from only 30% in 2008. Only about one quarter (27%) of the respondents said they have a full-time CPO, up from 7% in 2008." See note 7, supra.

[50] NACD Cyber-Risk Oversight Handbook, https://www.nacdonline.org/files/FileDownloads/NACD%20Cyber-Risk%20Oversight%20Handbook%202017.pdf.

[51] See, e.g., In re Caremark International, 698 A.2d 959, 971 (Del. Ch. 1996).

The safest measure is for Boards to appoint outside experts to evaluate internal security; courts likely will treat such measures as virtually per se evidence of good faith and valid reliance that will serve to insulate members from culpability. Conversely, the Board should assert its independence against such experts when necessary to fulfill its leadership obligations. The Georgia Tech Report advises Boards to rely on, but maintain independence from, such outside experts, and clearly differentiate roles and responsibilities: "Ensure that privacy and security roles within the organization are separated and that responsibilities are appropriately assigned. The CIO, CISO/CSO, and CPO should report independently to senior management."[52]

D. Audit Committees

Audit committees also can provide Boards with effective advice, and offer evidence that they have engaged in good faith assessments of security risks or breaches. In the Wyndham case, the court looked favorably on the fact that the Board, after suffering three data breaches over a two-year period, met with its audit committee to address cyber-attacks multiple times over four years, and hired and followed the recommendations of technology firms.[53] The court interpreted the spacing and frequency of these audits as substantive evidence of the Board's good faith oversight.[54]

E. After a Breach

After a breach, companies should offer an array of services to any potentially affected customers, including fraud alerts, monitoring protection, and increased security. The Board should have a detailed and complete rapid response plan ready to implement in advance of any cyber-attack. It should train and fund a designated emergency response unit.

1. Disclosing Risks and Reporting Breaches

If a Board is aware of specific rather than general threats, based on past events or credible intelligence, then it should respond specifically and cannot claim ignorance if it fails to act: "The October 2011 SEC staff guidance addresses the obligations of public companies to disclose cybersecurity risks and cyberincidents, which companies should consider when assessing and disclosing cybersecurity risks. Failure to do so certainly increases the risk that the securities plaintiffs' bar may bring an action against the board and the public company."[55]

Boards should be aware that, "[a]s of 2016, 47 states (all U.S. states except Alabama, New Mexico and South Dakota), plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted breach notification laws. The Health Insurance Portability and Accountability Act
provides for breach notification. Other countries have breach notification laws. The U.S. Securities and Exchange Commission provides guidance regarding disclosure of cybersecurity risks and cyber-incidents."[56] In California, a recently amended code section requires businesses to disclose breaches of personal information to affected California residents, and, if the company was the source of the

---

[52] Georgia Tech Report, supra, note 7.
[53] Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 WL 5341880 at *2 (D.N.J. Oct. 20, 2014).
[54] Id. at *5-6.
[55] Black, supra note 8.
[56] Krasnow, supra note 7.

breach, to offer to provide free identity theft prevention and mitigation services to them for at least one year.[57]

Before or after breaches, Boards should be careful not to make any factual claims about security that could be disproven or allow plaintiffs to claim justified reliance on a falsehood. A corporation likely could face potential liability for its assertions regarding cyber-security only if it has scienter, that is knowledge, that it was making misrepresentations. Courts typically will evaluate a corporation's failure to disclose significant breaches in the context of the risk at stake, but seem more forgiving regarding omissions than provably false statements. Though the following discussion comes from an unpublished opinion in a case involving a class action, and does not pertain to personal Board liability, its analysis is worth considering:

> [N]one of the allegedly fraudulent statements were rendered misleading by Defendants failure to disclose the SQL attack. Heartland's 10–K only sought to describe how Heartland's security system functioned in a general way; the report did not imply that Heartland had never experienced any security problems. . .. Similarly, the statements on the November 4 conference call only dealt with Heartland's intention to pursue certain security measures . . .. These statements did not become misleading just because Heartland did not disclose past security incidents . . ..[58]

But the court also implied that had the corporation lied in response to questions about specific breaches, it then could be liable for material misrepresentations or omissions.[59] This reasoning generally comports with Caremark and Stone, which held in different contexts that Directors could be liable only if they "consciously failed to monitor or oversee [] operations . . . [and] knew that they were not discharging their fiduciary obligations."[60]

By contrast, the Central District of California faulted a health care company not for failing to secure information, but for *misrepresenting* its efforts to secure that information: "Cottage's failure to continuously implement the procedures and risk controls identified in its" application for insurance, "including, but not limited to, its failure to replace factory default settings [and] its failure to ensure that its information security systems were securely configured," led not only to legal liability, but prompted the company's insurance provider to seek to recover its settlement.[61] Here, the corporation made itself vulnerable to both plaintiffs and its insurance company because it failed to follow the security procedures it had publicly claimed to have adopted.

