


12-1-2016

The Cybersecurity Threat: Compliance and the Role of Whistleblowers

Jennifer M. Pacella

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/bjcfcl>

 Part of the [Administrative Law Commons](#), [Computer Law Commons](#), [Labor and Employment Law Commons](#), [Legal Ethics and Professional Responsibility Commons](#), and the [Securities Law Commons](#)

Recommended Citation

Jennifer M. Pacella, *The Cybersecurity Threat: Compliance and the Role of Whistleblowers*, 11 Brook. J. Corp. Fin. & Com. L. (2016). Available at: <https://brooklynworks.brooklaw.edu/bjcfcl/vol11/iss1/3>

This Article is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Brooklyn Journal of Corporate, Financial & Commercial Law by an authorized editor of BrooklynWorks.

THE CYBERSECURITY THREAT: COMPLIANCE AND THE ROLE OF WHISTLEBLOWERS

Jennifer M. Pacella *

ABSTRACT

In today's technologically dependent world, concerns about cybersecurity, data breaches, and compromised personal information infiltrate the news almost daily. The Securities and Exchange Commission (SEC) has recently emerged as a regulator that is keenly focused on cybersecurity, specifically with respect to encouraging disclosures in this arena by regulated entities. Although the SEC has issued non-binding "guidance" to help companies navigate their reporting obligations in this sector, the agency lacks binding cybersecurity disclosure regulations as they pertain generally to public companies. Given that the SEC has already relied on such guidance in threatening enforcement actions, reporting companies are increasingly pressured for compliance in this arena. This Article addresses the importance of establishing effective internal reporting channels and other internal compliance mechanisms in meeting the SEC's expectations and highlights the role of "cybersecurity whistleblowers," specifically those reporting internally, in building the type of improved corporate culture necessary to discover and remediate cybersecurity risks. Cybersecurity whistleblowers, like all whistleblowers, commonly experience retaliation for their efforts. Despite the SEC's commitment to providing whistleblowers retaliation protections through statutes like the Sarbanes-Oxley and Dodd-Frank Acts, the absence of binding cybersecurity regulations translates into a direct problem for cybersecurity whistleblowers, because their reports are likely to fall outside the scope of "protected activity" enumerated under these statutes. This Article discusses this gap in protections in light of the SEC's heightened cybersecurity focus, the feasibility of SEC adoption of binding cybersecurity disclosure regulations, and the broad contributions of whistleblowers to compliance systems generally.

* Professor Jennifer Pacella is an Assistant Professor of Law at the City University of New York (CUNY), Zicklin School of Business, Baruch College, in Manhattan, and an Adjunct Professor at State University of New York (SUNY) Buffalo Law School. The author expresses gratitude to James Fanto and Brooklyn Law School for the invitation to present this article as part of the annual Symposium of the Brooklyn Journal of Corporate, Financial & Commercial Law, and thanks all of the Symposium participants for their feedback and insights. The author also thanks Guyora Binder, Joseph Gerken, Michael Halberstam, James G. Milles, Matthew Steilen, Rick Su, Larry Trautman, Jay Weiser, and David Zaring for their valuable comments on prior drafts of this article. The author would also like to thank each of the discussants and participants of the Sixteenth Huber Hurst Research Seminar, sponsored by the University of Florida's Warrington College of Business, for their very helpful feedback on an earlier version of this article.

INTRODUCTION

In today's compliance-focused environment, the need to detect and remediate problems of potentially alarming degrees is essential to ensuring effective regulation. Information security systems and technologically savvy business practices are conducive to success in this digital era and have emerged as important tools in compliance monitoring, as they allow compliance officers to identify and address problems through automated reporting and review channels.¹ Although reliance on technology is unquestionably important in the regulation of modern-day business and financial services industries, it simultaneously carries the associated risk of vulnerability to data breaches and other cybersecurity-related threats. The potentially devastating consequences of these threats present compliance challenges for all industries.

Whistleblowers, especially those reporting internally, have emerged as critical players in compliance, bringing red flags to the forefront to ensure that their places of employment are continuously operating within the confines of the law.² "Cybersecurity whistleblowers," defined herein as individuals who escalate concerns regarding internal management of cyber-risks, cyber threats, data breaches, or other cybersecurity related information to supervisors, compliance officers, and boards of directors, play a crucial role in the modern-day compliance functions of regulated entities. The role of whistleblowers generally in corporate compliance and as an "institution" in modern corporate governance has received relatively minimal scholarly attention.³

Whistleblowers are important to good corporate governance and compliance because they are essentially "volunteers" with no pre-existing duty to come forward and often do so out of a personal interest to conform to

1. See Robert C. Bird & Stephen Kim Park, *The Domains of Corporate Counsel in an Era of Compliance*, 53 AM. BUS. L.J. 203, 214 (2016) ("Compliance work can also involve training specialists in the enterprise to work with software or other technology to ensure that the process of monitoring compliance practices occurs smoothly."); see James A. Fanto, *Advising Compliance in Financial Firms: A New Mission for the Legal Academy*, 8 BROOK. J. CORP. FIN. & COM. L. 1, 10 (2013) (discussing how today's "compliance monitoring is aided by technology"); see generally Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in A Digital Age*, 88 TEX. L. REV. 669 (2010) (discussing the use of technology in compliance and risk management).

2. See GEOFFREY PARSONS MILLER, *THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE* 271 (2014) (describing whistleblowing as "an increasingly important mechanism for enhancing an organization's compliance with legal norms"); Jennifer M. Pacella, *Advocate or Adversary? When Attorneys Act as Whistleblowers*, 28 GEO. J. LEGAL ETHICS 1027, 1061 (2015) (internal citations omitted) (discussing the contributions of whistleblowers to compliance, especially with respect to strengthening internal reporting channels).

3. See Matt A. Vega, *Beyond Incentives: Making Corporate Whistleblowing Moral in the New Era of Dodd-Frank Act "Bounty Hunting"*, 45 CONN. L. REV. 483, 485 (2012) (noting that most whistleblowing scholarship highlights the "unwillingness or incapacity of employees to blow the whistle").

legal rules and norms.⁴ Contrary to what may be popular belief, most whistleblowers report internally, rather than externally to the government or third parties, and are often considered very “loyal” employees.⁵ In this way, they provide significant value to an entity’s internal compliance function by raising issues that may otherwise remain unnoticed or ignored. Despite their value, retaliation against whistleblowers remains common, often manifesting itself as retaliatory discharge, ostracism, alienation, job stagnation, or blacklisting.⁶

One of the most increasingly vocal regulators in both the areas of cybersecurity and whistleblower protections is the Securities & Exchange Commission (SEC). The SEC has called upon entities to publicly disclose the cybersecurity and technology-related risks that they face because of the significant impact that the agency believes these issues have on shareholders in making investment decisions.⁷ In October of 2011, the SEC issued non-binding guidance (the 2011 Guidance) alerting public companies to already-existing disclosure requirements that would capture cybersecurity risks and cyber-incidents as material information subject to mandatory disclosure for investors.⁸ This focus on disclosure was emphasized in the SEC’s Roundtable on Cybersecurity, held in March of 2014 (the Roundtable), in which the

4. See MILLER, *supra* note 2, at 271–72 (noting that a whistleblower reports misconduct without being required to do so).

5. See, e.g., Terry Morehead Dworkin, *SOX and Whistleblowing*, 105 MICH. L. REV. 1757, 1760 (2007) (noting that “internal reporting is the most common type of initial whistleblowing”); Christopher M. Matthews, *Most Whistleblowers Report Internally, Study Finds*, WALL ST. J. (May 30, 2012, 9:25 PM), <http://blogs.wsj.com/corruption-currents/2012/05/30/most-whistleblowers-report-internally-study-finds/> (citing an Ethics Resource Center survey finding that in 2011, only 2% of employee-whistleblowers reported externally); Richard E. Moberly, *Sarbanes-Oxley’s Structural Model to Encourage Corporate Whistleblowers*, 2006 BYU L. REV. 1107, 1158 (2006); Robert G. Vaughn, *Statutory Protection of Whistleblowers in the Federal Executive Branch*, 1982 U. ILL. L. REV. 615, 616 n.6 (1982) (“[W]histleblowers are often the most loyal employees.”).

6. See, e.g., Norman D. Bishara, Elletta Sangrey Callahan & Terry Morehead Dworkin, *The Mouth of Truth*, 10 N.Y.U. J.L. & BUS. 37, 56–57 (2013) (noting that it is common for whistleblowers to experience some sort of reprisal, although not all may experience severe retaliation); see generally ETHICS RES. CTR., RETALIATION: WHEN WHISTLEBLOWERS BECOME VICTIMS A SUPPLEMENTAL REPORT OF THE 2011 NATIONAL BUSINESS ETHICS SURVEY 2 (2012); see also *Proof of Retaliation Against Whistleblowers Grows Exponentially According to NAVEX Global’s 2015 Ethics and Compliance Hotline Benchmark Report*, NAVEX GLOBAL (Mar. 10, 2015), <http://www.navexglobal.com/company/press-room/proof-retaliation-against-whistleblower-s-grows-exponentially-according-navex>.

7. Mary Jo White, Chair, U.S. Sec. & Exch. Comm’n, Opening Statement at SEC Roundtable on Cybersecurity (Mar. 26, 2014) [hereinafter White Statement], <http://www.sec.gov/News/PublicStmnt/Detail/PublicStmnt/1370541286468>.

8. Div. of Corp. Fin., U.S. Sec. & Exch. Comm’n, *CF Disclosure Guidance: Topic No. 2*, U.S. SEC. & EXCH. COMM’N (Oct. 13, 2011), <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm> [hereinafter *CF-2 Disclosure Guidance*]; see also Constance E. Bagley, Joshua Mitts & Richard J. Tinsley, *Snake Oil Salesmen or Purveyors of Knowledge: Off-Label Promotions and the Commercial Speech Doctrine*, 23 CORNELL J.L. & PUB. POL’Y 337, 372 (2013) (discussing the mandatory disclosure regulatory regime of the SEC and the way in which mandatory disclosure “reduc[es] misallocation of resources” and ensures that consumers have access to essential information).

agency solicited views about managing cybersecurity from various players in the industry, academics, attorneys, SEC staff, and the general public.⁹

At the same time, the SEC has taken a firm stance on protecting whistleblowers from retaliation and encouraging them to report wrongdoing. SEC Chair, Mary Jo White, recently discussed the “invaluable public service” that whistleblowers provide, urging companies, especially in the years since the financial crisis, to set aside whatever “mixed feelings” they may have traditionally harbored about whistleblowers and consider them as key players in the “new, more aggressive ways” of improving compliance and corporate culture.¹⁰ Chair White also stated that the SEC increasingly views itself as “the whistleblower’s advocate” and noted that the whistleblower program of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), enacted in 2010, “has proven to be a game changer.”¹¹ Dodd-Frank offers strong retaliation protections for whistleblowers who report on violations of the securities laws, including a private right of action in federal court, a lengthy statute of limitations, double back pay, and bounty rewards.¹² Although retaliation protections are also available for whistleblowers under the Sarbanes-Oxley Act of 2002 (SOX), this statute offers only an administrative remedy of filing a retaliation complaint with the Occupational Safety and Health Administration (OSHA) and a shorter statute of limitations.¹³

In light of the key roles that information gathering and internal reporting play in managing the compliance function,¹⁴ this Article proposes that cybersecurity whistleblowers are essential to helping meet the demands of the SEC’s rapidly developing reporting requirements. The emerging phenomenon of cybersecurity whistleblowing has been deemed “the next wave of SEC whistleblowing,”¹⁵ and the relationship between whistleblowers in this sector, retaliation protections, and compliance is ripe for scholarly attention. Compliance in this arena has become even more important given that the SEC has started to bring enforcement actions against

9. See generally White Statement, *supra* note 7.

10. Mary Jo White, Chair, U.S. Sec. & Exch. Comm’n, Speech, The SEC as the Whistleblower’s Advocate, Ray Garrett, Jr. Corporate and Securities Law Institute-Northwestern Univ. Sch. of Law Chicago, Illinois (Apr. 30, 2015), <http://www.sec.gov/news/speech/chair-white-remarks-at-garrett-institute.html>.

