CYBERSECURITY: GETTING BEYOND TECHNICAL COMPLIANCE GAPS

*Rebecca Weinstein**

INTRODUCTION

[Cyberspace] is a matter . . . of America's economic competitiveness . . . . [Cybersecurity] is one of the most serious economic and

* J.D. 2016, New York University School of Law; Senior Quorum Editor, Journal of Legislation & Public Policy (2015–16). Many thanks to Phoebe King for her comments and to the senior staff of the NYU Journal of Legislation & Public Policy for their excellent editorial work.

> *national security challenges we face as a nation . . . . [The] status quo [in place to protect cyberspace] is no longer acceptable—not when there's so much at stake. We can and we must do better.*
>
> —President Barack Obama, May 29, 2009[1]

America's economic prosperity in the twenty-first century depends on advancing cybersecurity protocols, procedures, and practices to protect against cyber-breaches.[2] In fact, the intelligence community now lists cyber-breaches as a greater threat to U.S. economic well-being than terrorism.[3] Without adequate cyber-safeguards, thieves can steal millions of dollars in minutes, destroy infrastructure through the smallest of security oversights, and compromise countless pieces of sensitive information from across the globe.[4] It is, therefore, not surprising that corporate efforts to combat cyber-crime stem from more than just patriotism—businesses and government entities alike are harmed by cyber-criminals. As digital commerce expands and electronic storage of consumer information increases,[5] the fortification of corporate cybersecurity protocols will continue to rise to the forefront of private, public, and regulatory priorities.[6] Yet, despite the complex-

1. President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

2. *See id.* This paper defines "cybersecurity" as consistent with the definition set forth in 44 U.S.C. § 3542(b)(3) (2012): "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction." A failure of such information security protection is referred to herein as a "cyber-breach."

3. Martha Mendoza, *AP Impact: U.S. Agencies Struggle vs. Cyberattacks*, U.S. NEWS (Nov. 10, 2014, 4:10 PM), http://www.usnews.com/news/articles/2014/11/10/ap-impact-us-agencies-struggle-vs-cyberattacks.

4. *See* Nadia Damouni, *Exclusive: U.S. Companies Seek Cyber Experts for Top Jobs, Board Seats*, REUTERS (May 30, 2014, 1:15 AM), http://www.reuters.com/article/idUSKBN0EA0BX20140530 ("[I]n many cases, a business's survival relies on the security of the technology."); *see also* Marc Summe, *Have Online Payments Become Safer Than Offline?*, WIRED, http://www.wired.com/insights/2014/12/have-online-payments-become-safer-than-offline/ (last visited Oct. 28, 2016) (discussing the corporate costs of recent high-profile data breaches).

5. *See, e.g.*, David Gray et al., *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 747–48 (2013) ("Consumers have become more dependent on networked devices and . . . public spaces [that] are increasingly tracked and traced, [thereby] expos[ing] more of [them]selves to governmental actors and to third parties."); Summe, *supra* note 4 ("Ecommerce is growing fast at 9.5% a year, and is expected to outpace sales growth at brick-and-mortar stores over the next 5 years.").

6. *See, e.g.*, Alina Selyukh, *U.S. Offers Companies Broad Standards to Improve Cybersecurity*, REUTERS (Feb. 12, 2014, 3:20 PM), http://www.reuters.com/article/us-usa-cybersecurity-standards-idUSBREA1B0AL20140212 ("[Cybersecurity gaps have] recently became a household topic . . ..").

ity and seriousness of cyber-threats, the average corporate coffer of consumer information is currently protected from poor corporate cyber-management by a disjointed mixture of privately enforced standards,[7] post-data breach regulatory actions,[8] and nonbinding federal guidelines.[9] Overall, existing federal legislation lacks a clear definition of reasonable, pre-breach corporate security mechanisms and, within this void, corporate liability for data breaches remains uncertain.[10]

Identifying this growing problem is relatively easy—finding an effective way to minimize corporate cybersecurity risks is more difficult. To help incentivize corporate adoption of responsible cyber-practices, forty-seven states and some U.S. territories independently regulate corporate post-breach procedures and consumer notification performance.[11] Nevertheless, slapping corporations on the wrist after a

7. *See* Obama, *supra* note 1 ("The vast majority of our critical information infrastructure in the United States is owned and operated by the private sector. [The federal government must] collaborate with industry to find technology solutions that ensure our security and promote prosperity.").

8. *See, e.g.*, *Enforcing Privacy Promises*, FED. TRADE COMM'N, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Oct. 28, 2016). *See generally* Kathryn F. Russo, FTC v. Wyndham Worldwide Corporation, et al. *and the FTC's Authority to Regulate Companies' Data Security Practices*, 23 COMPETITION: J. OF THE ANTITRUST & UNFAIR COMPETITION L. SEC. OF THE ST. B. OF CAL. 164 (2014) (noting that a federal district court rejected the argument that the FTC must have clear cyber-breach rules and regulations to bring a cyber-breach claim and, instead, found sufficient authority for a cyber-breach case in the flexible standards of Section 5 of the FTC Act).

9. *See, e.g.*, NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 7 (2014), http://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf; *see also* Kristin Shields, *Cybersecurity: Recognizing the Risk and Protecting Against Attacks*, 19 N.C. BANKING INST. 345, 358 (2015) (noting that over the last five years, Congress has failed to turn nearly 100 proposed cybersecurity standards into law).

10. Patricia Bailin & Arielle Brown, *Preparing for a Data Breach: Data Security Regulations and Best Practices*, 23 WESTLAW J. HEALTH L. 2 (2015) ("[T]he majority of industries in the United States fall under the jurisdiction of the Federal Trade Commission, which . . . enforce[s] reasonable data security practices. . . . Though the FTC expects companies to implement 'reasonable' data security practices, it has never officially defined the term."). Industry-specific information security standards required by federal legislation, such as those outlined in the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA), do not govern the practices of most corporate entities and, as such, this paper does not analyze their role in the broader push for corporate risk management procedures. *See, e.g.*, Bret Cohen, *The Evolving Legal Framework Regulating Commercial Data Security Standards*, 47 MD. B. J. 30, 33–34 (2014) (noting that "[a] handful of federal laws regulate commercial data security in specific industry sectors," such as healthcare and finance).

11. *See Summary of U.S. State Data Breach Notification Statutes*, DAVIS WRIGHT TREMAINE LLP, http://www.dwt.com/statedatabreachstatutes/ (last visited Oct. 22, 2016).

cyber-breach occurs is a proverbial stick without its carrot: Such post-breach punishment creates minimal incentives for companies to adopt strong, pre-breach cyber-practices.[12] Moreover, even among the U.S. companies that employ high-tech cybersecurity teams, many companies and their upper management professionals lack an effective company-wide cybersecurity strategy.[13] Even though companies have rapidly increased awareness of risk-based cybersecurity frameworks, corporate self-assessment questionnaires demonstrate that the implementation of such programs still leave much room for improvement.[14]

To improve pre-breach adoption of effective cybersecurity practices, private and public liability proponents emphasize two different models: technical cybersecurity remedies and holistic risk management frameworks. Technical standards stress a checklist of computerized-solutions including electronic specifications on types of firewalls, encryptions, passwords, and penetration testing. However, rapidly evolving tactics of cyber-criminals often outpace the technology that powers such fixes.[15] A holistic risk management standard, on the other

12. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 928 (2007) (discussing how economic forces undermine regulatory attempts to incentivize strong pre-breach adaption of cybersecurity practices).

13. TANIUM & NASDAQ, THE ACCOUNTABILITY GAP: CYBERSECURITY & BUILDING A CULTURE OF RESPONSIBILITY (2016), http://media.scmagazine.com/documents/223/the_accountability_gap_report__55615.pdf (reporting data on the "dissonance between corporate leaders' current awareness and readiness for cybersecurity challenges, and where they need to be"); *see* Sommi Sengupta, *Executives May Be Too Confident on Cybersecurity, Survey Finds*, N.Y. TIMES: BITS (Sept. 15, 2011, 8:00 AM), http://bits.blogs.nytimes.com/2011/09/15/executives-are-bullish-on-cybersecurity-spending-survey-finds/ (reporting that only 16% of executives interviewed believed their company was cyber-ready).

14. *See, e.g.*, PONEMON INST., 2015 GLOBAL STUDY ON IT SECURITY SPENDING & INVESTMENTS 3 (May 2015), https://dsimg.ubm-us.net/envelope/361113/383513/Ponemon%20Report-%202015%20Global%20Study%20on%20IT%20Security%20Spending%20&%20Investments.pdf (demonstrating stark differences between upper-management and IT beliefs about cybersecurity objectives and needs); PWC, GLOBAL STATE OF INFORMATION SECURITY SURVEY 2016: TURNAROUND AND TRANSFORMATION IN CYBERSECURITY: KEY FINDINGS FROM THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 4, 18 (2016), https://www.pwc.fi/fi/julkaisut/tiedostot/global-state-of-information-security-survey-2016.pdf [hereinafter PWC, GSIS 2016 SURVEY] (showing that while 91% of surveyed companies claimed to have implemented a risk-based framework, less than 45% identified a clear pathway of communication between the Chief Information Security Officer and executive corporate leaders).

15. *See* VERIZON, 2016 DATA BREACH INVESTIGATIONS REPORT 74–75 (2016), www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf (follow "Download the 2016 DBIR" hyperlink) ("After you mitigate the first few [technical security flaws], the effectiveness simply falls off. . . . [Thus,] [d]efining the roads most traveled by your likely adversary as well as the ones that lead to the greatest impact to you is key.").

hand, encourages executive-level cyber-awareness through corporate self-evaluation of cyber-risks, threats, and internal controls.[16] Emphasizing a strong corporate cyber-risk management program shifts corporate readiness away from a rigid checklist culture and helps to bolster the first line of reasonable business practices: informed business leaders.[17] If corporations need to be equally as agile as the criminals they are protecting themselves against, then holistic frameworks should become a more prominent consideration when private and public adjudicators assess corporate liability for cyber-breaches.