Personal liability aside, Board members therefore should be careful not to attest to or promise anything that is inaccurate, especially with regard to forms of certification; they need to distinguish

---

57 Cal. Civ. Code § 1798.82 (West).

58 In re Heartland Payment Sys., Inc. Sec. Litig., No. CIV. 09-1043, 2009 WL 4798148, at *6 (D.N.J. Dec. 7, 2009).

59 See id. at *6.

60 Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006).

61 Columbia Cas. Co. v. Cottage Health Sys. 2015 WL 3751196 (C.D. Cal. 2015). The insurer claimed Cottage Health breached a clause in its policy that precluded coverage related to any "failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance. . .." Roberta Anderson, *The Devil Is in the Details of Cyber*, June 3, 2015, http://insurancethoughtleadership.com/tag/columbia-casualty-company-vs-cottage-health-system/.

security-puffery from objective assertions that could induce reliance and incur liability for intentional misrepresentation.[62]

F. Other Specific Recommendations:

Experts and attorneys generally agree that a

> company's failure to do the following will likely be found unreasonable: Remedy "known security vulnerabilities" such as allowing insecure server/network connections; Employ commonly used methods to require user IDs and passwords that are difficult for hackers to guess; Adequately inventory computers to manage network devices; Employ reasonable measures to detect and prevent unauthorized access or to conduct security investigations; Follow proper incident response procedures, including monitoring computer

---

[62] False or misleading claims about a company's compliance with security standards also could raise additional regulatory issues:

> In May 2016, the FTC settled its charges against Vipvape [in In re Very Incognito Technologies, Inc., d.b.a. Vipvape] for misrepresenting that it was a participant in [and certified by] the Cross-Border Privacy Rules (CBPR) program between the Asia-Pacific Economic Cooperation (APEC) countries and the E.U. . . . In March 2016, "the CFPB announced its first consent decree [in Dwolla] . . .. The CFPB alleged that the respondent payment technology company had "(mis)represented to consumers that its network and transactions were 'safe' and 'secure,'" and that it was PCI [payment card industry]-compliant.

Mark Mao et al., Data Privacy: The Current Legal Landscape Quarterly Update, June 30, 2016, https://www.troutmansanders.com/files/Uploads/Documents/TS_Article_DataPrivacy_TheCurrentLegalLandscape_June_2016.pdf; see also https://www.ftc.gov/enforcement/cases-proceedings/162-3034/very-incognito-technologies-matter; In the Matter of: Dwolla, Inc., CFPB File No. 2016-CFPB-0007, Consent Order dated March 2, 2016, available at http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.

In July 2016, the FTC reversed the decision of an administrative law judge who had dismissed charges against LabMD, for its failure to protect medical and other private information of consumers, and found that the company's

> data security practices were unreasonable and constitute an unfair act or practice that violated Section 5 of the Federal Trade Commission Act. . ..
>
> LabMD's security practices were unreasonable, lacking even basic precautions to protect the sensitive consumer information maintained on its computer system. Among other things, it failed to use an intrusion detection system or file integrity monitoring; neglected to monitor traffic coming across its firewalls; provided essentially no data security training to its employees; and never deleted any of [its] consumer data . . ..

https://www.ftc.gov/news-events/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

network[s] for malware used in a previous intrusion; and, Adequately restrict third party vendor access.[63]

Because they could (at least theoretically) be held to a standard of "reasonableness" under Caremark,[64] Boards should implement the following best practices:

- Research, identify and adapt industry-specific best practices and address any potential gaps in your system and coverage. Have reputable third parties regularly check your systems for vulnerabilities.

- Simulate realistic attacks and responses in real time: stage cyber-drills that alert your entire enterprise to the threats your employees face, the measures they should be adopting, and the protocols with which they should be versed.

- Train employees to prevent the downloading of any malware; avoid the ever-expanding array of phishing scams; identify and replace software with known vulnerabilities; and when and how to communicate with members of IT departments.