11. *Id.*

12. Securities Exchange Act of 1934 (Exchange Act), Pub. L. No. 94-29, §17, 89 Stat. 97 (1975) (codified as amended at 15 U.S.C. § 78u-6 (2012)).

13. Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley Act), Pub. L. No. 107-204, 116 Stat. 745 (2002) (codified as amended at 18 U.S.C. § 1514A (2012)).

14. See White Statement, *supra* note 7; Office of Compliance Inspections & Examinations, *OCIE’s 2015 Cybersecurity Examination Initiative*, NAT’L EXAM PROGRAM RISK ALERT, Sept. 2015, at 1 (noting the importance of governance and risk assessment, employee training, internal controls, and other related measures as essential for managing cybersecurity risks).

15. Webinar, *Cybersecurity Whistleblowers: The Next Wave of SEC Whistleblowing*, ORRICK, HERRINGTON & SUTCLIFFE LLP (Dec. 8, 2015), <https://www.orrick.com/Events/2015/12/Cybersecurity-Whistleblowers-The-Next-Wave-of-SEC-Whistleblowing>.

entities for failing to adequately respond to cybersecurity risks,¹⁶ thereby evidencing yet another way that the agency has significantly expanded its enforcement powers in recent years—an area subject to active scholarly debate.¹⁷

In addition to addressing these issues, this Article finds that the absence of binding SEC cybersecurity regulations, which currently exist only in the non-binding form of the 2011 Guidance, translate into a direct problem for cybersecurity whistleblowers. Such persons are likely to be excluded from the protections of Dodd-Frank and SOX because their disclosures would be beyond the scope of protected activity enumerated under those statutes, which only cover explicit violations of the federal securities laws, rules, or regulations subject to the SEC's jurisdiction.¹⁸

Part I of this Article focuses on the importance of effective information gathering and internal reporting in ensuring that cybersecurity risks are promptly detected and remediated, while also considering the role of compliance officers and boards of directors in processing this information. In creating this type of corporate culture, the critical role of cybersecurity whistleblowers is addressed. Part II explains the weaknesses of whistleblower protections under SOX and Dodd-Frank in light of the absence of binding SEC cybersecurity regulations for reporting companies, which has the likely effect of removing cybersecurity whistleblowers from the category of those who are eligible for relief under the statutes. Part III discusses the general prevalence of cybersecurity-related threats and data breaches in recent years, evidencing that the reports of cybersecurity whistleblowers are increasingly valuable and should be subject to ample protections under the law. Finally, although cybersecurity threats appear to affect consumers more than investors, and thus would seem to fall within the purview of the Federal Trade Commission (FTC) as regulator rather than the SEC, this section hones in on the shareholder effects of such threats as a means to justifying the SEC's stance as a major regulator in this arena.

16. See, e.g., Press Release, U.S. Sec. & Exch. Comm'n, Morgan Stanley Failed to Safeguard Customer Data (June 8, 2016), <https://www.sec.gov/news/pressrelease/2016-112.html>; Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach (Sept. 22, 2015) [hereinafter Press Release, SEC Charges Investment Adviser], <https://www.sec.gov/news/pressrelease/2015-202.html>; Corey Bennett, *SEC Goes After Investment Adviser for Poor Cybersecurity*, THE HILL (Sept. 22, 2015, 4:33 PM), <http://thehill.com/policy/cybersecurity/254554-sec-goes-after-invest-ment-firm-for-poor-cybersecurity>.

17. See David Zaring, *Enforcement Discretion at the SEC*, 94 TEX. L. REV. 1155, 1163–71 (2016) (discussing the controversy surrounding the SEC's recent expanded enforcement powers to heavily pursue administrative, rather than judicial, adjudication); see Jed S. Rackoff, Practicing Law Inst. Sec. Regulation Inst., Keynote Address Is the S.E.C. Becoming a Law unto Itself? (Nov. 5, 2014), <http://assets.law360news.com/0593000/593644/Sec.Reg.Inst.final.pdf> (discussing this “administrative creep” of the SEC and vast expansion of its enforcement powers in recent years).

18. Sarbanes-Oxley Act, 116 Stat. 745; Exchange Act, Pub. L. No. 94-29, §17, 89 Stat. 97 (1975) (codified as amended at 15 U.S.C. § 78u-6 (2012)).

I. WHISTLEBLOWING AND CYBERSECURITY COMPLIANCE

The financial scandals and crises of the twenty-first century have brought the issue of compliance to heightened focus.¹⁹ Effective internal reporting channels that facilitate the receipt of information pertaining to corporate wrongdoing and a prompt management response are some of the most crucial components of a successful compliance program.²⁰ Cybersecurity has been widely recognized as a compliance issue with important ramifications for the general public, the management of which is shaped, to a large degree, by corporate social responsibility principles, effective internal controls, and a corporate culture that promotes the free flow of information.²¹ Since the issuance of the 2011 Guidance, the SEC has consistently advised that cybersecurity breaches and risks are most effectively handled through compliance measures that include increased involvement of compliance officers, periodic internal cybersecurity assessments, routine monitoring and testing of information systems, improved knowledge and oversight by the board of directors, and the implementation of employee policies to detect and report cybersecurity threats.²² Whistleblowers are enormously beneficial in many of these efforts. “Whistleblowers can be the canaries in the mine shaft, providing early warning of imminent disaster.”²³

19. See, e.g., James A. Fanto, *Surveillant and Counselor: A Reorientation in Compliance for Broker-Dealers*, 2014 BYU L. REV. 1121, 1150 (2014) (discussing the growth of compliance obligations as financial sector regulation has grown over the years, especially in light of scandals); Andrew Weissmann & David Newman, *Rethinking Criminal Corporate Liability*, 82 IND. L.J. 411, 442 (2007) (noting the importance of corporate compliance measures in the wake of the Enron collapse and other corporate scandals).

20. See Cynthia Estlund, *Corporate Self-Regulation and the Future of Workplace Governance*, 84 CHI.-KENT. L. REV. 617, 625–26 (2009) (discussing the key role that employees play in self-regulation to ensure compliance and the dangers of employer reprisals in this context).

21. See, e.g., Noah G. Susskind, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573, 576 (2015) (noting “mismanagement” as a contributor to cybersecurity problems); Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board’s Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L. 313, 315–16 (2011) (discussing the role of the board in managing IT-related issues); Danielle Warner, *From Bombs and Bullets to Botnets and Bytes: Cyber War and The Need for A Federal Cybersecurity Agency*, 85 S. CAL. L. REV. POSTSCRIPT 1, 22 (2012) (“[T]ougher regulation of critical infrastructure’s cybersecurity paired with a system of auditing and accountability have the ability to greatly enhance the security of our nation and its networks.”); Emmanuel Olaoye, *Cybersecurity Should be a Compliance Issue*, REUTERS (Aug. 27, 2013), <http://blogs.reuters.com/financial-regulatory-forum/2013/08/27/cybersecurity-should-be-a-compliance-issue-says-expert/>.

22. U.S. SEC. & EXCH. COMM’N, DIVISION INV. MGMT, CYBERSECURITY GUIDANCE (2015), <http://www.sec.gov/investment/im-guidance-2015-02.pdf>; *SEC Releases Cybersecurity Guidance, Highlights Compliance Role*, NAT’L L. REV. (May 1, 2015), <http://www.natlawreview.com/article/sec-releases-cybersecurity-guidance-highlights-compliance-role>.

23. Constance E. Bagley, Mark Roellig & Gianmarco Massameno, *Who Let the Lawyers Out?: Reconstructing the Role of the Chief Legal Officer and the Corporate Client in a Globalizing World*, 18 U. PA. J. BUS. L. 419, 469 (2016) (citing CONSTANCE E. BAGLEY, MANAGERS AND THE LEGAL ENVIRONMENT: STRATEGIES FOR THE 21ST CENTURY 37 (8th ed. 2016) (“Like the birds taken into mines to detect deadly gases, they often perceive dangers before top management.”)).

Despite their contributions, whistleblowers have not traditionally been viewed as key players in modern corporate governance—instead, they are commonly labeled with pejorative titles like “snitch,” “rat,” or “traitor.”²⁴ Although negative perceptions of whistleblowers have started to change in recent years,²⁵ whistleblowers still face an uphill battle and commonly experience retaliation for their efforts, especially among the many organizations that manifest a culture or environment of silence and ignore or punish whistleblowers as dissenters to group consensus.²⁶ There is extensive research to reveal that most whistleblowers opt for internal reporting and will only seek to externally report information when they have been ignored in the past or when internal reporting channels are simply not available or futile.²⁷ As such, an organizational culture of encouraging and responding to whistleblowers and internal reports is of fundamental importance to regulated entities. Not only are internal controls and reporting channels mandated by legislation like SOX,²⁸ they serve as mitigating factors in the Department of Justice’s decision regarding whether to criminally indict a corporation and in sentencing decisions under the Federal Sentencing Guidelines.²⁹ There are

24. See, e.g., Geoffrey Christopher Rapp, *False Claims, Not Securities Fraud: Towards Corporate Governance by Whistleblowers*, 15 NEXUS: CHAPMAN’S J.L. & POL’Y 55, 61 (2010); Vega, *supra* note 3, at 491; see also Frank J. Cavico, *Private Sector Whistleblowing and the Employment-at-Will Doctrine: A Comparative Legal, Ethical, and Pragmatic Analysis*, 45 S. TEX. L. REV. 543, 642 (2004) (each discussing common retaliatory reactions to whistleblowers).

25. Geneva Campbell, *Snitch or Savior? How the Modern Cultural Acceptance of Pharmaceutical Company Employee External Whistleblowing is Reflected in Dodd-Frank and the Affordable Care Act*, 15 U. PA. J. BUS. L. 565, 573–75 (2013) (noting a recent increased sense of accepting whistleblowers); Yuval Feldman & Orly Lobel, *The Incentives Matrix: The Comparative Effectiveness of Rewards, Liabilities, Duties, and Protections for Reporting Illegality*, 88 TEX. L. REV. 1151, 1159 (2010) (noting a shift in perceptions of whistleblowing to be viewed as “a heroic act”).

26. See, e.g., James Fanto, *Whistleblowing and the Public Director: Countering Corporate Inner Circles*, 83 OR. L. REV. 435, 469 (2004) (discussing “organizational silence” in light of groupthink and other social psychological research that reject any internal negative views of the firm); see also Jamie Darin Prekert, Julie Manning Magid & Allison Fetter-Harrott, *Retaliatory Disclosure: When Identifying the Complainant is an Adverse Action*, 91 N.C. L. REV. 889, 933 (2013) (noting that the threat of reprisal to whistleblowers is often the most harsh “when it is combined with the tyranny of the majority”).