This paper explores the risk management standards that have been erected in the shadow of an unruly cybersecurity liability landscape. Part I of this paper provides a brief overview of chief cybersecurity issues and corporate cybersecurity obligations. Part II of this paper explores the background benefits and limitations of tech-focused security checklists, such as the Payment Card Industry's Data Security Standard, as a basis for corporate compliance and liability. Part III explains the broader holistic approach of guidelines, such as the National Institute of Standards and Technology Framework, and discusses why flexible standards for risk management are critical for developing a national cybersecurity infrastructure. Part IV proposes that emphasizing holistic cyber-crime compliance structures over technical cyber-threat stopgaps should be a greater component in determining corporate cyber-breach liability.

I.
OVERVIEW

> *Too many people still see information security as a principally technical problem and believe that simply buying the right software will cause the problem to go away. Information security involves people, processes, and technologies—getting all three in the right measure is the real art of a successful security program.*
>
> —PWC, Global State of Information Security Survey 2015[18]

16. Kristin N. Johnson, *Managing Cyber Risks*, 56 GA. L. REV. 547, 561–62 (2016) ("Risk management thus involves organizational processes that generally include risk identifying, measuring, and mitigating procedures, [and is used to identify and combat] bad outcomes that could occur in an uncertain future.") (internal citations and quotations omitted).

17. *See* TANIUM & NASDAQ, *supra* note 13.

18. PWC, GLOBAL STATE OF INFORMATION SECURITY SURVEY 2015: MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD 31 (Sept. 30, 2014), http://www.pwccn.com/home/eng/rcs_info_security_2015.html [hereinafter PWC, GSIS 2015 SURVEY].

A. The Current Corporate Perspective

The last few years have seen reports of corporate cyber-breaches blasted through headlines, listing costs in the multi-millions at a frequency as "commonplace as the weather forecast."[19] Unsurprisingly, cybersecurity concerns among CEOs and Boards of Directors are at an all-time high.[20] Nevertheless, most global information security budgets stalled between 2010 and 2015,[21] a majority of information technology (IT) professionals believe their allocated cybersecurity budgets are inadequate,[22] and while more companies are claiming to implement preventative frameworks, only forty-three percent of security leaders surveyed in a recent PWC report "approach[ ] information security as an enterprise risk-management issue."[23] Moreover, there is a stark difference in the perceived corporate adoption of risk management frameworks and the as-implemented risk management programs.[24] For instance, sixty-four percent of IT professionals do not feel that Boards of Directors are "made fully aware of security priorities and required investments."[25] Moreover, studies show that the

19. *Id.* at 5 ("Security incidents outpace GDP and mobile phone growth."); *see, e.g.*, Steve Rosenbush, *The Morning Download: Sony Breach Could Cost $100 Million*, WALL ST. J.: CIO J. (Dec. 10, 2014, 7:39 AM), http://blogs.wsj.com/cio/2014/12/10/the-morning-download-sony-breach-could-cost-100-million/.

20. Stephen Gandel, *CEOs Around the World Are Running Scared*, FORTUNE (Jan. 19, 2016, 4:09 PM), http://fortune.com/2016/01/19/pwc-ceo-survey/ (describing cybersecurity as the number one business concern of 2015); *see also* PWC, U.S. CYBERCRIME: RISING RISKS, REDUCED READINESS: KEY FINDINGS FROM THE 2014 U.S. STATE OF CYBERCRIME SURVEY 7 (2014), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-2014-us-state-of-cybercrime.pdf [hereinafter PWC, RISING RISKS] (finding that 59% of respondents to the US State of Cybercrime Survey indicated that "they were more concerned about cybersecurity threats this year than in the past").

21. PWC, GSIS 2015 SURVEY, *supra* note 18, at 19–20.

22. PONEMON INST., *supra* note 14.

23. PWC, GSIS 2016 SURVEY, *supra* note 14, at 18; *see also* Selyukh, *supra* note 6 ("Many experts have expressed alarm about the lack of awareness or reluctance among some companies' leaders to spend more money on cyber defenses."); *Survey: 82% of Boards are Concerned About Cybersecurity, Yet Just 1 in 7 Security Chiefs Reports Directly to CEO*, ISACA (Feb. 29, 2016), http://www.isaca.org/About-ISACA/Press-room/News-Releases/2016/Pages/Survey-82-percent-of-Boards-Are-Concerned-about-Cybersecurity.aspx ("The majority of CISOs still report to CIOs, which shows cybersecurity is viewed as a technical rather than business issue.").

24. *E.g.*, Stuart R. Levine, *Cybersecurity Threats Are Real: You and Your Organization Could Be in Danger*, FORBES (Apr. 25, 2016), http://www.forbes.com/sites/forbesinsights/2016/04/25/cybersecurity-threats-are-real-you-and-your-organization-are-in-danger/#68dee9af70ee ("91% of high vulnerable board members said they can't read a cybersecurity report and are not prepared to handle a major attack. The worst part . . . is that 40% said they feel no responsibility for the consequences of being hacked.").

25. PONEMON INST., *supra* note 14, at 2.

communication between IT and high-level management on control of security practices and budgeting for security resources is far from streamlined or cohesive.[26]

Understanding cyber-breach costs is essential for incentivizing corporate risk management systems but exceedingly difficult to accomplish. Costs from even a single breach vary wildly and, by the time a breach is discovered, several breach incidents have often occurred.[27] The variation of such costs also stem from post-breach reputational damage, flawed cyber-standards of third-party partners, and theft of information that is not easily assigned a monetary value.[28] Even after removing sizable legal fees and technical repairs, a "typical" data breach claim for these additional factors can cost anywhere from $25,000 to $400,000, with a median claim payout of $242,500.[29] This valuation problem exacerbates the difficulty of incentivizing companies to invest in pre-breach cybersecurity efforts and obfuscates the benefits of an enterprise-wise cyber-management risk framework that goes beyond specific technical deficiencies.

Nevertheless, some companies demonstrate mindfulness about cybersecurity and have increased hiring of cybersecurity expert positions.[30] Furthermore, high-profile data breaches have fostered a new expectation that "Chief Information Security Officers (CISO) understand not just technology but also a company's business and risk management" structure.[31] These nascent efforts reframe the cybersecurity conundrum from a pure IT issue to a risk management issue. As one

26. *Id.*

27. *See, e.g.*, Robert Westervelt, *Massive Target Breach Puts Spotlight on PCI Complexity*, CRN (Dec. 19, 2013), http://www.crn.com/news/security/240164888/massive-target-breach-puts-spotlight-on-pci-complexity.htm (describing the two-week period when cyber thieves compromised Target's data information systems).

28. *See, e.g.*, Robert Hackett, *How Much Do Data Breaches Cost Big Companies? Shockingly Little*, FORTUNE (Mar. 27, 2015, 5:28 AM), http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/ ("Sony's November 2014 hacking led to the disclosure of . . . personal data—including Social Security numbers—of 47,000 celebrities and employees . . . . Still, Sony estimates its breach's financial impact has been just $15 million to date . . . . That's barely a blip on the radar.").

29. Eric G. Orlinsky et al., *Cybersecurity: A Legal Perspective*, 47 MD. B.J. 32, 34 (Nov./Dec. 2014).

30. *See, e.g.*, Damouni, *supra* note 4 (noting that "the largest U.S. bank will have about 1,000 people focused on cybersecurity, compared with 600 people two years ago" and that Target "is searching for a CISO, a newly created role" in the wake of a massive 2013 data breach).

31. *Id.*; *see also* Paul Ferrillo, *Changing the Cyber Security Playing Field*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. (Jan. 20, 2015), http://corpgov.law.harvard.edu/2015/01/20/changing-the-cyber-security-playing-field-in-2015/ ("Though every organization has to make its own determination as to whether such a position is

top executive stated: "managing risk . . . [t]hat is what executive teams do."[32] As sectors outside of the traditional "tech" industry, such as retailers[33] and service organizations,[34] increasingly process digital consumer information through web-based operations, a wider array of corporations must follow suit in adopting risk management strategies for combatting cyber-theft and protecting consumer information.

B. Cyber-Litigation and the Liability Landscape

Corporate liability for a data breach rests on a wide combination of legal factors. While some sector-specific federal data regulations exist,[35] there is no federal statute creating a general corporate duty or standard for the protection of personal data.[36] Instead, over fifty federal statutes, which are not cyber-specific, are used to hold companies accountable for their ineffective cybersecurity programs.[37] Since 2002, for example, the Federal Trade Commission (FTC) has brought more than fifty cases under the FTC Act's Section 5 to target corporations for "unfair" and "deceptive" safekeeping of consumer information.[38] Guidance from the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (SEC's OCIE) also requests, as part of compliance examination, that firms publicly disclose perceived cyber-risks and corporate controls in place to handle such risks.[39] Additionally, most states have enacted broad laws

---

needed within its company, at the very least *someone* needs to be 100% responsible for network security issues. That role is often filled by the CISO.").

32. Joe Mont, *New PCI Standard Pushes Toward Risk Management*, COMPLIANCE WK. (March 2015), http://mydigimag.rrd.com/article/New+PCI+Standard+Pushes+Toward+Risk+Management/1942293/0/article.html; framing cybersecurity as "just a different type of risk" makes it more manageable for corporate leaders. *Id.*

33. *See, e.g.*, *In re Target Corp. Customer Data Security Breach Litig.*, 64 F. Supp. 3d 1304 (D. Minn. Dec. 2, 2014); *see also* Westervelt, *supra* note 27.

34. *See, e.g.*, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014).