- Limit access to your critical data to "a need-to-access" basis; narrow the points of access to your data in every context, and especially in terms of outside third parties; terminal and remote access; administrative privileges; and ability to share data, especially in unencrypted form.

- Implement multi-tiered security for vital information by requiring users to log in from recognized or approved devices, or answer unique additional security questions. This process is especially advisable for any email accounts employees use to do business, since they could serve as "ur-sources" for hackers—i.e., one-stop portals to obtain records, passwords, and information that will give them access to an array of databases.

- Require automatic log-outs after a specified time for all computer terminals and mobile devices that access corporate information.

- Employ a system that can audit computer access and log-ins and effectively monitor those records.

- Archive (off-line) or delete any data that your company does not need to access on a current or regular basis.

- Make sure cyber-protocols are updated or reviewed consistently so that former employees no longer have access to or retain confidential data, and ensure that all discarded computers and devices have been fully erased and retain no data that could be retrieved.

---

[63] Alexa King et al., *Cybersecurity Governance Duties*, http://www.fbm.com/files/Uploads/Documents/October%202016%20-%20ACC-Docket%20-%20Alameda.pdf.

[64] See In re Caremark International, 698 A.2d 959, 971-72 (Del. Ch. 1996).

- Encrypt all sensitive data, especially when it will be routinely transmitted electronically, and require especially that all mobile devices use encryption.[65]

- If merging with or acquiring another firm, ensure your due diligence includes a separate cybersecurity analysis.

- Conduct at least a semi-annual review not only of cybersecurity measures, breaches, and compliance issues, but of new regulations. Such documented reviews—which should include regular reports and detailed minutes of all meetings that address cyber-threats—will both help the Board stay informed and offer proof of ongoing diligence.

Director liability aside, the typical costs of a data-breach to a corporation are chastening, and should encourage Boards to investigate the feasibility of obtaining comprehensive cybersecurity insurance. The data breach Target suffered in 2013 wound up costing around

> $252 million in mitigation, response, and defense expenses, and [Target] expected to recover only some $100 million from its insurers. . .. The SEC's recent OCIE information requests expressly ask whether registered entities "maintain insurance that specifically covers losses and expenses attributable to cybersecurity incidents." So, too, the DHS has opined that a "robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection."[66]

Address your known unknowns, which in the abstract could include deep-structure malware you can't detect or Russian hackers, but in concrete terms should include the vulnerabilities of partners, ISPs, vendors and independent contractors. No matter how comprehensive your internal security is, if you have no oversight of these third-parties, you are leaving gaping holes in your security; your actions might be equivalent to installing state-of-the-art alarms throughout your house, but giving

---

[65] For example, in the case filed against Target for breach of 110 million of its customers' financial and personal data—which caused such a backlash the corporation's CEO had to resign—plaintiffs sought "'appropriate injunctive relief' including an order that Target encrypt all customer data from the point of sale through Target's payment system, comply with federal and Minnesota law regarding data security and the retention of data, adopt EMV chip technology for Target-issued credit and debit cards, and requiring Target to provide extended credit-monitoring services to Plaintiffs and class members." In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1161 (D. Minn. 2014); Danielle Douglas, *Target CEO Resigns After Massive Data Breach,* THE WASHINGTON POST, May 5, 2014, available at https://www.washingtonpost.com/business/economy/target-ceo-resigns-after-massive-data-breach/2014/05/05/ef6cbee2-d457-11e3-8a78-8fe50322a72c_story.html?utm_term=.b1004139a886.

Shareholders filed two derivative lawsuits against Target and its directors and officers, alleging that they were aware of "the importance of protecting customer and cardholder data and failed to take appropriate steps to prevent the breach. The claims included breach of fiduciary duty, waste of assets, gross mismanagement, and abuse of control." Georgia Tech Report, supra, note 7. The Target suit, along with similar derivative suits against Home Depot and Wyndham, was dismissed.

[66] Davis et al., supra note 4 at 646-47 (citations omitted).

the security codes to an unvetted contingent of revolving employees at your post office, heating service, grocery delivery agency, and singing-telegram company.