27. See, e.g., Orly Lobel, *Citizenship, Organizational Citizenship, and the Laws of Overlapping Obligations*, 97 CALIF. L. REV. 433, 463 (2009) (discussing “empirical research confirm[ing] that whistleblowers indeed prefer internal speech to immediate outside reporting”); Elletta Sangrey Callahan & Terry Morehead Dworkin, *Who Blows the Whistle to the Media, and Why: Organizational Characteristics of Media Whistleblowers*, 32 AM. BUS. L.J. 151, 170–79 (1994) (noting that employees are more likely to externally report when there has been no effective response to their internal disclosure); MARCIA P. MICELI & JANET P. NEAR, *BLOWING THE WHISTLE THE ORGANIZATIONAL AND LEGAL IMPLICATIONS FOR COMPANIES AND EMPLOYEES* 511–15 (1992).

28. See Sarbanes-Oxley Act, Pub. L. No. 107-204, 116 Stat. 745 (2002) (codified as amended at 15 U.S.C. § 7262 (2012)); 7 C.F.R. § 240.13a-15(a) (2016).

29. See U.S. SENTENCING GUIDELINES MANUAL § 8C2.5(f)(1) (U.S. SENTENCING COMM’N 2012); Memorandum from Mark R. Filip, Deputy Att’y Gen., to Heads of Dep’t Components & U.S. Att’ys, Principles of Federal Prosecution of Business Organizations 3–4 (Aug. 28, 2008), <https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf>.

also countless organizational benefits to whistleblowing, including the avoidance of negative press and litigation commonly associated with external reporting, the ability to correct wrongdoing in a timely manner to decrease potential overall harm, an improvement in overall work environment and employee morale, and company commitment to an ethical culture.³⁰

Internal whistleblowing in this context is especially beneficial to reporting companies in that it may help gather the necessary information that is required for compliance with the 2011 Guidance.³¹ The materiality thresholds for such reporting requires information that would influence the decision of a “reasonable investor” in this context—cybersecurity-related problems are likely to negatively affect the company’s stock price, financial posture, or carry other investor risks, and the whistleblower’s discovery and reporting of such information, if substantiated, is likely to help companies become aware of such information when it may otherwise remain undetected.³²

In promoting the goals of the 2011 Guidance, the SEC has consistently called upon senior management, including corporate boards and officers, to play a pronounced and “proactive” role in the detection and prevention of cybersecurity threats by ensuring that the company has proper mechanisms in place to catch such issues before any real threat occurs.³³ In her opening remarks at the 2014 Roundtable, SEC Chair White noted that while the SEC’s formal jurisdiction over cybersecurity is “directly focused on the integrity of our market systems, customer data protection, and disclosure of material information,” every government agency must understand and assess the cybersecurity risks relevant to its respective area of regulation.³⁴ Cybersecurity experts speaking at the Roundtable noted the importance of early detection of cyber threats, which allows companies to more quickly

30. See, e.g., Kevin Rubinstein, *Internal Whistleblowing and Sarbanes-Oxley Section 806: Balancing the Interests of Employee and Employer*, 52 N.Y. L. SCH. L. REV. 637, 650 (2007–2008) (noting that whistleblowing provides many benefits to organizations); Letter from Alexander M. Cutler, Chair, Bus. Roundtable, to Elizabeth M. Murphy, Sec’y, U.S. Sec. & Exch. Comm’n (Dec. 17, 2010), <http://www.sec.gov/comments/s7-33-10/s73310-142.pdf>; Elletta Sangrey Callahan et al., *Integrating Trends in Whistleblowing and Corporate Governance: Promoting Organizational Effectiveness, Societal Responsibility, and Employee Empowerment*, 40 AM. BUS. L.J. 177, 195–96 (2002) (discussing the organizational benefits of internal whistleblowing); Orly Lobel, *Linking Prevention, Detection, and Whistleblowing: Principles for Designing Effective Reporting Systems*, 54 S. TEX. L. REV. 37, 41–42 (2012) (“[A]ttempts to resolve compliance issues should first be made internally.”).

31. Elizabeth C. Tippet, *The Promise of Compelled Whistleblowing: What the Corporate Governance Provisions of Sarbanes-Oxley Mean for Employment Law*, 11 EMP. RTS. & EMP. POL’Y J. 1, 31–33 (2007).

32. *Id.*; see also William H. Simon, *Wrongs of Ignorance and Ambiguity: Lawyer Responsibility for Collective Misconduct*, 22 YALE J. ON REG. 1, 7 (2005) (discussing materiality standards); 17 C.F.R. § 229.601(b) (2016).

33. Ben DiPietro, *The Morning Risk Report: Cybersecurity Responsibility Falling to Boards*, WALL ST. J. (Mar. 4, 2015, 7:29 AM), <http://blogs.wsj.com/riskandcompliance/2015/03/04/the-morning-risk-report-cybersecurity-responsibility-falling-to-boards/>.

34. White Statement, *supra* note 7.

remediate issues before they escalate into more serious and alarming degrees.³⁵ Noting that cyber-threats cannot be completely avoided but must instead be managed and mitigated, the discussants expressed that such responsibilities cannot be “one person’s job” or the job solely of the “tech or IT” employees; instead they called for a “multi-stakeholder effort” within organizations involving the preparation and coordination of all constituents.³⁶ Commentators noted that one of the most significant challenges is the communication of cyber-risks to senior executives and boards of directors and the need to create a “culture” within companies in which cybersecurity issues “start[] at the keyboard . . . with every single employee,” who must themselves be empowered to report any concerns when they are observed.³⁷ To this end, commentators have emphasized the need for boards of directors to ensure that there are clear reporting channels and compliance programs in place for employees to “feel able to report data security issues” and an effective system to investigate and record actions taken in response to reported information.³⁸

It is within this very context that cybersecurity whistleblowers play a key role. Although the connection between the securities laws, cybersecurity, and whistleblowing may not be immediately apparent, the contributions of the latter are directly linked to raising red flags within the company pertaining to cyber-related threats. Important areas of whistleblower disclosures in the cybersecurity arena may include reporting on inadequate risk controls to counter the effects of cyber-threats, the need for increased public company disclosures relating to computer hacking or other cybersecurity-related incidents, suspicious activity occurring among a company’s online systems, and taking caution that cyber-related risks do not remain undetected for extended periods of time.³⁹

35. *Id.*

36. *Id.*

37. *Id.*

38. See, e.g., Thad A. Davis, Michael Li-Ming Wong & Nicola M. Paterson, *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 651 (2015) (discussing the benefits of establishing a “culture of data security compliance”); Lawrence J. Trautman, *The Matrix: The Board’s Responsibility for Director Selection and Recruitment*, 11 FLA. ST. U. BUS. REV. 75, 113–15 (2012) (discussing the role of corporate directors in overseeing cybersecurity and technology-related risks and issues); Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?*, 11 DEPAUL BUS. & COM. L.J. 205, 233 (2013) (proposing that IT experience and expertise should be considered in director recruitment to avoid expensive costs and lawsuits related to cybersecurity issues).

39. See, e.g., Jordan Thomas & Vanessa De Simone, *Cybersecurity - Growing Technological Threats Raise New Issues for Investors and the SEC*, SECWHISTLEBLOWERADVOCATE (May 1, 2014), <http://www.secwhistlebloweradvocate.com/secwhistlebloweradvocate/cybersecurity-growing-technological-threats-raise-new-issues-for-investors-and-the-sec>; Eric Young, *An Important Areas for Whistleblowers*, MCELDREW YOUNG, <http://www.mceldrewyoung.com/whistleblower/sec/cybersecurity/> (last visited Oct. 5, 2016); Igor Volovich, *Cyber Whistleblowing Pivotal in Ensuring Corporate Transparency and Accountability in the IoT Era*, PEERLYST (Sept. 25, 2015), <https://www.peerlyst.com/posts/cyber-whistleblowing-pivotal-in-ensuring-corporate->

Attorneys in the field have called upon SEC-regulated companies to “get serious about protecting customer data” and to be “forthright about potential risks” related to cyber-threats, while also expressing that the “lesson” for would-be whistleblowers is not to assume that any wrongdoing that they observe involving these issues would be outside the realm of the SEC’s regulatory authority.⁴⁰ Two attorneys skilled in retaliation law who have spoken on the issue and have represented whistleblowers reporting in the cybersecurity arena acknowledged that although none of the “highly public ‘mega breaches’” involving cybersecurity have involved a whistleblower, “[i]t is only a matter of time . . . before we see a headline announcing that a hacked company knew about its vulnerabilities yet did nothing to protect its customers, but instead fired the whistleblower who identified and sought to fix the problem.”⁴¹

There have been several recent examples of retaliation against cybersecurity whistleblowers spanning across a wide range of industries, including individuals who themselves work in the cybersecurity arena. In one instance, Richard Wallace, a former investigator at the cybersecurity company Tiversa, blew the whistle on his employer by alleging that the company had invented false data breaches for the purpose of inducing clients to buy the company’s cybersecurity services.⁴² In one particularly egregious instance, Wallace revealed that Tiversa falsely informed LabMD, a cancer testing company, that it had been hacked and then offered it emergency “incident response” cybersecurity services.⁴³ When LabMD refused, Tiversa allegedly threatened to inform federal regulators about the company’s data breach and ultimately informed the FTC of the incident, which brought charges against LabMD, forcing the company to fight the charges in court, ultimately lose, and close down its business.⁴⁴

Another example involved an employee-whistleblower of the investment company Vanguard, who claimed that the company’s password policy was

transparency-and-accountability-in-the-iot-era; Lance Hayden, *What’s Your Cybersecurity Whistleblower Strategy?*, CSO (Jan. 5, 2016 5:31 AM), <http://www.csoonline.com/article/3018853/leadership-management/whats-your-cybersecurity-whistleblower-strategy.html> (offering the example of an employee who reports vulnerabilities about the company’s infrastructure and the increased interest of lawyers in such cases).

40. Thomas & De Simone, *supra* note 39; Young, *supra* note 39; *see generally* *SEC Disclosure and Corporate Governance*, WEIL, GOTSHAL & MANGES LLP (Jan. 23, 2015), http://www.weil.com/~media/files/pdfs/pcag_sec_discl_alert_jan_2015.pdf.

41. Debra Katz & Alexis H. Ronickher, *Ignoring Issues Raised by Cybersecurity Whistleblowers Only Compounds the Problem*, KATZ, MARSHALL & BANKS (Sept. 11, 2015), <http://www.kmblegal.com/publications/ignoring-issues-raised-cybersecurity-whistleblowers-only-compounds-problem>.

42. Jose Pagliery, *Whistleblower Accuses Cybersecurity Company of Extorting Clients*, CNN MONEY (May 7, 2015, 2:32 PM), <http://money.cnn.com/2015/05/07/technology/tiversa-labmd-ftc/>; Cale Guthrie Weissman, *A Cybersecurity Firm is Being Accused of Extorting Clients*, BUS. INSIDER (May 7, 2015, 6:02 PM), <http://www.businessinsider.com/a-whistleblower-claims-that-cybersecurity-firm-tiversa-fakes-hacks-to-get-companies-to-pay-for-services-2015-5>.