35. *See* Cohen, *supra* note 10, at 33–34 (2014) ("A handful of federal laws regulate commercial data security in specific industry sectors, but the most comprehensive ones are those embodied in the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA). HIPAA directly regulates the collection and use of health information [and] GLBA requires covered 'financial institutions' . . . to adopt a comprehensive data security program[s].").

36. *See* Orlinsky, *supra* note 29, at 36; *see also* Shields, *supra* note 9, at 358.

37. *See* Orlinsky, *supra* note 29, at 36.

38. *2015 Privacy and Data Security Update*, FED. TRADE COMM'N (2015), https://www.ftc.gov/reports/privacy-data-security-update-2015; *see also* Abraham Shaw, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 538 (Summer 2010).

39. *See* Brad Lunn, *Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations*, 4 J.L. & CYBER WARFARE 109, 114–15 (2014) (citing *Regulation Systems Compliance and Integrity*, SEC. AND EXCH. COMM'N, Mar. 7,

that require breached companies to investigate and reveal cyber-breaches to impacted consumers after a breach is discovered.[40] Nevertheless, the majority of these state laws, the FTC Act, and SEC guidance do not directly set metrics that companies must use to safeguard digital information.[41] Thus, companies and adjudicators primarily turn to non-federalized sources and existing case law to determine their potential responsibility for cyber-breaches.[42]

Countless shareholder derivative suits, for instance, argue that the fiduciary duties of a corporation's Board of Directors include oversight of cyber-risk management programs.[43] These cases assert that Boards have a duty to act in protecting sensitive information and cyber-infrastructure and that when a Board fails to act in implementing necessary cyber-safeguards, it exhibits "conscious disregard" for its fiduciary duties.[44] This does not mean that Boards and individual

---

2013, 17 C.F.R. Parts 242 and 249, Release No. 34-69077, https://www.sec.gov/rules/proposed/2013/34-69077.pdf (last visited Oct. 22, 2016)). *See generally* SEC OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATION, OCIE CYBERSECURITY INITIATIVE (2014), www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert—Appendix—-4.15.14.pdf.

40. *See Summary of U.S. State Data Breach Notification Statutes*, *supra* note 11. Breaches arising under state claims, in particular, have been shown to expose companies and individual board members to suits. Heather Egan Sussman, *Tracking State Data Protection Enforcement in 2014*, LAW360 (Dec. 19, 2014, 5:16 PM), http://www.law360.com/articles/606359/tracking-state-data-protection-enforcement-in-2014.

41. *See* John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW. 199, 206 (2013) ("Although several states have data security laws that require businesses to adopt reasonable security measures to protect personal information, of which the most notable and comprehensive may be Massachusetts Regulation 17, those statutes do not define what constitutes reasonable data security."); SEC OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATION, *supra* note 39 (merely outlining as guidance what the SEC OCIE *may* use in examining cybersecurity issues); Patricia Balin, *Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, IAPP (2014), https://iapp.org/resources/article/study-what-ftc-enforcement-actions-teach-us-about-the-features-of-reasonable-privacy-and-data-security-practices-2/ (suggesting "possible guidelines for complying with FTC privacy and data security standards based on what the FTC has determined is *in*adequate") (emphasis in original).

42. *See* Douglas H. Meal, *Private Data Security Breach Litigation in the United States*, *in* PRIVACY AND SURVEILLANCE LEGAL ISSUES: LEADING LAWYERS ON NAVIGATING CHANGES IN SECURITY PROGRAM REQUIREMENTS AND HELPING CLIENTS PREVENT BREACHES (2014), 2014 WL 10442, at *7 (Jan. 2014) ("In addition to common law claims, data breach plaintiffs frequently assert causes of action under state consumer protection statutes.").

43. *See* Vincent R. Johnson, *Data Security and Tort Liability*, 11 J. INTERNET L. 22, 25 (2008) ("[I]t is reasonable to argue that regardless of whether general tort principles would impose a duty, the fiduciary is obliged to protect computerized information relating to the data subject from unauthorized access by third parties.").

44. *See, e.g.*, *Stone ex rel. AmSouth Bancorporation v. Ritter,* 911 A.2d 362 (Del. 2006) ("The fiduciary duty of loyalty is not limited to cases involving a financial or

corporate directors are "expected to make perfect decisions" or be "cyber-experts."[45] In fact, Directors are often shielded from liability when flaws of complex business decisions become apparent only after harm has materialized.[46] In the modern era of the ever-present cyber-threat, however, the courts may hold Boards accountable for ineffective corporate cyber-practices.[47] At present, though, the primary threat of such derivatives suits is not legal liability but, instead, the negative press and costs from defending such suits.[48]

Breach of contract claims are also integral to the cybersecurity debate and hold potential for increasing corporate cyber-accountability.[49] For instance, any cyber-breach that impacts credit card information automatically raises legal questions of liability over the specific security requirements set by merchant contracts with credit card companies.[50] Such incidents expose merchants to breach of contract

---

other cognizable fiduciary conflict of interest. It also encompasses cases where the fiduciary fails to act in good faith . . . . [If] directors utterly failed to implement any reporting or information system or controls; or . . . having implemented such a system . . . , consciously failed to monitor or oversee [the operation, shareholders can prevail.]"); *see also In re Target Corp., supra note 33*; Stephen M. Bainbridge, *Caremark and Enterprise Risk Management*, 34 J. OF CORP. L. 967, 977 (2009) ("In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations.").

45. Lunn, *supra* note 39, at 134 ("[D]irectors are not expected to be cyber-risk or technology experts, but they are fully expected to appropriately oversee important corporate affairs on an informed basis, and in this modern era, it certainly includes cybersecurity for almost all organizations."); Bainbridge, *supra* note 44, at 985 (noting that liability can be found if a board failed "to assure the existence of reasonable information and reporting systems" or if "red flags were raised by such systems or otherwise that the directors ignored those red flags"); see Roland L. Trope, *"There's No App For That": Calibrating Cybersecurity Safeguards and Disclosures*, 68 BUS. LAW. 183, 187 (2012) ("[Compliance with] established, good security procedures was not enough to exonerate a bank from accepting . . . fraudulent wire-transfer orders . . . . [T]he circumstances surrounding them should have aroused suspicions, prompted questions, and led to a hold on processing.").

46. *See* Corey Field, Note, *Corporations and Copyright in Cyberspace: "Hidden" Internet Regulation and the Corporate Director's Duty to Monitor*, 27 DEL. J. CORP. L. 99, 117–18 (2002); Emily Kuwahara, *Torts v. Contract: Can Microsoft be Held Liable to Home Consumers for its Security*, 80 S. CAL. L. REV. 997, 1003 (2007) ("[T]he economic loss doctrine precludes recovery [in tort] for the financial damage resulting from a security breach because there is often no physical injury or harm to other property").

47. *See* Lunn, *supra* note 39, at 135 (predicting that "corporate law will evolve to hold corporate directors more accountable for cybersecurity oversight").

48. *See, e.g.*, Hackett, *supra* note 28 (describing costs of litigation from major data breaches as "slaps-on-the-wrist").

49. *See* Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 667 (2000); *infra* Part IV.B; *see also* Meal, *supra* note 42, at *5.

50. *See* Peter Sloan, *The Reasonable Information Security Program*, 21 RICHMOND J.L. & TECH. 1, 42 (2014) ("[C]ompanies that store, process, or transmit payment card

claims from card issuers, such as banks and credit unions,[51] and costly litigation about contracted fines from the card brands, including Visa, MasterCard, and others.[52] This system is formally known as the Payment Card Industry's Data Security Standard (PCI-DSS) and is a prototypical example of a technology-focused framework for cyber-readiness.[53] However, consumers of breached companies have rarely

information may by contract be subject to the Payment Card Industry (PCI) Data Security Standard, which sets forth extensive, detailed security safeguards and controls for cardholder data. Organizations should therefore consider their contractual obligations when identifying the types of information to which they will apply security safeguards."); Jason Wright & Kevin Lyles, *Merchants Must Be Aware of Potentially Mishandled Credit Card Information*, PRIVACY & DATA SECURITY L.J., May 2009, at 457, http://www.jonesday.com/files/Publication/1146afd4-5553-447d-b15b-04d9c22f04f4/Presentation/PublicationAttachment/cd1d72c9-9ae0-44f2-b93f-098707140f9c/wright.pdf ("When sued by issuers, merchants may also find the basis of liability is their failure to comply with the PCI Data Security Standards ('PCI DSS').").

51. Note that two major credit card brands, American Express and Discover, are both a card issuer and a card processor. Dawn Papandrea, *Processors vs. Issuers: What Consumers Should Know*, CARDRATINGS (Mar. 15, 2016), http://www.cardratings.com/processors-vs-issuers-what-consumers-should-know.html.