IV. Other Resources:

In addition to the resources already mentioned, Boards should consult the plethora of available Commission, institute, and think-tank policy guides and recommendations: for example,

> Further direction for boards dealing with cybersecurity governance issues can be found from organizations such as the Committee of Sponsoring Organizations of the Treadway Commission, or COSO, and the National Association of Corporate Directors, or NACD. . ..
> In January 2015, COSO published "COSO in the Cyber Age," a long overdue publication that provides guidance on cybersecurity controls in the context of corporate governance. . ..
> Further support for considering information security an essential part of corporate governance can be found in the Business Roundtable's 2005 publication, "The Principles of Corporate Governance."[67]

In terms of critical resources, S.E.C. Commissioner Aguilar has asserted that the NIST *Framework for Improving Critical Infrastructure Cybersecurity* "should serve as a reference point for boardrooms."[68] NIST avers that its "Framework may become the standard for federal cybersecurity regulations, and there is a growing consensus that it is fast becoming the de facto standard for private sector cybersecurity."[69]

To address international compliance, Boards should consult the publications of U.S. and foreign enforcement agencies: "U.S. enforcement agencies jointly published the *Foreign Corrupt Practices Act Enforcement Manual* in 2012. . .. the enforcement principles articulated in the FCPA Manual . . . are useful predictors of how regulators may generally approach future data security investigations. The Manual identifies core concepts for such a program."[70]

V. Cyber-CSR:

Much as Board members once overlooked the security dimension of governance, they might still overlook the Corporate Social Responsibility ("CSR") dimension of cybersecurity. CSR stands for the proposition that private corporations effectively owe a duty of care to improve, or at least not impair, the common good, which in this context entails protecting consumer privacy. While a failure to consider CSR, absent a specific legal mandate, will impose no liability on a Board, its consideration can enhance reputation, profits, and the common good.

---

67 Romaine Marshall, *Cybersecurity: What Are Corporate Directors' Duties?*, 34 WESTLAW JOURNAL COMPUTER AND INTERNET 1 (2017); for COSO, see https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf.
68 Davis et al., supra note 4 at 630; for the *NIST Framework*, see note 16 supra.
69 *The NIST Cybersecurity Framework*, Practical Law Practice Note 5-599-6825.
70 Davis et al., supra note 4 at 628–29.

As required by President Obama's Executive Order 13646, "Improving Critical Infrastructure Cybersecurity," Appendix B of NIST's Framework, the Privacy Methodology, "provides guidance on privacy and civil liberties considerations for the selected Categories and Subcategories," of cybersecurity practices, in intimating the connection between best practices in terms of data protection and best practices in terms of CSR.[71] According to Scott J. Shackelford et al., Boards should consider corporations to function not just as legal entities, but socially-situated institutional actors:

> This view impacts managers by calling for the exercise of "a multifiduciary duty to stakeholders . . . [and] a sense of distributive justice." . . . [S]uch an interpretation of the role of business in society essentially considers the firm as "a parallel communitarian construct of the state," meaning that the innovative elements of an independent private sector may be underappreciated, including the ability of firms to contribute to enhancing cybersecurity.[72]

It makes sense, as Shackelford et al. have proposed, that Boards should address "cybersecurity as a matter of CSR to safeguard their customers and the public, such as by securing critical national infrastructure. It is in corporations' own long-term self-interest (as well as that of national security) to take such a wider view of private-sector risk management practices so as to encompass less traditional factors akin to what companies have done with respect to sustainability."[73]

If, as Shackelford et al. contend, the internet is a kind ecosystem we all share, but also a site of warfare, we might employ the same models of sustainability and the same principles of CSR to cybersecurity as we would to environmental protection and international cooperation.[74]

Barnali Choudhury proposes that regulatory agencies could "provide informational guidance to corporations on completing social disclosure obligations. The SEC has previously employed this approach by providing interpretive guidance to corporations in completing their disclosure obligations relating to climate change and cybersecurity issues."[75] An array of agencies could expand that imperative to cover, in systematic and uniform contexts, disclosure of security measures, breaches, and compliance. In this area, regulatory agencies could spur a significant transformation of Cyber-CSR practices by offering both guidelines and incentives.

---

71 https://www.nist.gov/sites/default/files/documents/itl/preliminary-cybersecurity-framework.pdf., p. 9.
72 Shackelford et al., *How Businesses Can Promote Cyber Peace*, 36 U. Pa. J. Int'l L. 353, 382–83 (2014) (citations omitted).
73 Shackelford et al., *Sustainable Cybersecurity*, 2016 U. ILL. L. REV. at 1997.
74 Id. at 2001, 2003.
75 Barnali Choudhury, *Social Disclosure*, 13 BERKELEY BUS. L.J. 183, 215 (2016) (citation omitted).