43. *See id.*

44. *See* Pagliery, *supra* note 42.

too weak to withstand susceptibility to cyber-attacks.⁴⁵ This whistleblower internally revealed that she and clients of the company were able to successfully log into online accounts despite typographical errors in providing security password answers.⁴⁶ The whistleblower, a client relationship manager, had received complaints from angry customers about this problem and, for two years, flagged this issue to upper management as a major cybersecurity concern for the company's twenty million customers. The manager also communicated an additional security issue pertaining to the voice verification system.⁴⁷ Her reports were futile—she never received a formal response from management and was told “to stop complaining,” which prompted her to file whistleblower tips directly with the SEC and the Financial Industry Regulatory Authority (FINRA), which both investigated her concerns.⁴⁸ Subsequent to her revelations, she was fired for being in “violation of Vanguard's Professional Conduct Policy,”⁴⁹ thus providing an example of what appears to be a clear case of retaliation.

Other examples of whistleblowers reporting on cybersecurity-related issues include a tip that led to charges by the Department of Health and Human Services against a hospital for improperly storing protected health information electronically,⁵⁰ and a case of alleged retaliation against a whistleblower who disclosed security violations at a U.S. Department of Veterans Affairs regional office that included unauthorized access and use of data and information systems, the falsification of security reports, and the sharing of passwords.⁵¹

Another related subset of whistleblowing involves cybersecurity professionals, including information-security researchers or technicians, who assess and expose vulnerabilities or flaws in the information systems of companies and act as “fact-checkers” of information technology.⁵² These professionals commonly act as cybersecurity consultants and many are hired by public companies and government agencies to ensure the safety of internal

45. Clayton Browne, *Does Low-Cost Vanguard Have Low-Cost (& Quality) Cyber Security?*, VALUEWALK (Aug. 11, 2015, 10:11 AM), <http://www.valuwalk.com/2015/08/vanguard-cyber-security/>; Susan Antilla, *Is Vanguard Making It Too Easy for Cybercriminals to Access Your Account?*, THESTREET (Aug. 10, 2015, 12:27 PM), <http://www.thestreet.com/story/13213265/1/is-vanguard-making-it-too-easy-for-cybercriminals-to-access-your-account.html>.

46. See Browne, *supra* note 45.

47. Antilla, *supra* note 45.

48. *Id.*

49. Susan Antilla, *Vanguard Group Fires Whistleblower Who Told TheStreet About Flaws in Customer Security*, THESTREET (Sept. 18, 2015, 12:20 PM), <https://www.thestreet.com/story/13293245/1/vanguard-group-fires-whistleblower-who-told-thestreet-about-flaws-in-customer-security.html>.

50. Mark Mermelstein, *The Rise of the Cybersecurity Whistleblower*, ORRICK (Oct. 1, 2015), <https://www.orricks.com/Insights/2015/10/The-Rise-of-the-Cybersecurity-Whistleblower>.

51. *Daniels v. Dep't. of Veteran Affairs*, 276 F. App'x 1002, 1002–04 (Fed. Cir. 2008).

52. Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 821 (2013).

information systems.⁵³ Otherwise known as “white hat hackers” or “ethical hackers,” such persons are employed to find security holes with the permission of the owner, without exploiting them, which is conducted through mechanisms such as penetration testing, vulnerability assessments, and the testing of in-place security systems.⁵⁴ One famous example of a “white hat hacker” attempting to help a company address a security problem is Michael Lynn, an experienced security researcher for the firm Internet Security Systems Inc., who followed protocol by probing for flaws in computer hardware and software with the intent of discovering security issues.⁵⁵ Lynn discovered one such flaw at Cisco Systems Inc.—a way to crack open the company’s operating system on its internet routers, which posed a huge infrastructure risk.⁵⁶ After Lynn reported the problem to Cisco, the company issued a patch to correct it, but, concerned about “damaging the invincible image of its products,” it refused to alert customers to the problem, thereby placing their personal information at risk.⁵⁷ Lynn, concerned about the lack of public disclosure of this problem, prepared a presentation for the Black Hat hacker conference in Las Vegas that would describe the details of the particular bug.⁵⁸ Cisco fiercely objected, citing violations of intellectual property law, and obtained a restraining order preventing Lynn from presenting his information.⁵⁹ Lynn gave his presentation regardless and, at least as of 2012, was employed by a competitor of Cisco as a senior engineer.⁶⁰

Depending on their employment situation, cybersecurity researchers like Lynn have increasingly identified themselves as whistleblowers for being in possession of valuable information that is not likely to be discovered by anyone else.⁶¹ When the owner of the system fails to take action to address or remedy the security issue, cybersecurity researchers are often viewed as whistleblowers for “alerting the world to unsafe business practices,” “breaking important news on topics of public interest,” and “engaging in scientific or academic commentary.”⁶² The revelation of such information,

53. Nadia Kovacs, *What is the Difference Between Black, White, and Grey Hat Hackers?*, SYMANTEC NORTON CMTY (Aug. 11, 2015, 8:50 AM), <http://community.norton.com/en/blogs/norton-protection-blog/what-difference-between-black-white-and-grey-hat-hackers>.

54. *Id.*

55. Derek E. Bambauer & Oliver Day, *The Hacker’s Aegis*, 60 EMORY L.J. 1051, 1053–54 (2011).

56. *Id.* at 1053.

57. *Id.*

58. *Id.*

59. *Id.* (Cisco also “forced conference organizers to rip the printed version of Lynn’s slides out of the conference materials, and to turn over CDs containing a copy of his slideshow.”)

60. Jordan Robertson, *Famous Hackers: Then and Now*, BLOOMBERG BUS. (Apr. 19, 2012), <http://www.bloomberg.com/slideshow/2012-04-18/famous-hackers-then-and-now.html#slide7>.

61. Matwyshyn, *supra* note 52, at 829. The scarcity of the information that these types of whistleblowers possess is precisely what makes it so valuable. *See also id.* at 822 n.133 (noting that a “metaphor for information security researchers might be one of whistleblowers”).

62. *Id.* at 829.

due to its sensitive and proprietary nature, which may also include trade secrets, is likely to expose whistleblowers not only to retaliation at work, but also to a risk of criminal prosecution or civil suits.⁶³

II. PROTECTING CYBERSECURITY WHISTLEBLOWERS

A. THE ABSENCE OF RETALIATION PROTECTIONS FOR CYBERSECURITY WHISTLEBLOWERS

Information is key to mitigating the effects of cybersecurity breaches and whistleblowers stand to play a crucial role in discovering and reporting information to effectively manage the problem. As discussed, despite recent trends in society viewing whistleblowers in a more positive light,⁶⁴ they still commonly experience negative reactions for the information they have brought forward.⁶⁵ Reactions to cybersecurity whistleblowers have been no different.⁶⁶ It is believed that the reason cybersecurity whistleblowers face employer resistance is due to senior management's immense difficulty handling cybersecurity vulnerabilities and the constant evolution of such threats.⁶⁷ For example, executives who are accustomed to long-standing cybersecurity systems may not wish to consider or address the new challenges that the whistleblower has reported and may feel that the costs of doing so are too great in the interim and may compromise current business practices or opportunities.⁶⁸ As noted previously, employer concerns may also center on the repercussions for exposed intellectual property or other trade secrets. However, ignoring cybersecurity whistleblowers is detrimental to employers and regulated entities, especially in light of the 2011 Guidance's requirements.

The 2011 Guidance was prompted by a letter to former SEC Chair Mary Schapiro from former Senator John D. Rockefeller and four other members of Congress urging the SEC, in light of the several recent cyber-attacks on well-known public companies, to develop guidelines explaining a company's duty to publicly disclose information in this arena.⁶⁹ The SEC's Division of

63. *See id.*

64. *See* Feldman & Lobel, *supra* note 25, at 1159 (describing a shift in perception of whistleblowers).

65. *See generally* ETHIC RES. CTR., NATIONAL BUSINESS ETHICS SURVEY OF THE U.S. WORKFORCE 13 (2013), <https://www.ibe.org.uk/userassets/surveys/nbes2013.pdf> (describing retaliation as a widespread problem); *see generally* Stephen Kohn, *Retaliation against Whistleblowers at All-Time High*, WHISTLEBLOWERS LEGAL PROTECTION BLOG (Dec. 10, 2014), <http://www.whistleblowersblog.org/2014/12/articles/false-claims/retaliation-against-whistleblowers-at-all-time-high/>.

66. *See* Katz & Ronickher, *supra* note 41; *see supra* Part I.

67. *See* Katz & Ronickher, *supra* note 41.

68. *See id.*

69. *See* Letter from John D. Rockefeller IV, Chairman, U.S. Senate Comm'n on Commerce, Sci. & Transp. et al., to Mary Schapiro, Chair, U.S. Sec. & Exch. Comm'n (May 11, 2011);

Corporate Finance then issued the 2011 Guidance in light of the market's "increasing dependence" on technology.⁷⁰ In this vein, the 2011 Guidance attempts to alert public companies to the various disclosure obligations that are already in existence under SEC regulations that, although do not "explicitly refer[] to cybersecurity risks and cyber incidents," would prompt reporting companies to "discuss" such concerns in their public filings as material information for investors.⁷¹ The SEC focused on existing reporting requirements that "may impose an obligation" on registrants to also disclose cybersecurity information.⁷² These existing requirements are mostly codified in various items of Regulation S-K, which prompt ongoing disclosures under the Securities Act of 1933 and the Securities Exchange Act of 1934 (Exchange Act) for public company issuers of securities, registrants, and filers.⁷³ Specifically, the SEC invoked the following items of Regulation S-K as being relevant to the disclosure of cybersecurity risks: Items 101 (Description of Business), 103 (Legal Proceedings), 303 (Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)), 307 (Disclosure Controls and Procedures), and 503 (Risk Factors).⁷⁴

One of the most significant problems with the 2011 Guidance is that it lacks the force of law of a binding SEC regulation. The non-binding nature of the 2011 Guidance is explicit in that it begins with the qualification that "[t]his guidance is not a rule, regulation, or statement of the Securities and Exchange Commission" and "the Commission has neither approved nor disapproved its content."⁷⁵ As such, a gray area has emerged with respect to whether cybersecurity whistleblowers are eligible for the robust retaliation protections under the federal securities laws, specifically under the whistleblower programs of SOX and Dodd-Frank. Under Section 806 of SOX, which was enacted in 2002, employees of publicly-traded companies blowing the whistle on reasonably believed violations of the federal securities laws are protected from retaliation if they report such information either i) internally to someone with supervisory authority over them or ii) externally to a federal regulatory or law enforcement agency or member or committee of Congress.⁷⁶ To exercise this right, an aggrieved whistleblower must undergo the administrative remedy of filing a complaint before the Secretary of Labor within 180 days of the alleged retaliation, and, if substantiated, may

Norah C. Avellan, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 206–07 (2014).

70. See *CF-2 Disclosure Guidance*, *supra* note 8, at 2.

71. *Id.* at 2.