52. Processors generally pass portions of this cost on to non-compliant merchants. Eduard Goodman, *Store's Data Breach Reveals Payment Card Liability Quandary*, BUS. INS. (July 5, 2015, 12:01 AM), http://www.businessinsurance.com/article/20150705/ISSUE0401/307059999/data-breach-at-midwest-grocer-schnucks-reveals-payment-card?tags=%7C302%7C75%7C299 ("[P]ayment card institutions . . . [hold] retailer[s] liable for . . . various fines and penalties . . . [and] most organizations prefer to pay these assessments rather than fight them."). Ultimately, merchant companies are at risk from major lawsuits filed by credit card issuers and banks that cover costs of fraudulent charges as banks have sought indemnification from merchants based on compliance standards. Wright & Lyles, *supra* note 50, at 457, 460 ("Credit card issuers have been pointing to merchants' failure to comply with the PCI DSS as a basis after the data security breach. These cases are significant to merchants because liability for acquiring banks will swim upstream to merchants."). Card payment brands are also allowed to fine banks $5,000 to $100,000 a month for PCI violations. *PCI Facts*, PCICOMPLIANCEGUIDE.ORG, https://www.pcicomplianceguide.org/pci-faqs-2/ (last visited Oct. 22, 2016). Note, the credit card industry has responded to increasing levels of data theft by adopting chip-and-pin technology and, as of October 2015, this new security model shifts pre-existing liability frameworks under PCI-DSS. Now "if a retailer is not using a terminal that can read the new cards and a security breach occurs involving a chip card, the retailer will be liable . . . [but if] the retailer is chip-and-PIN enabled, the card issuer will be liable." Nandita Bose, *Costly Shift to New Credit Cards Won't Fix Security Issues*, REUTERS (Mar. 3, 2015, 5:09 PM), http://www.reuters.com/article/us-usa-cybersecurity-retail-insight-idUSKBN0LZ0GC20150303. Nevertheless, not all retailers implement chip readers and these chips do not prevent thieves from stealing card numbers for online use. Marco Borza, *EMV Chip and PCI DSS Integration Is the Way to Secure Cardholder Data*, NTT SECURITY (July 9, 2015), http://blog.ntt-security.com/emv-chip-and-pci-dss-integration. Thus, chip technology should be used in combination with PCI-DSS compliance, not in lieu of it. *Id.*

53. *See* Jaikumar Vijayan, *After Target, Neiman Marcus Breaches, Does PCI Compliance Mean Anything?*, COMPUTERWORLD (Jan. 24, 2014, 3:58 PM), http://www.computerworld.com/article/2486879/data-security/after-target—neiman-marcus-breaches—does-pci-compliance-mean-anything-.html (stating that given the recent

been able to recover under this framework and are overwhelmingly unsuccessful in relying on a corporation's implied "contractual promise to protect personal information and [a] breach [of that] obligation" as a basis for harm.[54] Consumers have had equal difficulty asserting negligence claims under state tort laws.[55]

Thus, broadening business cyber-liability is critical for establishing effective and "reasonable" corporate cyber-safeguards. Such safeguards are especially necessary since consumer plaintiffs continue to struggle with holding breached companies accountable for poor corporate cyber-practices.[56] Until existing questions around corporate cybersecurity fiduciary duties and regulatory obligations are clarified, private cyber-standards stand out as the most useful benchmark in framing broader corporate cyber-responsibilities.

II.
TECHNICAL CYBERSECURITY SOLUTIONS AND THE PCI-DSS

Any business that takes card payments is a potential target.

—Verizon, PCI Compliance Report 2015[57]

A. Credit Card Breach Reform is Key to Advancing the Cybersecurity Conversation

The credit card payment industry is among the most rapidly evolving industries in America. Card payment transactions comprise

---

breach at an arguably PCI-DSS compliant company like Target, "it would be counterproductive to try to jam attack-specific requirements into standards. It makes no sense"); Seth Harrington, Michelle Visser & David Cohen, *FTC Study Could Lead to Changes in PCI DSS Certification*, LAW360 (Sept. 1, 2016, 10:31 AM), www.law360.com/articles/777947/ftc-study-could-lead-to-changes-in-pci-dss-certification (By understanding the PCI DSS process, "the FTC can apply the lessons learned to advocate for similar models being adopted outside the payment card industry").

54. Meal, *supra* note 42, at *5; *see, e.g.*, *In re Zappos.com, Inc.* ., No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013) (court declined to equate general corporate privacy policies with enforceable contracts). Note, however, that business-to-business contract claims have been largely more successful than business-to-consumer ones.

55. *See, e.g.*, *In re* Sony Gamin Networks and Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 962–63 (S.D. Cal. 2012) ("The breach of a duty causing only speculative harm or the threat of future harm does not normally suffice to create a cause of action for negligence.").

56. *See* Black, *supra* note 41, at 206 ("As most data breach class actions have been dismissed for lack of damages, courts generally have not examined what might constitute reasonable data security when plaintiffs allege negligence.").

57. VERIZON, 2015 PCI COMPLIANCE REPORT 4 (2015), http://www.verizonenterprise.com/pcireport/2015/ (follow "Get 2015 PCI report" hyperlink) [hereinafter VERIZON 2015 PCI REPORT].

over two-thirds of U.S. purchases, totaling an annual value of over $1 trillion dollars.[58] Recent technological developments in the industry include mechanisms for contactless payments, cloud-storage, and mobile payments, and each of these new payment technologies adds potential for novel cyber-breach issues.[59] The technology-savvy and rapidly changing nature of payments make credit card information theft and corresponding corporate liability a useful reference point for the evolving infrastructure of the broader business community.[60]

The prevalence of online credit card theft and the relative ease of calculating the harms from such theft place credit information security at the epicenter of a broader debate on reasonable and necessary cyber-measures. Two features of the credit industry forced credit card companies to become leaders in developing private pre-breach cybersecurity standards. First, multi-stop circulation between payment terminals and payment processors makes credit card information particularly vulnerable.[61] Second, thieves and fraudsters can quickly monetize credit card information, which makes such information a likely target.[62] Under this evolving high-risk and high-cost environment, the PCI-DSS developed to be "the most comprehensive and specific set of [pre-breach] security controls ever compiled into a major industry standard or law."[63]

---

58. FED. RESERVE SYS., THE 2013 FEDERAL RESERVE PAYMENTS STUDY 14, 26 (Dec. 18, 2013), https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf.

59. *See* Edward A. Morse & Vasant Raval, *Private Ordering in Light of the Law: Achieving Consumer Protection Through Payment Card Security Measures*, 10 DEPAUL BUS. & COM. L.J. 213, 234 (2012) ("As cloud computing practices emerge, moving the locus of data from the source to third-parties and public clouds, additional players in the PCI domain may bear responsibility for security, adding to the complexity in this environment. Thus, the industry faces an essential challenge of addressing security needs in this dynamic environment.").

60. *See id.* at 233–34.

61. *See* FIRST DATA THOUGHT LEADERSHIP & ROB MCMILLON, WHERE SECURITY FITS IN THE PAYMENTS PROCESSING CHAIN 3 (May 2010), https://www.firstdata.com/downloads/thought-leadership/where_security_fits.pdf ("As cardholder data flows from one entity to another and is aggregated at various collection points . . . . [criminals] . . . target the most vulnerable links in this chain.").

62. *See* Westervelt, *supra* note 27 ("Thieves will continue to strike at massive retailers and credit card processors to make a quick sale of the data on underground forums.").

63. *Top 10 Misconceptions About PCI*, FOCUS ON PCI, http://www.focusonpci.com/site/index.php/Articles/pci-misconceptions.html (last visited Sept. 27, 2016) ("Unlike most security standards today . . . PCI has done more than require simple frameworks for security. There is a 73 page document outlining the Requirements and Security Assessment Procedures with other supporting documents on the PCI Security Standards Council website.").

Two recent cases highlight the interplay between private-compliance contracts and the broader boundaries of security responsibilities.[64] In *Genesco, Inc. v. Visa U.S.A., Inc.*, Visa sought $13.3 million of PCI-DSS fines when the cyber-practices of Genesco, an apparel retailer, did not prevent hackers from targeting unencrypted credit card data in transit.[65] Genesco, however, argued that its practices should not be subject to such fines since the privatized security protocol merely recommended, and did not require, adoption of certain technical solutions like network segmentation.[66] Additionally, Visa "conceded that there's no forensic evidence that any data related to a Visa account was stolen," thereby emphasizing the importance of calculating harm that arises from the mere possibility of information theft.[67] This case highlights the limitations of enforcing a strict, technical checklist security standard and could impact the scope of privatized penalties for cyber-breaches.

Another notable case is the 2013 Target breach that compromised as many as seventy million customer accounts.[68] Target was PCI-DSS compliant at the time of the breach.[69] Nevertheless, Target's directors and officers were eventually hit with derivative lawsuits alleging "breaches of fiduciary duty, gross mismanagement, waste of corporate assets and abuse of control."[70] This case puts into question both the effectiveness of technical standards for preventing cyber-breaches and the usefulness of technical standards as a shield for liability. Given the prevalence of such legal questions in credit information breach cases,

64. *See, e.g.*, Westervelt, *supra* note 27 ("You can have encrypted everything, but a breakdown in the process or in your organization will open up security problems and you have a breach . . . . [thus,] [b]eing PCI-compliant doesn't make you secure; it only [helps to] protect[ ] you from the lawsuits.").

65. Genesco, Inc. v. Visa, U.S.A., Inc., 302 F.R.D. 168, 171 (M.D. Tenn. 2014).

66. *Id.* at 173–74; *see also* David L. Silverman, *Developments in Data Security Breach Liability*, 70 BUS. LAW. 231, 239–41 (2014/2015).

67. Emily Field, *Retailer Moves for Win in $13M Visa Data Breach Suit*, LAW360 (Nov. 24, 2015), http://www.law360.com/articles/731094/retailer-moves-for-win-in-13m-visa-data-breach-suit; Genesco, Inc. v. Visa, U.S.A. Inc., No. 3:13cv202, 2013 WL 3790647, at *7 (M.D. Tenn. July 18, 2013).

68. Summe, *supra* note 4 ("Target announced that hackers stole personal information . . . .").

69. *See In re Target Corp., supra note 33* ("Target held itself out as having secure data systems . . . ."); Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 17, 2014, 10:31 AM), http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data (then-CEO affirming that "Target was certified as meeting the standard for the payment card industry (PCI) in September 2013. Nonetheless, we suffered a data breach").