72. *Id.*

73. See 17 C.F.R. §§ 229.101–702 (2016).

74. See *id.*; see also 17 C.F.R. §§ 229.101, 229.103, 229.303, 229.307, 229.503(c).

75. See *CF-2 Disclosure Guidance*, *supra* note 8, at supplementary information.

76. Sarbanes-Oxley Act, Pub. L. No. 107-204, 116 Stat. 745 (2002) (codified as amended at 18 U.S.C. § 1514A(a) (2012)).

obtain compensatory damages consisting of reinstatement of employment, back pay with interest, and litigation and attorneys' fees.⁷⁷ As discussed, in 2010, Congress enacted Dodd-Frank, which established a solid whistleblower program providing stronger retaliation protections than SOX and a generous bounty reward program to incentivize whistleblowing.⁷⁸

Although the statutory language of the SOX and Dodd-Frank programs is not identical, both statutes protect whistleblowers who provide information that they reasonably believe involves possible violations of the federal securities laws, rules, or regulations under the SEC's jurisdiction.⁷⁹ SOX protects whistleblower disclosures reasonably believed to "constitute[] a violation of section 1341, 1343, 1344, or 1348, *any rule or regulation of the Securities and Exchange Commission*, or any provision of Federal law relating to fraud against shareholders" when the whistleblower reports such information either externally or internally.⁸⁰ The protected activity enumerated in the language of SOX sections 1341, 1343, 1344, and 1348 consists of mail fraud, wire fraud, banking fraud, and securities fraud, respectively.⁸¹ Similarly, Dodd-Frank, which protects whistleblowers from retaliation, regardless of whether they are eligible for a bounty award,⁸² includes the following categories as protected activity under subsection (h) thereof: i) providing information to the SEC; ii) initiating, testifying, or assisting in any investigation, judicial, or administrative action of the SEC; or iii) making disclosures "that are required or protected under [SOX, the Securities Exchange Act of 1934, 18 U.S.C. § 1513(e) (retaliating against a witness, victim, or informant)] and any other *law, rule, or regulation subject to the jurisdiction of the [SEC]*."⁸³

77. 18 U.S.C. §§ 1514A(b), 1514A(c). If the Secretary of Labor has not issued a final decision within 180 days of the filing of the complaint and there is no evidence that the delay is due to bad faith of the whistleblower, then the whistleblower may bring an action in federal district court. *Id.*

78. Exchange Act, Pub. L. No. 94-29, § 17, 89 Stat. 97, (1975) (codified as amended at 15 U.S.C. § 78u-6(b) (2012)); *see also* Geoffrey C. Rapp, *Four Signal Moments in Whistleblower Law: 1983-2013*, 30 HOFSTRA LAB. & EMP. L.J. 389, 400 (2013) (discussing the incentives that Dodd-Frank creates for whistleblowers).

79. *See* 18 U.S.C. § 1514A; 15 U.S.C. § 78u-6(h); *see also* 17 C.F.R. § 240.21F-2 (2016).

80. 18 U.S.C. § 1514A(a) (emphasis added).

81. *Id.* (as set forth above, the language of SOX references the various statutory citations of these types of fraud, which, for i, ii, iii, and iv. listed above are 18 U.S.C. §§ 1341, 1343, 1344, or 1348, respectively).

82. *See* 17 C.F.R. § 240.21F-2. To be eligible for a bounty award, whistleblowers must ensure that they provide "original information" leading to a successful SEC enforcement action resulting in monetary sanctions of at least \$1,000,000. *See* 15 U.S.C. §§ 78u-6(a), 78u-6 (b).

83. 15 U.S.C. § 78u-6(h) (emphasis added). There is a current division in the courts as to whether, under Dodd-Frank, a whistleblower who reports only internally and not externally to the SEC or another federal agency, is eligible for retaliation protection under *the statute due* to the definition of whistleblower in the statute as individuals who "provide information . . . to the [SEC]." *Id.* § 78u-6(a)(6); *see generally* Jennifer M. Pacella, *Inside or Out? The Dodd-Frank Whistleblower Program's Antiretaliation Protections for Internal Reporting*, 86 TEMP. L. REV. 721 (2014) (discussing the division of courts in this arena).

Against this backdrop, it is likely that whistleblower disclosures relating to an employer's perceived violations of the SEC's 2011 Guidance are not included among the various types of protected activity captured by the two statutes; as such, violating the 2011 Guidance would neither constitute a violation of the laws enumerated within SOX or Dodd-Frank nor a duly-authorized SEC law, rule, or regulation. Thus, employees who are contemplating blowing the whistle in this arena cannot be assured that they are protected in the event of reprisal for their reporting. As discussed earlier, management's response to a cybersecurity whistleblower may not be positive, as revelation of cybersecurity vulnerabilities will often result in higher costs for the entity, an unwillingness to alter long-standing cybersecurity systems, concern over compromised intellectual property, or a lack of understanding as to the complexity of the issues.⁸⁴

Specifically relating to retaliation protections under SOX, empirical studies have revealed that when whistleblowers are unsuccessful in obtaining relief under the statute, one of the most common reasons is due to a failure to categorize the whistleblower's disclosure as "protected activity" as defined.⁸⁵ Such studies have revealed that in cases in which OSHA and Administrative Law Judges (ALJs) (on appeal) have decided in favor of employers, the reason has been due to whistleblowers reporting on information in "other" fraud categories, general fraud, or accounting irregularities that did not fit squarely within one of the six clearly enumerated categories of protection under SOX.⁸⁶ As such, OSHA and ALJs have conveyed a narrow interpretation of what constitutes protected activity under the statute that requires the whistleblower to directly link his or her disclosure to specific instances of shareholder fraud.⁸⁷ In the same vein, cybersecurity whistleblowers that report concerns are likely to find that their disclosures do not fall within the enumerated categories eligible for retaliation protections.

Similarly, under Dodd-Frank, the definition of "whistleblower" mandates that the individual provide "information relating to a violation of the securities laws to the [SEC], in a manner established, by rule or regulation, by the [SEC]."⁸⁸ Beyond the face of the statute itself, the SEC regulations interpreting Dodd-Frank, as well as federal courts that have examined the issue, have all made clear that a whistleblower must report on

84. See *infra* Part IIB.

85. See Richard Moberly, *Unfulfilled Expectations: An Empirical Analysis of Why Sarbanes-Oxley's Whistleblowers Rarely Win*, 49 WM. & MARY L. REV. 65, 113–15 (2007) (conducting an empirical study revealing the lack of success of whistleblowers under SOX); Richard Moberly, *Sarbanes-Oxley's Whistleblower Provisions: Ten Years Later*, 64 S.C. L. REV. 1, 10 (2012) (discussing the continued lack of success years later); see generally Beverley H. Earle & Gerald A. Madek, *The Mirage of Whistleblower Protection Under Sarbanes-Oxley: A Proposal for Change*, 44 AM. BUS. L.J. 1 (2007) (discussing the shortcomings of the SOX whistleblower program).

86. Moberly, *supra* note 85, at 116–18 (explaining the various hurdles that whistleblowers have faced in claiming that they engaged in "protected activity").

87. See *id.*

88. 15 U.S.C. § 78u-6(a)(6) (emphasis added).

an explicit violation of the federal securities laws to be protected from retaliation.⁸⁹ The SEC regulations implementing Dodd-Frank state that the statutory definition of “whistleblower” clarifies that the [whistleblower] submission must relate to a violation of the *Federal securities laws*, or a rule or regulation promulgated by the [SEC],” thus specifically excluding retaliation protections for whistleblowers who report on a state or foreign law violation.⁹⁰ The term “securities laws” also very clearly includes only the following statutes: the Securities Act of 1933, the Securities Exchange Act of 1934, the Sarbanes-Oxley Act of 2002, the Trust Indenture Act of 1939, the Investment Company Act of 1940, the Investment Advisers Act of 1940, and the Securities Investor Protection Act of 1970.⁹¹

Given the takeaways of the 2014 Roundtable calling for all employees to be actively involved in reporting cyber-related concerns, the need to protect whistleblowers in this arena is crucial. The transformation of the 2011 Guidance into binding SEC regulations as they relate to cybersecurity would solicit feedback from important players in the industry through an official notice and comment rulemaking period, create stronger incentives for companies to adhere to the reporting requirements, and justify the SEC’s imposition of sanctions or threatened enforcement actions.⁹² Such an action would also have the effect of including cybersecurity-related disclosures as a clear and enumerated category of protected whistleblower activity under both SOX and Dodd-Frank.

B. JUDICIAL INTERPRETATIONS

Judicial decisions interpreting the extent to which whistleblowers are protected under the federal securities laws do not guarantee retaliation protections for cybersecurity whistleblowers. Since SOX provides only an administrative remedy for retaliation, the federal cases shedding light in this area have all interpreted Dodd-Frank. Many such cases have emphasized that

89. *See id.* Securities Whistleblower Incentives and Protections, 76 Fed. Reg. 34,300, 34,300 (June 13, 2011) (codified at 17 C.F.R. pts. 240, 249); Caroline E. Keen, *Clarifying What Is “Clear”*: *Reconsidering Whistleblower Protections Under Dodd-Frank*, 19 N.C. BANKING INST. 215, 219 n.43 (2015).

90. Securities Whistleblower Incentives and Protections, 76 Fed. Reg. at 34,302–03 (emphasis added).

91. Exchange Act, Pub. L. No. 94-29, 89 Stat 97 (1975) (codified as amended at 15 U.S.C. § 78c (2012)) (as stated in Section 3(a)(47) of the Securities Exchange Act of 1934).

92. *See, e.g.,* Matthew Ferraro, “*Groundbreaking or Broken?*” *An Analysis of SEC Cybersecurity Disclosure Guidance, its Effectiveness, and Implications*, 77 ALB. L. REV. 297, 340–41 (2014) (proposing that a note and comment period prior to the issuance of binding SEC cybersecurity regulations would “promote fact-finding that could inform the policy” and “promote acceptability” among entities subject to the regulations); Sam Young, *Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches*, 38 J. CORP. L. 659, 676–77 (2013) (noting that adoption of binding, formal rules would create affirmative legal obligations for regulated companies); Avellan, *supra* note 69, at 222–24 (noting that various benefits that regulated entities would derive from binding regulations).

whistleblowers seeking protection under Dodd-Frank must have reported on an “explicit” violation of the federal securities laws.⁹³ In the absence of establishing this type of reporting, whistleblower-plaintiffs have often not been successful in moving past the motion to dismiss stage.

One of the most illustrative cases to date as to how a cybersecurity whistleblower is likely to fare is the U.S. District Court for the Southern District of New York’s decision in *Egan v. TradingScreen, Inc.*⁹⁴ In this case, whistleblower Patrick Egan internally reported that the CEO of the company for which he worked, TradingScreen, Inc., was diverting the company’s corporate assets to another competitor company that the CEO solely owned.⁹⁵ Egan was later fired for his allegations and sought relief under Dodd-Frank for retaliation, to which the company and CEO responded with a motion to dismiss.⁹⁶ One of the most telling aspects of this case is the court’s consideration of Egan’s argument that he disclosed the CEO’s alleged violations of rules promulgated by FINRA, which would arguably fall under Dodd-Frank’s protection of disclosures “subject to the jurisdiction of the [SEC].”⁹⁷ Egan alleged that the CEO had violated FINRA Rule 2010 by misappropriating confidential client information of the company and FINRA Rule 3270 by failing to report his position at the competitor company to TradingScreen Inc.’s board of directors.⁹⁸

The court was clear in rejecting this argument on the basis that Dodd-Frank does not protect whistleblower disclosures that reveal violations of just “any” laws or regulations subject to the SEC’s jurisdiction, but rather protects only “disclosures that are *required or protected* under . . . any other law, rule, or regulation subject to the jurisdiction of the [SEC].”⁹⁹ In this case, the FINRA rules in question did not impose an explicit “duty to disclose,” as Rule 2010 contains only a “general obligation to ‘observe high standards of commercial honor and just and equitable principles of trade,’” while Rule 3270 imposes a duty to disclose on employees of FINRA member firms who receive compensation from business activities outside the scope of their relationship with the member firm, thus not being applicable to the CEO of

93. *See, e.g.*, *Genberg v. Porter*, 935 F. Supp. 2d 1094, 1106 (D. Colo. 2013) (noting that “the plain language” of Dodd-Frank “mandates that in order to qualify as a whistleblower, one must provide information to the SEC regarding an alleged federal securities law violation.”); *Wagner v. Bank of Am. Corp.*, No. 12-cv-00381-RBJ, 2013 WL 3786643, at *7–8 (D. Colo. July 19, 2013), *aff’d*, 571 F. App’x 698 (10th Cir. 2014) (finding that a whistleblower’s report was not protected under the statute); *Nollner v. S. Baptist Convention, Inc.*, 852 F. Supp. 2d 986, 994 (M.D. Tenn. 2012).