70. Collier v. Steinhafel, No. 0:14CV00266, 2014 WL 321798, at *44 (D. Minn. Jan. 29, 2014).

it is unsurprising that looking at the credit card industry's technical framework for cybersecurity gets to the heart of broader cybersecurity shortcomings and potential areas for improvement.[71]

B. PCI-DSS Overview

PCI-DSS is a multi-tiered, annual audit-based protocol, instituted in 2005 by a consortium of payment card brands, known formally as the Payment Card Industry's Security Standards Council (PCI-SSC).[72] Payment card issuers require PCI-DSS compliance from all merchants who collect credit card information from consumers.[73] Each payment card brand has a tiered, card-specific framework for merchant accountability levels and a corresponding enforcement system that incorporates PCI-DSS's twelve primary focus areas.[74] The PCI-DSS information supply chain is best summarized as follows:

---

71. *See* Goodman, *supra* note 52. *See generally* Paul R. Gupta et al., *Living in a Post-Breach World: What Regulators, the Courts, the Executive Branch, and Congress Are Doing About Cybersecurity*, 17 NO. 1 FINTECH L. REP. 1, 5 (2014) ("[S]tolen credit card information . . . cases have just begun to be filed in high-profile data breach events . . . and it remains to be seen how they play out.").

72. *See PCI Security*, PCI SECURITY STANDARDS, https://www.pcisecuritystandards.org/pci_security/ (last visited Oct. 29, 2016); Morse & Raval, *supra* note 59, at 235-36 (including, as an example, a chart of compliance requirements per merchant tier for Visa); Kim Zetter, *The 10 Biggest Bank Card Hacks*, WIRED (Dec. 2, 2014), http://www.wired.com/2014/12/top-ten-card-breaches/.

73. *See* JULIA S. CHENEY, FED. RESERVE BANK OF PHILA., HEARTLAND PAYMENT SYSTEMS: LESSONS LEARNED FROM A DATA BREACH 1 (Jan. 2010), https://www.phil.frb.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2010/d-2010-january-heartland-payment-systems.pdf ("The term 'merchants' is broadly defined to include not only retail merchants but also any entity, such as a doctor's office, that accepts card-based payments in exchange for goods or services.").

74. *See* PCI SEC. STANDARDS COUNCIL, PCI DSS QUICK REFERENCE GUIDE v. 3.1 9 (May 2015), https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf (listing the twelve focus areas as: 1) installing and maintaining firewalls; 2) using non-vendor supplied system passwords and security parameters; 3) protecting stored data; 4) encrypting data transfers in open, public networks; 5) using and updating of anti-virus programs; 6) developing and maintaining secure systems; 7) restricting access to data; 8) assigning unique IDs for data access 9) restricting physical access to data; 10) tracking and monitoring access to data; 11) regularly testing security systems; and 12) maintaining information security policy). *See generally The Data Security Operating Policy*, AM. EXPRESS, www.americanexpress.com/datasecurity (last visited Oct. 29, 2016); *Discover Information and Security Compliance (DISC)*, DISCOVER, www.discovernetwork.com/fraudsecurity/disc.html (last visited Oct. 29, 2016); *PCI-DSS-Payment Card Industry Data Security Standard*, JCB INT'L, http://www.jcbeurope.eu/business_partners/security/pcidss.html (last visited Nov. 2, 2016); *Protecting the Payments Ecosystem*, MASTERCARD, www.mastercard.com/sdp (last visited Oct. 29, 2016); *Data Security Compliance*, VISA INC., www.visa.com/cisp (last visited Oct. 29, 2016); *Security*, VISA EUROPE, www.visaeurope.com/ais (last visited Oct. 29, 2016).

> When a customer presents her credit card to a merchant, the merchant swipes the card to transmit confidential data of her account to an "Acquirer Bank," which relays the data to a "Payment Processor," that then forwards it to the Issuer Bank that issued the customer her card. The Issuer Bank checks if the cardholder has sufficient credit in her account and, if so, approves the payment and transmits its decision back through the chain . . . . In [the] Visa and MasterCard network[s], there is a contract between a merchant and an Acquirer Bank, and a contract between an Acquirer Bank and a Payment Processor, but not between Issuer Banks and Payment Processors.[75]

Additionally, card processors require merchants with high card-transaction rates to employ a third-party Qualified Standard Assessor (QSA) to measure and certify PCI-DSS compliance,[76] although smaller organizations are able to achieve compliance status through "Self-Assessment Questionnaires" (SAQs).[77] Companies that choose not to comply with PCI-DSS are likely to get less beneficial commercial terms, including outright preclusion from participating in the payment card system.[78]

PCI-DSS standards amount, in short, to "a list of requirements . . . that companies processing credit or debit card payments [must] have in place."[79] The breadth of the twelve general requirements creates the illusion that the PCI-DSS framework "is rarely prescriptive about specific technologies."[80] In reality, however, each general requirement of PCI-DSS has several subdivisions that include more technical specifications, such as installing "a firewall configuration," updating "anti-virus software," changing "vendor-supplied defaults for system passwords," and "encrypt[ing] transmission of cardholder data across open, public networks," to name a few.[81] These subdivisions total to more than 300 technical requirements[82]—over 100 of which were new requirements added in 2015.[83]

---

75. Richard L. Trope & Lixian Loong Hantover, *In the Wake of Cyber Damage: Significant Decisions in Cybersecurity 2013-2014*, 70 BUS. LAW. 223, 224 (2014/2015).

76. CHENEY, *supra* note 73, at n.10 (noting that over 100 companies act as QSAs).

77. PCI SEC. STANDARDS COUNCIL, *supra* note 74.

78. J. Craig Shearman, *Retailers Ask FTC to Investigate Credit Card Industry's PCI Security Group for Antitrust Concerns*, NAT'L RETAIL FED'N (June 2, 2016), nrf.com/media/press-releases/retailers-ask-ftc-investigate-credit-card-industrys-pci-security-group.

79. Zetter, *supra* note 72.

80. VERIZON 2015 PCI REPORT, *supra* note 57, at 30.

81. PCI SEC. STANDARDS COUNCIL, *supra* note 74.

82. Morse & Raval, *supra* note 59, at 230.

83. Mont, *supra* note 32.

C. The Shortcomings of PCI-DSS's Emphasis on Technical Solutions

By focusing on technical fixes to security issues, it becomes easy for companies to meet the PCI-DSS requirements—to avoid breach of contract liability, a company merely needs to update systems once a year before their annual compliance certification.[84] While there was an eighty percent increase in the number of PCI-DSS compliant companies between 2014 and 2015,[85] the fact that four out of five compliant companies still fail interim assessments of security controls remains troubling and shows the loopholes of technical cybersecurity solutions.[86] Furthermore, several of the required technologies, such as SSH, VPN, and TLS for password protection, are "easy-to-use" despite the fact that businesses frequently fail to implement them.[87] These statistics reflect that most companies "run upgrades of security software and hardware only when they approach an annual compliance check," leaving them vulnerable to attacks during most of the year.[88] Verizon's highly-regarded PCI report suggests these failures show a "lack of process" for managing and monitoring technical security mechanisms on a regular basis.[89]

Because these companies treat PCI requirements as a one-and-done security checklist,[90] it is not surprising that nearly every certified, PCI-compliant company who is breached has their compliance status retroactively questioned in a post-breach assessment.[91] For data protection and continual PCI-DSS compliance to become business as usual, organizations must integrate improved risk-management sys-

84. Bose, *supra* note 52; Nandita Bose, *Eighty Percent of Global Merchants Fall Short on Card Compliance: Report*, REUTERS (Mar. 11, 2015), http://www.reuters.com/article/us-cybersecurity-usa-idUSKBN0M70BD20150311.

85. VERIZON 2015 PCI REPORT, *supra* note 57, at 2.

86. *Id.*

87. *Id.* at 33.

88. *See* Bose, *supra* note 84.

89. *See* VERIZON 2015 PCI REPORT, *supra* note 57, at 33 (stating that "[t]here is no reason for so many companies to fail" at implementing common breach-preventative technologies).

90. *See* CISCO, 2016 MIDYEAR CYBERSECURITY REPORT 53 (2016), https://www.cisco.com/c/dam/assets/offers/pdfs/midyear-security-report-2016.pdf ("Organizations of all sizes and in all industries need to move beyond 'checking off the boxes' approaches that are no longer sufficient for modern threats."); *see also* VERIZON 2015 PCI REPORT, *supra* note 57, at 27 ("[M]any companies still treat compliance as a one-off tick-box exercise or fire drill that the security team owns and the rest of the organization begrudges. This is not only expensive and disruptive, but doing so leaves them more vulnerable to data breaches caused by changes to processes or infrastructure that happen between assessments.").

91. Zetter, *supra* note 72.

tems.[92] However, many organizations continue to utilize ineffectively "designed and/or implemented controls, or manual operations that are both error-prone and costly to maintain."[93]

Many people argue that breaches at companies that have passed PCI-DSS assessments still occur because PCI standards function as a baseline, not a foolproof barrier.[94] For instance, some of the technologies PCI-DSS explicitly requires are "consider[ed] outdated" by security professionals.[95] Unless companies go beyond the baseline, this technology will not adequately protect digital information.[96] Even more generalized requirements within PCI-DSS, such as the "protection of cardholder data," are ineffective unless a company incorporates cybersecurity into its risk management system. The necessity of a company-wide framework for cyber-risks also manifests in technical implementation issues, such as using ineffective encryption mechanisms.[97] In sum, when companies "don't know what [the] risks are, [they are] just crossing . . . [their] fingers and hoping [they] are buying the right tools and investing in the right people and processes."[98] A company-wide risk management framework, instead of a checklist standard, fosters thoughtful cyber-breach preparedness tailored to each business's needs and priorities.[99]

As written, the annual certification of PCI-DSS compliance is not sufficient to incentivize companies to adopt a risk management framework that incorporates continuous assessments of threats and protocols.[100] The PCI-SSC has recognized this shortcoming. In response,

92. TANIUM & NASDAQ, *supra* note 13.

93. VERIZON 2015 PCI REPORT, *supra* note 57, at 26.

94. CHENEY, *supra* note 73, at 4.

95. VERIZON 2015 PCI REPORT, *supra* note 57, at 31.

96. *See* TANIUM & NASDAQ, *supra* note 13, at 5 ("Even when an organization has the best technology in the world, if the people who are safeguarding that organization's most trusted information don't know how to be accountable and responsible, the company is still at great risk.").

97. THOMAS L. HAHLER, DATA BREACH ENCRYPTION HANDBOOK 237 (Lucy Thomson ed., 2011), http://www.americanbar.org/content/dam/aba/publications/books/data encryption.authcheckdam.pdf (detailing scenarios where encryption fails to protect data); *see, e.g.*, CISCO, *supra* note 90, at 33 ("The time has come for many organizations to face the reality that they must move away from products that are no longer supported and cannot be upgraded to meet today's security challenges.").

98. Mont, *supra* note 32 ("[Cybersecurity] [s]uccess will hinge on changing the payment industry's mindset from a focus on technology, to one centered around risk mitigation.")

99. CISCO, *supra* note 90, at 53 (emphasizing that "true threat intelligence" requires context-specific business assessments).

100. *See* VERIZON 2015 PCI REPORT, *supra* note 57, at 2 (recent review of PCI-compliance found that even among companies instituting the standards, four out of five companies fail at interim assessments of security controls); *see also* NRF, PCI

the 2010 revision to the PCI standard added a requirement for all organizations to self-identify cyber-risks.[101] The third iteration of the PCI-DSS framework in 2015 further embraced a corporate risk management process as one of its twelve principal areas.[102] Nevertheless, in the five years since a holistic element was added among the PCI-DSS's requirements, PCI-DSS certified companies have continued to suffer from data breaches and still report difficultly in conducting internal risk assessments.[103] In other words, its numerous technical security requirements overshadow the PCI-DSS holistic risk management parameters.[104]

It is noteworthy that the PCI-SCC releases a framework of best practices. But, it is unclear how, if at all, companies are motivated to adopt these practices[105] when "companies are not being assessed for their readiness in dealing with new threats."[106] Instead, technical requirements need to be detangled from holistic cyber-mindfulness if top-down, risk management systems are to incentivize better business objectives. Elevating liability for poor risk management under the PCI-DSS is, thus, critical to increasing the corporate adoption of effective cybersecurity practices.[107]

DATA SECURITY STANDARDS: FEDERAL STANDARD-SETTING AND COMPETITION POLICY CONCERNS 10 (May 23, 2016), https://nrf.com/sites/default/files/PCI-2016-NRF%20White%20Paper%20on%20PCI%20DSS.pdf ("PCI's standards do not prioritize effectiveness or performance-based measures of success [and instead impose] detailed, highly complex, costly technical specifications.").

101. PCI SEC. STANDARDS COUNCIL, PCI DSS QUICK REFERENCE GUIDE v. 3.0 (Aug. 2014), https://www.pcisecuritystandards.org/documents/PCISSC%20QRG%20August%202014%20-print.pdf.

102. Mont, *supra* note 32; *PCI 2.0 Encourages Risk-based Process: Three Things You Need to Know*, THE TECHNOLOGY SIDE OF GRC (Aug. 23, 2010), https://agiliance.wordpress.com/2010/08/23/pci-2-0-encourages-risk-based-process-three-things-you-need-to-know/ [hereinafter *PCI 2.0*].

103. *See* Vijayan, *supra* note 53; Mont, *supra* note 32 (emphasizing internal, regular risk-assessments as one of the biggest challenges to meeting PCI DSS requirements).

104. *See PCI 2.0*, *supra* note 102 (noting that emphasis on security requirements and products can distract from a bigger picture view of cybersecurity risks).

105. VERIZON 2015 PCI REPORT, *supra* note 57, at 27 (evaluating four types of necessary PCI-DSS Requirements sustainability); *see* Avivah Litan, *How PCI Failed Target and U.S. Consumers*, GARTNER (Jan 20, 2014), http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/ ("[PCI] eliminated that safe harbor right"); Mont, *supra* note 32 (noting that a "large number of organizations" postpone implementation of these practices until an "annual attestation window[ ] approaches").

106. Vijayan, *supra* note 53.

107. *See* Mont, *supra* note 32; *see also* Shaw, *supra* note 38, at 558 (noting that PCI DSS principals for data security can be expanded from credit cards to other types of protectable data).

III.
HOLISTIC RISK MANAGEMENT AND THE NIST FRAMEWORK FOR CYBERSECURITY

> *[C]ompanies could have better protected consumers' information if they had followed fundamental security practices like those highlighted in the [NIST] Framework.*[108]
>
> —Federal Trade Commission Guidance, Aug. 31, 2016

A. The Importance of Holistic Risk Management

Technology-agnostic standards—standards that do not focus on specific technical requirements—have a clear future in defining corporate liability for cybersecurity breaches.[109] There is a need for cross-industry guidelines to raise corporate cyber-preparedness and incentivize pre-breach protocols that protect information assets. Moreover, holistic risk management is an "elegant" and flexible mechanism to "steer conversation[s] regarding how a company should review its core [cyber-]processes" and attribute responsibility for cyber-breaches.[110] With broad parameters for "reasonableness" and a technology-neutral focus, holistic frameworks allow companies to adopt risk management systems regardless of a company's size, current cyber-sophistication level, or compliance infrastructure.[111]

B. NIST Framework Overview

The most prominent holistic framework for pre-breach cyber-preparations is the government-created National Institute of Standards and Technology (NIST) Framework.[112] Adopted on February 12,

108. Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMM'N (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

109. *See* FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES 8 (2015), http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf ("Failure to address cybersecurity risks adequately from a governance perspective . . . increases regulatory risks for firms.").

110. Ferrillo, *supra* note 31 ("[There is a grave] need to help companies organize their discussions around cyber security in a way that could be used by all directors, officers, and employees, whether they are technologically savvy [or] not . . . . [a]nd that is what the [NIST] Framework is all about.").

111. Shields, *supra* note 9, at 347–48. Lei Shen, *The NIST Cybersecurity Framework: Overview and Potential Impacts*, 10 NO. 6 THE SCITECH LAWYER at 17 (2014).

112. *See Cybersecurity Framework Workshop 2016*, NIST, https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016 (last visited Oct. 29, 2016) (noting that President Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013, which "directed NIST to work with stakeholders to develop a voluntary framework"—based on existing standards, guidelines, and practices—"for reducing cyber risks to critical infrastructure");

2014, the NIST Framework is purposefully "abstract" so that it may function as a living document.[113] For instance, it "never uses the word 'firewall,'"[114] a common, technological component of network security.[115] The three components of the NIST Framework—the Core,[116] the Profiles,[117] and the Tiers[118]—allow organizations to "correct[ly] mix . . . people, process, and technologies" to develop or review corporate cyber-risk protocols.[119] The voluntary framework outlined by NIST was created for critical infrastructure sectors,[120] but many diverse industries have adopted it willingly and several governmental organizations have issued guidance on its relationship to enforcement actions.[121] With such widespread incorporation, the question is what,

---

Joe Adler, *Why Obama's 'Voluntary' Cybersecurity Plan May Prove Mandatory*, AM. BANKER (Feb. 14, 2014), http://www.americanbanker.com/issues/179_32/why-obamas-voluntary-cybersecurity-plan-may-prove-mandatory-1065651-1.html.

113. Selyukh, *supra* note 6.

114. *Id.*

115. Mae Anderson, *Companies' Data Security in Question After Sony Breach*, SALON (Dec. 19, 2014), http://www.salon.com/2014/12/19/companies_data_security_in_question_after_sony_hack/ ("'In the past people were looking for a firewall or an individual product,' for protection, says Chapman, a retired Navy intelligence officer who specialized in hunting down hackers. 'Now, they're realizing there is a human element.'").

116. Shen, *supra* note 111, at 17 ("The Core presents a variety of cybersecurity-related activities and outcomes that can be found in a cybersecurity program, such as the performance of vulnerability scans and the detection of malicious code.").

117. *Id.* (finding that Profiles summarize and align "an organization's cybersecurity activities (such as those found within the Framework Core) with its business requirements, risk tolerances, and organizational resources").

118. *Id.* at 18 ("There are four Tiers available, ranging from Tier 1 (Partial) to Tier 4 (Adaptive). Each Tier refers to an increasing level of rigor and sophistication in an organization's cybersecurity practices.").

119. PWC, GSIS 2015 SURVEY, *supra* note 18, at 32; *see also* Selyukh, *supra* note 6 ("The White House has emphasized the voluntary nature of the framework and the need for companies to view cybersecurity as a business decision, part of its risk-management strategy.").

120. NAT'L INST. OF STANDARDS & TECH., *supra* note 9, at 3. (noting that the Framework was created to "manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services"); *see also* Mike Flack, *What the New NIST Cybersecurity Framework Means to You*, CIPHERPOINT (June 30, 2014), https://cipherpoint.com/2014/06/what-the-new-nist-cybersecurity-framework-means-to-you/ (listing the critical industries as: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, Water and Wastewater Systems).