94. *Egan v. TradingScreen, Inc.*, No. 10 Civ. 8202(LBS), 2011 WL 1672066, at *6 (S.D.N.Y. May 4, 2011).

95. *Id.* at *2.

96. *Id.*

97. *Id.* at *6–7 (citing 15 U.S.C. § 78u–6(h)(1)(A)(iii) (2012)).

98. *Id.* at *6 (citing FINRA MANUAL RULES 2010, 3270).

99. *Id.* (emphasis added).

TradingScreen, Inc.¹⁰⁰ The court went on to state that “[m]erely alleging the violation of a law or rule under the SEC’s purview is not enough; a plaintiff *must allege that a law or rule in the SEC’s jurisdiction explicitly requires or protects disclosure of that violation.*”¹⁰¹ In this way, the court declared that Dodd-Frank does not protect whistleblowers who report violations of SEC laws or regulations that do not impose a duty to disclose, thus barring Egan from relief. This case takes the law one step further by requiring whistleblowers to report on violations involving mandatory duties to disclose, rather than simply general violations of the law. Subsequent cases have relied on *Egan* and have adopted this same reasoning.¹⁰²

Based on this logic, the non-binding nature of the 2011 Guidance makes it unlikely that a whistleblower could claim that it mandates an explicit duty to disclose. Rather than invoking a clear duty to disclose cybersecurity information, the 2011 Guidance states that its goal is to “provide guidance that *assists registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant’s specific facts and circumstances.*”¹⁰³ The 2011 Guidance makes specific reference to the fact that, although “no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents,” reporting companies should be mindful of whether their current disclosures relating to cybersecurity are adequate in light of the federal securities laws.¹⁰⁴ This language leaves much discretion to a reporting company to decide whether a cybersecurity report is warranted based on the materiality threshold. Given the discretionary decisions that must be made before it is determined whether such a disclosure is necessary, cybersecurity whistleblowers are likely to face obstacles in relying solely on believed violations of the 2011 Guidance as support for their retaliation protections under Dodd-Frank.

Additional cases interpreting Dodd-Frank have been similarly restrictive. In 2012, the U.S. District Court for the Middle District of Tennessee held that the retaliation protections of Dodd-Frank “extend only to any ‘law, rule, or regulation subject to the jurisdiction of the Commission,’” thus only protecting employees from retaliation “if the federal violation falls within the SEC’s jurisdiction.”¹⁰⁵ In *Nollner v. Southern Baptist Convention, Inc.*, two

100. *Id.* (internal citations omitted).

101. *Id.* (emphasis added).

102. *See* *Nollner v. S. Baptist Convention, Inc.*, 852 F. Supp. 2d 986, 994 (M.D. Tenn. 2012) (“[A]nti-retaliation provision part (iii) only protects disclosures that are ‘required or protected’ by laws, rules, or regulations within the SEC’s jurisdiction. Thus, an employee is not protected from retaliation if the disclosure at issue—even if relates to an actual legal violation by the employer—concerns a disclosure that is not ‘required’ or otherwise ‘protected’ by a law, rule, regulation within the SEC’s jurisdiction.”); *Asadi v. G.E. Energy (USA), LLC*, No. 4:12-345, 2012 WL 2522599, at *6 (S.D. Tex. June 28, 2012), *aff’d*, 720 F.3d 620 (5th Cir. 2013) (relying on *Egan* for the same interpretation).

103. *CF-2 Disclosure Guidance*, *supra* note 8 (emphasis added).

104. *Id.*

105. *Nollner*, 852 F. Supp 2d at 994.

individuals who had blown the whistle on suspected violations of the Foreign Corrupt Practices Act (FCPA) were not eligible for retaliation protection under Dodd-Frank because their disclosures did not fall within the jurisdiction of the SEC.¹⁰⁶ The court explained that the FCPA violations apply only to “issuers” of securities (defined as companies registered under the Exchange Act or required to file reports with the SEC thereunder) and “domestic concerns” (defined as citizens, nationals, or residents of the United States).¹⁰⁷ The court went on to explain that the SEC has jurisdiction only over FCPA violations by “issuers,” while the Department of Justice has jurisdiction over domestic concerns and other non-issuers who commit FCPA violations.¹⁰⁸ Because the defendants in this case were domestic concerns and not issuers, the court straightforwardly found that the disclosures would not constitute “protected activity” under Dodd-Frank, thereby barring the whistleblowers from moving forward with their case to seek relief.¹⁰⁹

In a case before the U.S. District Court for the Eastern District of Wisconsin, Nicholas Zillges, the president and CEO of a bank, blew the whistle to the bank’s board of directors, the FTC, and the Federal Deposit Insurance Corporation (FDIC) on conduct that he had observed violating the federal banking laws.¹¹⁰ After being terminated for these reports, Zillges sued his former employer for retaliation under Dodd-Frank. He was denied relief after the court determined that Zillges did not meet the statutory definition of “whistleblower,” because his disclosure did not relate to a “violation of the securities laws.”¹¹¹ Zillges argued that his disclosure fell within the third category of protected activity under the Dodd-Frank whistleblower program, subsection (h), which protects “disclosures that are required or protected under [SOX] . . . including . . . section 1513 (e) of title 18.”¹¹² Section 1513(e) of Title 18 criminalizes interference with a person’s employment when such person provides information to a law enforcement officer about the commission or possible commission of a federal offense.¹¹³ Zillges alleged that he was retaliated against under Section 1513(e) for making a disclosure to law enforcement officers of the FTC and FDIC about the defendant’s possible violation of certain banking laws.¹¹⁴ The court reasoned that because the banking laws that Zillges reported on are not “securities laws,” which are specifically defined to include only the Securities Act of 1933, the Securities Exchange Act of 1934, the Sarbanes-Oxley Act of 2002, the Investment

106. *Id.*

107. *Id.* at 996 (citing 15 U.S.C. §§ 78dd-1(a), 78dd-2(a) (2012)).

108. *Id.*

109. *Id.*

110. *Zillges v. Kenney Bank & Tr.*, 24 F. Supp. 3d 795, 797 (E.D. Wis. 2014).

111. *Id.* at 801.

112. *Id.*; 15 U.S.C. § 78u-6(h)(1)(A)(iii).

113. *Zillges*, 24 F. Supp. 3d at 801; *see also* 15 U.S.C. § 78u-6(h)(1)(A)(iii); Sarbanes-Oxley Act, Pub. L. No. 107-204, 116 Stat. 745 (2002) (codified as amended at 18 U.S.C. § 1513(e) (2012)).

114. *See Zillges*, 24 F. Supp. 3d at 801.

Company Act of 1940, the Investment Advisers Act of 1940, and the Securities Investor Protection Act of 1970,¹¹⁵ Zillges could not avail himself of Dodd-Frank's whistleblower protections and was excluded from retaliation protection under the statute.

Since the 2011 Guidance cannot be described as an SEC rule, law, or regulation that is specifically subject to the agency's jurisdiction, employers are likely to be successful on their motions to dismiss against cybersecurity whistleblowers who sue them for retaliation. Until the SEC promulgates actual regulations in this arena, cybersecurity whistleblowers are likely to face an uphill battle in arguing that they should be subject to retaliation protections under the federal securities laws. Importantly, given that retaliation protections are not guaranteed, cybersecurity whistleblowers are likely to be dissuaded from making reports in the first instance, which would have a negative overall effect on building the type of corporate culture and free-flowing information channels that are necessary to effectively manage cybersecurity threats.

The risk for companies that ignore or silence cybersecurity whistleblowers is that such individuals, perceiving that their employers do not value their reports, will likely opt to externally report to the SEC, especially in light of the bounty incentives that are available for whistleblowers under Dodd-Frank.¹¹⁶ The Dodd-Frank whistleblower bounty program is notable in that the SEC is obligated to pay whistleblowers between 10% and 30% of the total monetary sanctions collected in a successful enforcement of a covered judicial or administrative action, or related action.¹¹⁷ "Covered judicial or administrative action" is defined as any "judicial or administrative action brought by the [SEC] under the securities laws that results in monetary sanctions exceeding \$1,000,000."¹¹⁸ In determining the appropriate percentage of the bounty award, the SEC will consider factors such as the significance of the whistleblower's tip to the success of the action and the degree of assistance the whistleblower has offered.¹¹⁹

Whistleblowers are eligible for bounties even if they are not ultimately successful on a retaliation claim.¹²⁰ The goal of Dodd-Frank's bounty program is to offset the costs that whistleblowers usually suffer for their reports, given the lasting effect of retaliation on their careers and livelihoods.¹²¹ To date, the Dodd-Frank bounty program has been enormously successful, resulting in millions of dollars in total payouts to

115. Exchange Act, Pub. L. No. 94-29, 89 Stat. 97 (1975) (codified as amended at 15 U.S.C. § 78c (2012)).

116. Katz & Ronickher, *supra* note 41; *see also* 15 U.S.C. §§ 78u-6(b), 78u-6(c).

117. *See* 15 U.S.C. § 78u-6(b).

118. *See id.* § 78u-6(a).

119. *Id.*

120. *See id.* § 78u-6(b).

121. S. REP. NO. 111-176, at 111 (2010).

numerous whistleblowers who have provided the SEC with successful tips.¹²² This program is further evidence of the SEC's increasing reliance on whistleblower tips to effectively govern the securities markets—a regulatory goal that the agency feels must respond to the “global threat” of cybersecurity.¹²³

III. SEC INVOLVEMENT IN CYBERSECURITY

A. SHAREHOLDER IMPACT AND THE SEC

Instances of cyber-attacks or data breaches seem to appear in the news on a near daily basis, posing a serious threat to both consumers and shareholders. One of the most notable breaches in recent years involved Target Corporation, where hackers stole credit and debit card information from forty million of the store's customers in 2013. It was not until a year later that the full effects of this breach were known, when the retailer revealed that additional personal information, including email and mailing addresses, had been stolen from between seventy and one hundred million people.¹²⁴ The financial effects of this particular breach were tremendous, as the company's gross total costs are believed to have reached \$191 million,¹²⁵ prompting the need for more than a hundred million customers to obtain new cards and closely monitor against fraud and identity theft.¹²⁶ In 2014, similar data breaches resulting in financial losses occurred at several other well-known companies, including Neiman Marcus, Michael's craft chain, P.F. Chang's Bistro, UPS, Dairy Queen, Home Depot, Staples, and Sony.¹²⁷ The year 2015 was no different—by mid-year, there had been an increase of about

122. Press Release, SEC Issues \$17 Million Whistleblower Award (June 9, 2016), <https://www.sec.gov/news/pressrelease/2016-114.html>.