121. *See, e.g.*, Arias, *supra* note 108; SEC OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATION, *supra* note 39; FIN. INDUS. REGULATORY AUTH., *supra* note 109.

if anything, the NIST Framework means for establishing a corporate liability "baseline" for cybersecurity practices.[122]

The Framework's priorities imply that best cyber-practices exist when organizations regularly review their cyber-activities, formally incorporate a cybersecurity program into operational risks, communicate effectively about cyber-issues, and are conscious of the shifting cybersecurity landscape.[123] The Framework's Core, for example, "steers conversations"[124] on corporate cyber-processes through a five-factor analysis: identification, protection, detection, response, and recovery, all of which help define valuable cyber-assets and set employee information access parameters.[125] Even so, the Framework's analytical process can be truly abstracted into "two simple questions": first, what is a company's current cybersecurity infrastructure, and second, what does a company want its cybersecurity program to be capable of going forward.[126]

C. NIST Framework Shortcomings

Many disagree with the significance of the Framework's broad scope and argue that such a cybersecurity standard inadequately considers "specific business risks."[127] However, arguing that the Frame-

122. Flack, *supra* note 120; *see* William T. Um & Paul T. Moura, *Shareholders, Regulators Clamp Down on Boards over Corporate Governance of Cyberrisk*, DEL. CORP. (Jan. 5, 2015) https://www.hunton.com/files/Publication/8dbb9351-62d4-47ce-b8e8-3ded24ce2eb4/Presentation/PublicationAttachment/21e2e662-921d-4661-af6d-9af7587d59de/Shareholders_regulators_clamp_down_on_boards_corporate_governance_cyberrisk.pdf ("Although the NIST framework is not binding law and is targeted at critical infrastructure systems, many consider it to be the best existing model of a 'standard of care' for data security, as well as a benchmark for future legislation."); Selyukh, *supra* note 6 ("NIST standards will become over the next year or two, while we are waiting for legislation, the de facto best practices, just because they are accessible and current.").

123. *See* Shen, *supra* note 111, at 17.

124. PWC, GSIS 2015 SURVEY, *supra* note 18, at 33; Selyukh, *supra* note 6 (finding that companies can use "sweeping categories such as 'access control' or 'data security' to evaluate how effectively a company identifies and protects network assets, and detects, responds to and recovers from breaches").

125. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 9, at 7 (explaining the "Framework Core"); Shen, *supra* note 111, at 17 ("For example, if an organization is concerned about its incident response plan, it can look within the 'Respond' Function. The Respond Function is divided into five Categories—Response Planning, Communications, Analysis, Mitigation, and Improvements. Each of those Categories is broken down into various Subcategories of cybersecurity activities. For example, the 'Response Planning' Category has one Subcategory (*i.e.*, 'Response plan is executed during or after an event').").

126. Ferrillo, *supra* note 31.

127. PWC, RISING RISKS, *supra* note 20, at 13 (emphasizing the importance of aligning a security strategy with business needs).

work is too easy to adopt and suggesting that "executives and employees of any company could [easily] determine the 'what, who, where, when and how'"[128] of cybersecurity best practices does not account for the multitude of companies that have utterly failed to consider and implement holistic cyber-awareness or protocol implementation.[129]

Other critics complain that cybersecurity frameworks need a checklist structure to help quantitatively demonstrate that a Board "exercised their fiduciary duties" despite a major cyber-breach.[130] Yet, simply utilizing a rigid compliance checklist for risk management governance raises many of the same issues that the PCI-DSS has faced: inflexible adjustments in the wake of dynamic threats, infrequent instead of sustainable checklist implementation, and the risk of walking-back compliance certifications in the event of breach. Significantly, enforcement actions have already elevated the perceived usefulness of liability standards similar to the NIST Framework.[131] Claiming that NIST's vague and qualitative parameters undermine its practicality as a cyber-standard reflects neither the reality of ongoing regulatory actions nor the need for greater cyber-responsibility incentives.

IV.
PROPOSAL

> *It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.*
>
> —Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"[132]

Although the NIST Framework is not binding law, many believe it is nevertheless "the best existing model of a 'standard of care' for

128. Ferrillo, *supra* note 31 (emphasis added).

129. *See, e.g.*, Selyukh, *supra* note 6 ("Many experts have expressed alarm about the lack of awareness or reluctance among some companies' leaders to spend more money on cyber defenses.").

130. *See* Ferrillo, *supra* note 31 (criticizing the lack of clarity about how companies are using the Framework).

131. *See, e.g.*, Arias, *supra* note 108; Shen, *supra* note 111, at 19 (noting in the recent data security case against Wyndham Hotels, the defendants' cited the NIST Framework as an exemplar of a reasonable security standard)

132. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

data security," and is likely to influence litigation outcomes.[133] This view has become even more prevalent following failures of private compliance checklists to protect against large-scale cyber-breaches.[134] While the latest versions of the PCI and NIST standards both encourage corporate cultures to "focus[ ] on achieving comprehensive and effective cybersecurity," only the NIST Framework prioritizes dynamic and holistic cybersecurity practices.[135] Moreover, this dueling approach to proper corporate cyber-practices hits on a key cyber-policy question: Without clear direction from Congress, how can public and private regulatory bodies best encourage corporate adoption of enterprise-wide cyber-policies and procedures?

Potential answers stem from expanding the boundaries of corporate law and reassessing cyber-breach contractual terms. By pushing forward more cases that assess the scope of unfair cyber-practices, regulators and shareholders can continue to help to clarify irresponsible corporate practices.[136] Moreover, changing the focus of private cyber-standards would rapidly encourage corporations to adopt reasonable, mindful, and enterprise-level cyber-protections and procedures.

A. Regulators Must Continue to Push the Boundaries of Fiduciary Duty

The fact that specific duty parameters of cyber-responsibilities are not "fully tested and defined [by] the courts"[137] should not impede regulators from trying to hold companies accountable for practices

133. Um & Moura, *supra* note 122, at 3.

134. *See, e.g.*, Riley, *supra* note 69 (discussing Target's 2013 breach despite the company's PCI-DSS compliance).

135. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-926T, CYBERSECURITY: CHALLENGES IN SECURING THE GRID 16 (2012) (noting that the existing regulatory environment focuses on compliance with requirements rather than on achieving comprehensive cybersecurity protection); *see* Lunn, *supra* note 39, at 123–24 (referring to court cases suggesting that corporate directors must actively seek out and prevent cybersecurity threats, rather than simply reacting to them); *see also* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 336 (noting that NIST creators "emphasized the importance of the Framework's implementation into all levels of an organization—from senior leadership to employees").

136. *See* Vincent Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 280–82 (2005) ("The duties imposed on a fiduciary—including loyalty, candor, and confidentiality—are sometimes coextensive with those that the law of negligence embraces.").

137. Field, *supra* note 46, at 148 (referring to the confusion of corporate responsibility in the wake of the Internet boom and the Digital Millennium Copyright Act of 1998).

that exacerbate cyber-risks. Luckily, the FTC has brought several enforcement actions on data security, the majority of which resulted in settlements that provide roadmaps for reasonable security management.[138] Additionally, the FTC does not back away when challenged on its authority to enforce data security standards.[139] The FTC successfully litigated that it had the authority to hold Wyndham Worldwide Corporation, a U.S. hotel chain, accountable for failing to "take appropriate steps in a reasonable timeframe" to prevent network compromises after the company discovered multiple cyber-intrusions.[140] Notably, the Wyndham decision suggests that having adequate cyber-protocols amounts to a fiduciary duty.[141] Moreover, since Wyndham arises under a general consumer protection "unfairness" standard, out-of-date presumptions of pre-breach corporate reasonableness should no longer be sufficient to avoid data breach liability.[142]

Critics argue that prosecuting unfair cyber-practices is tantamount to holding corporations accountable for negligence without informing them of specific standards to follow.[143] Nevertheless, litigation emphasizing the necessity of holistic cyber-risk protocols, and holding companies without such programs responsible for

138. *See* James Denvil & Brian Kennedy, *FTC Issues Data Security Guidance and Announces Data Security Conferences*, HOGAN LOVELLS CHRON. OF DATA PROTECTION (July 20, 2015), http://www.hldataprotection.com/2015/07/articles/consumer-privacy/ftc-issues-data-security-guidance-and-announces-data-security-conferences/.

139. *See, e.g.*, Federal Trade Commission Act, 15 U.S.C. § 45 (2011); FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (rejecting Wyndham's Motion to Dismiss); *see also* Russo, *supra* note 8, at 167–68 (describing the *Wyndham* case); Sloan, *supra* note 50, at 51 (describing litigation prosecuting "respondent's failure to develop a comprehensive written information security program.").

140. *See Wyndham*, 10 F. Supp. 3d at 607–08; Trope & Hantover, *supra* note 75, at 226 (discussing the *Wyndham* case).

141. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245 (3d Cir. 2015) ("A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."). *See generally* Lunn, *supra* note 39, at 121–22 (discussing the relationship between the business judgment rule and the duty of corporations to monitor for cyber threats).

142. *Compare* Lunn, *supra* note 39, at 121, 126 ("[Traditionally,] to overcome the [business judgment rule] presumption, a successful plaintiff must prove defendants' actions were grossly negligent."), *with Wyndham*, 799 F.3d at 246 ("If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act[,] whether innocent, negligent, intentionally tortious, or criminal[,] does not prevent the actor from being liable for harm caused thereby.") (citing RESTATEMENT (SECOND) OF TORTS § 449 (1965)).

143. *See* Morse & Raval, *supra* note 59, at 257 ("As long as the parameters of what is 'unfair' are undefined by regulation, a potential exists for . . . [the FTC's] power to be abused."). *But see* Russo, *supra* note 8, at 168 (explaining the *Wyndham* court's rejection of this argument).

breaches, creates a minimum baseline for framing negligent and unfair corporate actions. In the absence of clear statutes defining "unfair" cyber-compliance practices and without adequate avenues for reparations after a breach, enforcing the need for cyber-risk management is the first step in better protecting consumers' digital information.

B. Modifying Private Industry's Cybersecurity Contractual Penalties Re-aligns Corporate Incentives

Improving the transparency of private-sector cyber-liability systems would also promote a more comprehensive and effective adoption of cyber-risk management. Currently, the calculations of monetary penalties under the PCI-DSS standard are considered "secret, biased, and flawed"—breakdowns of penalties per type of violation remain hidden from the companies upon which they are imposed.[144] Companies subject to the PCI-DSS have no ability to review or challenge the PCI standards and the private companies setting the standards do not focus on encouraging the most effective security platforms because they do not pay the costs from a breach.[145] Refocusing the security standard on formalized, holistic procedures would increase the evidence available when challenging PCI liability, in addition to helping companies prepare for, react to, and recover from cyber-breaches.