123. See White Statement, *supra* note 7 (noting that cyber threats “are of extraordinary and long-term seriousness” and “pose non-discriminating risks” to the financial markets). Interestingly, some companies have provided their own types of bounties, through “bug bounty programs” to pay “[white hat and ethical] hackers” to make the discovery of security flaws even more likely so that companies can properly manage such risks. See, e.g., Susskind, *supra* note 21, at 629–33; Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. REV. 383, 397 (2014); Douglas A. Barnes, *Deworming the Internet*, 83 TEX. L. REV. 279, 323 (2004). Such practices are not dissimilar to statutory whistleblower bounty programs that have recognized the necessity of whistleblowers and the value they provide in reporting otherwise unknown information to protect the public interest. See Susskind, *supra* note 21, at 633 (noting that “[t]he reason we already reward whistleblowers, confidential informants, and witnesses—despite moral squeamishness—is necessity”).

124. Hiroko Tabuchi, *\$10 Million Settlement in Target Data Breach Gets Preliminary Approval*, N.Y. TIMES (Mar. 19, 2015), http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0.

125. Brian Prince, *Target Data Breach Tally Hits \$162 Million in Net Costs*, SECURITY WEEK (Feb. 26, 2015), <http://www.securityweek.com/target-data-breach-tally-hits-162-million-net-costs> (noting that this amount was partially offset by an insurance receivable in 2014 of \$46 million).

126. Susskind, *supra* note 21, at 576.

127. Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES (Jan. 13, 2015, 7:06 PM), <http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/>.

85% in the number of breaches in the banking and financial arenas compared to the prior year, and significant data breaches among the following sectors: Business (40.3%), Medical/Healthcare (35%), Banking/Credit/Financial (10%), Educational (7.7%), and Government/Military (7.3%).¹²⁸ Similar threats are expected to be even higher by 2016's end, as cyber-attacks are continually on the rise.¹²⁹

Why are these breaches so prevalent? They are directly correlated with societal advances in technology—as businesses and entities electronically collect, store, and transfer information about their business and compliance operations, customers, employees, and other related data, they are inevitably subject to technology's dark side of compromised privacy.¹³⁰ In today's digital age, unlike the times when data was physically stored in paper files, internal storage of electronic data and computer memories are constantly subject to system glitches, confusing technical requirements, and access by unauthorized persons that may lead to stolen intellectual property, with amplified risks when vendors or third parties manage information systems.¹³¹

The costs of these vulnerabilities are so vast that they are difficult to quantify. Various sources and surveys have attempted to provide estimates on the total aggregate costs stemming from cyber-breaches and attacks but such results vary depending on the study. One 2015 study examining 350 companies across eleven countries revealed that the average total cost of a data breach had increased by 23% over the prior two years to an estimated \$3.79 million.¹³² Some of the most common expenses associated with a breach include increased executive involvement in an organization's IT response and the purchase of insurance to mitigate the overall costs of a

128. Roy Urrico, *The 10 Worst Data Breaches of 2015 (So Far)*, CREDIT UNION TIMES (July 7, 2015), <http://www.cutimes.com/2015/07/07/the-10-worst-data-breaches-of-2015-so-far/>.

129. See Warren Gorham & Lamont, *ISACA Identifies Five Cyber Risk Trends for 2016*, BUS. WIRE (Dec. 16, 2015, 10:33 AM), <http://www.businesswire.com/news/home/20151216005814/en/>; see also Harriet Taylor, *Biggest Cybersecurity Threats in 2016*, CNBC (Dec. 28 2015, 1:17 PM), <http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html>.

130. See, e.g., Lawrence J. Trautman, *E-Commerce and Electronic Payment System Risks: Lessons from PayPal*, 16 U.C. DAVIS BUS. L.J. 24–37 (forthcoming 2016) (discussing the susceptibility of businesses engaged in e-commerce to cybersecurity risks); Lisa R. Lifshitz, Roland Hung & Evan Atwood, *The Canadian Approach to Data Breach Notification*, 66 CONSUMER FIN. L. Q. REP. 317, 318 (2012) (discussing that vast amounts of information in large databases increases risks of unauthorized access); MILLER, *supra* note 2, at 387–90 (“Accompanying the growth of data storage and communications . . . has been an ever-growing series of threats.”).

131. See David Orozco, *The Knowledge Police*, 43 HOFSTRA L. REV. 417, 424 (2014) (“Technological advancements . . . allow parties to infringe on IP rights at a relatively low cost.”); see also MILLER, *supra* note 2, at 388–90 (discussing increased reliance on technology as contributing to compromised data).

132. Larry Poneman, *Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis'*, SECURITY INTELLIGENCE (May 27, 2015), <https://securityintelligence.com/cost-of-a-data-breach-2015/#.Vc4PI1y4mT8>. The eleven countries included the United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, the Arabian region (United Arab Emirates and Saudi Arabia), and Canada. *Id.*

breach for persons affected.¹³³ Other associated costs include decreases in stock value, disruptions in regular business activities, stolen intellectual property, litigation and shareholder derivative lawsuits, and goodwill and reputational costs, all of which reached a high of one trillion dollars dating back to 2008 and are only expected to rise in future years.¹³⁴ A 2010 Symantec study that considered the costs associated with the different variables related to cyber-attacks found an average cost of \$2.8 million for large businesses and \$2 million annually for all businesses, while a McAfee report found that the average cost per firm was approximately \$1.2 million in 2010.¹³⁵ Despite attempts to quantify the costs of cyber-breaches, the true cost for the private sector remains unknown due to the fact that many cyber-attacks are often “unnoticed, unattributed, or at the very least underappreciated.”¹³⁶ The recent Cybersecurity Act, which became law in December of 2015, attempts to rectify the hesitation of entities to volunteer information out of fear of liability or future cyber-attacks by implementing a framework for private companies to safely share information about cybersecurity threats with other entities and the federal government.¹³⁷

Given the difficulty in determining just how far-reaching the costs of cyber-breaches and attacks may be, it is not surprising that a wide variety of regulatory and legislative efforts have increasingly sought to enforce data security safeguards by calling upon entities to publicly disclose their cybersecurity threats.¹³⁸ Several regulatory investigations into cyber-

133. *Id.*

134. Susskind, *supra* note 21, at 575 (citing THE WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION COMMUNICATIONS INFRASTRUCTURE (2009), https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf); *see also* David Z. Bodenheimer & Gordon Griffin, *Pillaging the Digital Treasure Troves the Technology, Economics, and Law of Cyber Espionage*, ABA SCITECH L., Winter 2014, at 16, 20; MILLER, *supra* note 2, at 400 (noting that class action attorneys “on the lookout for new cases” may be likely to file cybersecurity-related claims against companies “on behalf of thousands or millions of plaintiffs.”).

135. Scott J. Shackelford, Timothy Fort & Jamie D. Prenkert, *How Businesses Can Promote Cyber Peace*, 36 U. PA. J. INT’L L. 353, 371 (2014) (citing SYMANTEC, STATE OF ENTERPRISE SECURITY 9 (2010), https://www.symantec.com/content/en/us/about/presskits/SES_report_Feb_2010.pdf); MCAFFE & SCI. APPLICATIONS INT’L CORP., UNDERGROUND ECONOMIES: INTELLECTUAL CAPITAL AND SENSITIVE CORPORATE DATA NOW THE LATEST CYBERCRIME CURRENCY 3, 7 (2011), <http://www.ndia.org/Divisions/Divisions/Cyber/Documents/tp-underground-economies.pdf>).

136. Shackelford, Fort & Prenkert, *supra* note 135, at 371–72 (discussing the various reasons why such numbers are hard to pinpoint).

137. Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong. (2014); Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015); *see* Scott J. Shackelford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Comparative Case Study* 11 (Ind. Univ. Kelley Sch. of Bus. Research Paper No. 16-16, 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2714529 (discussing the provisions of the new Act).

138. *See* 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, 322 (2015) (discussing the efforts of the Federal Trade Commission (FTC) and the Securities and Exchange Commission

breaches have already occurred and regulators have stated that they will hold boards of directors, compliance personnel, and audit committees personally accountable for such risks.¹³⁹ One of the major areas of focus is improving the transparency of cyber-risks and guidelines for data breach notifications.¹⁴⁰ Beyond consumers, the effects of these threats on shareholders is especially important—the SEC recently noted that cybersecurity is the most significant risk currently facing the financial system.¹⁴¹ Such risks affect investment decisions, stock value, and investor access to information. Given the financial and reputational harm associated with cybersecurity vulnerabilities, one survey revealed that 78% of investors were “‘somewhat or very unlikely’ to invest in a company with a history of being targeted in cyber-attacks,” while 69% of investors were hesitant to invest in companies that have experienced one or more data breaches in their time.¹⁴²

This shareholder reluctance directly speaks to the core of “materiality,” which is the reporting threshold mandated by the SEC and defined under the federal securities laws as information that a reasonable investor would consider important in deciding whether to make an investment. Materiality is further defined as “a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the ‘total mix’ of information made available.”¹⁴³ Under this objective standard, inadequate disclosure of cybersecurity threats is likely to affect the investment decisions of shareholders, especially pertaining to the costs that such risks pose on stock price, interrupted business activity, stolen intellectual property, and the need for extra resources to purchase insurance or ensure adequate executive involvement.¹⁴⁴ Thus, it is to the financial detriment of reporting companies to be lax in these disclosures.

(SEC) in this sector); Davis, Wong & Paterson, *supra* note 38, at 629 (discussing regulatory efforts of the SEC, FTC, Federal Communication Commission, Department of Homeland Security, and Department of Justice in this arena).

139. Davis, Wong & Paterson, *supra* note 38, at 618.

140. Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 277–79 (2013) (noting that “as of August 2012, forty-six states and the federal government had adopted” some form of data breach notification law).

141. Lisa Lambert & Suzanne Barlyn, *SEC Says Cybersecurity Biggest Risk to Financial System*, REUTERS (May 18, 2016, 7:07 AM), <http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4>.

142. MILLER, *supra* note 2, at 400.

143. *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976).

144. *See, e.g.*, Roberta Anderson & Katherine Blair, 5 *Cybersecurity Considerations for Public Companies*, LAW360 (Feb. 10, 2014, 12:52 PM), <http://www.law360.com/articles/508038/5-cybersecurity-considerations-for-public-companies> (discussing Target as one example, whose stock price fell over 10.5% after the mega data breach and prompted a shareholder derivative lawsuit); Kevin M. Gatzlaff & Kathleen A. McCullough, *The Effect of Data Breaches on Shareholder Wealth*, 13 RISK MGMT. & INS. REV. 61 (2010) (utilizing event study methodology to conclude that the stock market reacts negatively to data breaches); Robert S. Thomas, *The Materiality Standard for Intellectual Property Disclosures*, 42 IDEA J.L. & TECH. 205, 225 (2002) (discussing the extent to which disclosure of intellectual property information is considered material).

They can ensure effectiveness by keeping abreast of any known cyber-risks that could potentially hurt their bottom line and their shareholders. Cybersecurity whistleblowers are well poised to contribute to these efforts by escalating all cyber-related concerns to management or boards of directors for prompt action.

Studies have revealed evidence that the stock market reacts more negatively if an entity fails to provide sufficient details about a cyber-breach.¹⁴⁵ Shareholders also commonly file derivative lawsuits in conjunction with data breaches, which seek to impose personal liability on directors or officers due to inadequate company management or disclosure of cybersecurity risks and breaches of fiduciary duty based on mismanagement.¹⁴⁶ For example, the several shareholder derivative lawsuits brought against Target alleged that top-level executives and directors waited too long to publicly disclose the mega data breach, thereby creating further damage and vulnerability to the company, and failed to take action despite having internally received information about potential security breaches several years prior.¹⁴⁷

Although the effects of the Target breach affected the sanctity of consumer debit and credit card information, the interest of shareholders in the matter was enormous. Shareholders highlighted that the breach “on the Company’s bottom line has been substantial” due to a damaged reputation and customer base, weakened sales and lost revenues, and the need for the company to reduce its fourth quarter 2013 adjusted earnings per share.¹⁴⁸ Additional effects on market value included increased costs due to lowered analyst ratings, price targets, and credit rating downgrades, various costs associated with investigations into the breach and consulting services, and numerous other related costs.¹⁴⁹ In addition to asserting claims for breaches of fiduciary duty, unjust enrichment, and corporate waste, the shareholders also called upon the company to “improve[] its corporate governance

145. Gatzlaff & McCullough, *supra* note 144, at 14, 17 (analyzing the effect of “firm response” after a breach and the extent to which firms were forthcoming about the details of a breach after having experienced one).