Assigning weighted monetary values to different types of cyber-risks also highlights risk management as the most important requirement in cyber-compliance checklists. Such a framework would detail why specific fines are levied for different types of infractions. Moreover, it could specifically impose additional fines if a corporation lacks a top-down cyber-risk management process. This framework could also follow the lead of federal sentencing guidelines that permit a downward adjustment for fines when a corporation has "appropriate and effective law compliance programs in place" or when a corporation contributed to cross-industry breach-sharing resources.[146]

C. Additional Positive Effects of Holistic Liability Programs

Leaving more-vulnerable companies behind is not an effective long-term solution for defeating cyber-criminals. Rather, business and

144. *See* Silverman, *supra* note 66, at 239–41 (describing concerns about liability calculations under the PCI standards).

145. *See* NRF, *supra* note 100.

146. Bainbridge, *supra* note 44, at 982; Julie Hirschfeld Davis, *Obama Calls for New Laws to Bolster Cybersecurity*, N.Y. TIMES (Jan. 14, 2015), http://www.nytimes.com/2015/01/14/us/obama-to-announce-new-cyberattack-protections.html.

regulators must work together to identify risks.[147] This partnership is critical given that corporate cybersecurity programs "do not rival the persistence, tactical skills, and technological prowess of their potential cyber adversaries."[148] In fact, a three-year study found that companies uncover their own breaches "in only thirty-one percent of cases" and, among retailers, only in five percent of instances.[149] Government entities and third-party business partners often alert companies to the existence of a data breach. Such statistics emphasize a commonly recognized lesson from data breaches: sharing breach techniques and ineffective technical solutions helps to limit cyber-risks.[150] Information sharing will lead to a greater understanding of how to assign penalties and focus security incentives on different technical areas of cyber-solutions.[151]

In publicly disclosing breaches, companies admit the technical shortcomings in their cybersecurity systems. Companies are, however, unlikely to be willing to have such discussions if monetary penalties or additional liability will then result from these admissions.[152] Current corporate reluctance to reveal compromised security systems is not surprising given that the PCI-SSC members eliminated a safe harbor exception for disclosures and regularly retroactively attest that compliant companies "must not have really been PCI compliant if they got breached."[153] Thus, imposing rigid technical requirements for cyber-liability disincentivizes information sharing and undermines an understanding of "how big a problem" cybersecurity is for all.[154]

147. *See* W. Edward Afield, *Dining with Tax Collectors: Reducing the Tax Gap Through Church-Government Partnerships*, 7 RUTGERS BUS. L.J. 53, 59 (2010) (arguing that similar partnerships in the tax arena would help "effect a culture change by providing more effective forums for . . . education").

148. PWC, RISING RISKS, *supra* note 20, at 4; VERIZON 2015 PCI REPORT, *supra* note 57, at 42 (describing malware at the heart of PCI breaches as "polymorphic" and "constantly changing to evade detection").

149. Riley, *supra* note 69.

150. *See* CHENEY, *supra* note 73, at 6-8 (discussing *Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421 (5th Cir. 2013)).

151. PWC, GSIS 2015 SURVEY, *supra* note 18, at 33 (reporting cyber breaches will aid industries and regulators in becoming "more lenient [on certain technical requirements] and [learn about] areas in which we should be more strict").

152. Id. at 7 (noting that many companies "do not report detected incidents for strategic reasons or because the attack is being investigated as a matter of national security").

153. Litan, *supra* note 105.

154. Hackett, *supra* note 28; *see also* PWC, GSIS 2015 SURVEY, *supra* note 18, at 32 (adopting NIST's agnostic-security approach, enhances awareness of risk through "collaboration and communication of security posture among executives and industry organizations, as well as potential future improvements in legal exposure and even assistance with regulatory compliance").

Refocusing liability on the implementation and effectiveness of risk management procedures could help diminish corporate fears of reporting technical cyber-problems.

Liability grounded in holistic risk management procedures could also help address corporate awareness of and responsibility for "third-party security." Third-party vendors are outside the scope of a company's ability to directly monitor technical requirements.[155] This makes vendors one of the most troubling areas of the current liability framework: their cyber-practices are a key way for criminals to access corporate information, and corporations exert little control over vendors' cyber-management. Increasing corporate awareness and formalized policies on cyber-issues can lead to smarter vendor choices, greater incentives to perform due diligence on chosen third-party vendors, and to align vendor and corporate cyber-privacy policies.[156] Without requiring companies to adopt their own cybersecurity risk management framework, companies cannot know how to hold third-party vendors and business partners accountable.

Pursuing liability through expanded focus on holistic approaches can additionally lead to low cost cybersecurity mechanisms addressing "the weakest link in the security chain"— humans.[157] For instance, in-house training on phishing attacks can help prevent cyber-fraud by forty-two percent while simultaneously raising employee awareness of cyber-issues.[158] The more eyes looking for enterprise-wide cyber-flaws, the more likely a company can prevent breaches from occurring.[159] In fact, "companies that do not have security training for new hires reported annual financial losses that are four times greater than

155. Third-party vendors are among the most significant sources of cyber-risks. PWC, GSIS 2015 SURVEY, *supra* note 18, at 25; *see also* Jaclyn Jaeger, *PCI Guidance Provides Clarity to Payment Card Industry*, COMPLIANCE WK. (Aug. 26, 2014), https://www.complianceweek.com/news/news-article/pci-guidance-provides-clarity-to-payment-card-industry (noting that the latest PCI update now "requires that companies continue to protect customers' credit card data even after outsourcing it to a third-party service provider"); PWC, RISING RISKS, *supra* note 20, at 6 ("[The NIST framework] provides a common language to promote an open dialogue on cybersecurity, both internally and with external entities such as third-party service providers and partners.").

156. *Id.*

157. PWC, GSIS 2015 SURVEY, *supra* note 18, at 27; CHENEY, *supra* note 73, at 8 (in evaluating the root cause of PCI breached in the wake of Heartland, analysts noted that "insider threats may not stem from intentional fraud but rather from misplaced employee goodwill").

158. PWC, RISING RISKS, *supra* note 20, at 14.

159. *See* Ferrillo, *supra* note 31 ("Network security takes a village, involving every employee of the company [and a] culture of security needs to be instilled in every person touching a keyboard or a keypad.").

those that do have training."[160] Implementing technology-blind awareness can help companies give greater consideration to more diverse sources of threats, including overlooked sources like insiders.[161]

V.
CONCLUSION

All of us have a common interest in being protected.

—Jamie Diamond, CEO of JPMorgan Chase[162]

Businesses of all types grapple with the need to adopt the latest technological platforms, even though such technologies are far from immune to data breach threats. Small businesses' misguided belief that they are "too insignificant" to attract threatening actors often translates into risky cyber-practices.[163] Medium-sized organizations, which lack the capital to spend millions on technical cyber-safeguards, are easy targets for cyber-criminals and, thus, are increasingly the focus of cyber-thefts. Even the largest organizations in the corporate system have demonstrated limited cyber-awareness and have not correlated cybersecurity with business success.[164] Given that the breadth of technical cyber-safeguards often overwhelms businesses of any size, making sure that corporations do not disengage and avoid the cybersecurity problem altogether is a priority for the current cyber-landscape. Contractual remedies and targeted litigation that push for baseline cyber-risk management processes are an ideal way to advance this goal. Holistic cyber-risk measures are attainable and effective at preventing breaches for businesses of all sizes and shapes.[165] Thus, the technical nature of cybersecurity is not a sufficient reason to forgo incorporation of enterprise risk management protections into privatized cybersecurity standards.

Looking at cybersecurity from a holistic risk management perspective is a chance for partners in risk to work together.[166] As Target,

160. PWC, GSIS 2015 SURVEY, *supra* note 18, at 34.
161. *See* PWC, RISING RISKS, *supra* note 20, at 9.
162. *Id.* at 6.
163. PWC, GSIS 2015 SURVEY, *supra* note 18, at 20.
164. Id. at 22.
165. *Id.* at 8 (noting that last year, organizations with revenues between $100 million and $1 billion experienced a 64% increase in cyber-incidents).
166. PWC, RISING RISKS, *supra* note 20, at 6 (noting that both retailers and banks have a "common interest in being protected" and can therefore work together to address cybersecurity risks); *see also* Shields, *supra* note 9, at 345 ("JPMorgan Chase ('JPMorgan') CEO Jamie Dimon warned that even though in 2014 alone the company would spend $250 million and assign 1,000 people to addressing cybersecurity issues, the protections still may not be enough to protect the company from cyberattack. Dimon's fears came to fruition just months later when JPMorgan and at least twelve

Wyndham, and the growing multitude of cyber-breaches show, it is too late to institute corporate controls for cybersecurity risk management if one merely waits until a breach happens. As parties on all sides are coming on board with the need for general corporate risk management infrastructure,[167] now is an ideal time for PCI-DSS and other private security standards to push for greater corporate liability when corporations lack holistic risk management procedures and processes.

other financial institutions became victims of a series of coordinated hacking attacks.").

167. J. Nicholas Hoover, *CEOs Voice Support for Cyber Legislation, With Caveats*, INFORMATIONWEEK (Feb. 1 2013), http://www.informationweek.com/regulations/ceos-voice-support-for-cyber-legislation-with-caveats/d/d-id/1108470?ngAction=register (noting that a 2013 Senate report indicated that "nearly every company that provided a thorough response expressed support for more robust, two-way cyber threat information sharing").