146. *See, e.g.*, Trial Filing, *Kulla v. Steinhafel, et al.*, No. 14-CV-00203(PAM-JJK), 2014 WL 2116594 (D. Minn. May 7, 2014) (representing the consolidated Target Corporation shareholder derivative lawsuits, alleging claims against officers and directors for breach of fiduciary duty, unjust enrichment, and corporate waste and seeking monetary relief “for these and other damages suffered by Target as a result of the individual defendants breaches of fiduciary duties”); *In re Heartland Payment Sys., Inc. Securities Litigation*, No. 09-1043, 2009 WL 4798148 (D.N.J. 2009) (shareholders accused the company’s directors and officers of fraudulently misrepresenting the state of data security in conference calls and financial statements); *see also* Victoria C. Wong, *Cybersecurity, Risk Management, and How Boards Can Effectively Fulfill Their Monitoring Role*, 15 U.C. DAVIS BUS. L.J. 201, 206 (2015) (discussing several examples of shareholder derivative lawsuits that seek to hold directors liable for improperly managing cybersecurity breaches).

147. *See generally* *Kulla*, 2014 WL 2116594 (claiming that many of these executives and directors were aware of potential security breaches as early as 2007).

148. *Id.*

149. *Id.*

structure.”¹⁵⁰ As may be seen from these allegations, shareholder interest in cybersecurity-related threats and data breaches is significant. Given that such breaches directly correlate with the financial health of affected entities, it is not surprising that the SEC, ever concerned with investor protection, has asserted itself as a key regulator in this arena.

B. THE SEC’S CYBERSECURITY FOCUS AND AUTHORITY

In the 2011 Guidance, the SEC only briefly discussed the extent to which public companies should report cybersecurity information under the categories of “Description of Business,” “Legal Proceedings,” and “Disclosure Controls and Procedures,” calling for general disclosure if cyber-incidents materially affect a registrant’s “products, services, relationships with customers or suppliers, or competitive conditions;” informing registrants that they “may need to” disclose information regarding any “material pending legal proceeding” involving cyber-incidents; and prompting registrants to consider the extent to which cyber-incidents threaten their ability to “record, process, summarize, and report [required] information.”¹⁵¹ The SEC provided slightly more detail in describing disclosure requirements under “Risk Factors” and “MD&A.” With respect to risk-factor disclosure, the SEC urged reporting companies to disclose whether the probability of cyber-incidents may render an investment in the company “speculative or risky” by considering prior cyber-incidents, the “quantitative and qualitative magnitude” of such risks, the risk that incidents remain undetected, and the adequacy of “preventative actions taken . . . in the context of the industry in which they operate.”¹⁵²

Importantly, the 2011 Guidance discourages the use of “generic risk disclosure” or “boilerplate” language to convey this information.¹⁵³ Although the SEC states that the federal securities laws would not require disclosure that “itself would compromise a registrant’s cybersecurity,” registrants “may” need to disclose existing or known threats to “place the discussion of cybersecurity risks in context.”¹⁵⁴ Under the MD&A category, the SEC calls upon registrants to disclose cybersecurity risks and incidents if the costs associated therewith represent a “material event, trend, or uncertainty that is reasonably likely” to: i) materially affect operations, liquidity, or financial condition; ii) lead to reduced revenues; iii) increase cybersecurity protection costs; or iv) threaten intellectual property rights if the effects of such incidents would be considered material.¹⁵⁵

150. *Id.*

151. See Letter from John D. Rockefeller IV, *supra* note 69; Avellan, *supra* note 69, at 206–07; see also *CF-2 Disclosure Guidance*, *supra* note 8.

152. *CF-2 Disclosure Guidance*, *supra* note 8, at 2.

153. *Id.*

154. *Id.*

155. See *id.*

As may be evident from reading the 2011 Guidance, companies are likely to experience considerable difficulty in determining whether they meet the materiality threshold for cyber-related disclosures given the lack of specific examples and general language. Further, the inability to use “boilerplate” language imposes a confusing standard on public companies as to the generality of their disclosures. Several commentators have already discussed the deficiencies of the 2011 Guidance, describing the guidelines as ambiguous and void of explicit definitions to adequately explain what type of information should be subject to disclosure or provide specific dollar or percentage amounts.¹⁵⁶ Further, there is also a risk that companies may reveal too much data and actually invite more cyber-risks, or make it easier for attackers to access their information systems.¹⁵⁷

Because the 2011 Guidance is not a binding regulation, some have argued that the SEC’s reliance on the 2011 Guidance, as an enforcement mechanism to target companies for providing what the agency deems insufficient cybersecurity disclosures, is a violation of administrative law.¹⁵⁸ Despite its mere advisory nature, the SEC has relied on the 2011 Guidance to threaten reporting companies with investigations, enforcement activity, and other penalties for non-compliance. In the eighteen months subsequent to the issuance of the 2011 Guidance, the SEC circulated comment letters to about fifty public companies to request information regarding their information security and cyber-related activity practices, which effectively required reporting companies to disclose information about past incidents.¹⁵⁹ Shortly thereafter, the SEC began to utilize actual enforcement mechanisms to ensure compliance with the 2011 Guidance by routinely policing whether reporting companies had adequately disclosed material information both after a known cyber-incident and on an ongoing basis to communicate the existence of cybersecurity risks.¹⁶⁰

The SEC has also specifically relied on the 2011 Guidance in imposing additional public reporting obligations on several well-known companies,

156. See, e.g., Avellan, *supra* note 69; Ferraro, *supra* note 92; see generally Young, *supra* note 92 (emphasizing the need for the SEC to establish a dollar threshold for prevention costs for cyberattacks, mitigations costs, and losses that, if exceeded, would require disclosure); Joel Bronstein, *The Balance Between Informing Investors and Protecting Companies: A Look at the Division of Corporation Finance’s Recent Guidelines on Cybersecurity Disclosure Requirements*, 13 N.C. J.L. & TECH. 257, 279 (2012) (discussing the inadequacies of the 2011 Guidance).

157. See, e.g., Bronstein, *supra* note 156, at 280–81; Jeff Roberts, *Will New SEC Guidelines Play Into The Hands of Cyber Attackers?*, GIGAOM (Nov. 14, 2011, 7:16 PM), <https://gigaom.com/2011/11/14/419-will-new-sec-guidelines-play-into-the-hands-of-cyber-attackers/>.

158. See, e.g., Ferraro, *supra* note 92, at 320–22 (discussing the non-binding effect of a non-legislative rule); Avellan, *supra* note 69, at 219 (noting that the 2011 Guidance “does not carry the authority of an official regulation”).

159. Daniel F. Schubert, Jonathan G. Cedarbaum & Leah Schloss, *The SEC’s Two Primary Theories in Cybersecurity Enforcement Actions*, THE CYBERSECURITY L. REPORT, Apr. 2015 (citing Letter from Mary Schapiro, Former Chair, U.S. Sec. & Exch. Comm’n, to Sen. John D. Rockefeller IV (May 1, 2013)).

160. See *id.*

leading these companies to believe that failure to respond would result in costly analysis and negative consequences, despite the fact that, in reality, there is no underlying binding force behind the guidance as an enforcement mechanism.¹⁶¹ These SEC inquiries have led to the use of comment letters by the agency to request revised or improved risk-factor disclosure regarding cybersecurity risk reporting and general monitoring of company press coverage of such events.¹⁶² Given the explicit internal disclaimer as to the non-binding nature of the 2011 Guidance, the lack of publication in the Federal Register, and the absence of any notice-and-comment period soliciting feedback as to proposed regulations, the 2011 Guidance has been described as having the same effect as a “speech an SEC staffer gave at a public conference about cybersecurity.”¹⁶³

In areas beyond public company disclosures, the SEC has used its regulatory authority to promulgate binding cybersecurity regulations. The SEC’s Regulation SCI is binding on self-regulatory organizations (SROs) like FINRA, alternative trading systems (ATSS), plan processors, and clearing agencies (collectively, SCI entities), requiring such entities to adopt procedures to ensure that their automated systems “have levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets.”¹⁶⁴ These procedures include mandated participation in the scheduled testing of business continuity operations and backup and disaster recovery plans; the coordination of this testing among other SCI entities; and the need to take corrective action with respect to systems disruptions and compliance issues, including mandated notices and reports to the SEC.¹⁶⁵

Similarly, Regulation S-ID, under which the SEC issued joint rules with the Commodity Futures Trading Commission (CFTC), requires financial institutions and creditors to design and implement written identity theft programs to protect the personal information of existing and prospective clients.¹⁶⁶ Regulation S-P is another related SEC regulation that is binding on investment advisers registered with the SEC, brokers, dealers, and investment

161. *See id.* (discussing several case studies of instances in which corporations altered their SEC disclosures based on the SEC’s request through reliance on the 2011 Guidance); Avellan, *supra* note 69.

162. David B.H. Martin et al., *SEC Activity Trends in Cybersecurity and Securities Law*, INSIDE COUNS. (Apr. 14, 2015), <http://www.insidecounsel.com/2015/04/14/sec-activity-trends-in-cyber-security-and-securities>.

163. Ferraro, *supra* note 92, at 323.

164. 17 C.F.R. § 242.1001 (2016); Regulation Systems Compliance and Integrity, Exchange Act Release No. 73,639, 110 SEC Docket 1377 (Feb. 3, 2015).

165. 17 C.F.R. § 242.1001; Regulation Systems Compliance and Integrity, Exchange Act Release No. 73,639, 110 SEC Docket 1377.

166. Identity Theft Red Flags Rules, Exchange Act Release No. 69,359, Investment Advisers Act Release No. 3582, Investment Company Act Release No. 30,456, 106 SEC Docket 165 (Apr. 10, 2013).

companies.¹⁶⁷ Regulation S-P mandates financial institutions to provide customers with notice of the institution's privacy procedures and prohibits the disclosure of personal consumer information to non-affiliated third parties.¹⁶⁸ In September 2015, the SEC pursued its first enforcement action specifically relating to cybersecurity against investment adviser R.T. Jones Capital Equities Management, which agreed to a cease-and-desist order and a \$75,000 penalty for failure to adopt Regulation S-P's required cybersecurity procedures, which had led to a breach that compromised the personal information of nearly 100,000 individuals.¹⁶⁹ This information was revealed after an SEC investigation found that the company had violated the "safeguards rule" of Regulation S-P by storing sensitive client information on a third-party web server, which was then attacked by an unknown hacker.¹⁷⁰ This enforcement action is further evidence of the agency's commitment to policing the financial markets for cybersecurity non-compliance.¹⁷¹

The SEC regulations described above are binding on SCI entities, financial institutions, creditors, investment advisors, brokers, dealers, and investment companies, thereby offering a legitimate enforcement mechanism to the agency to pursue inadequacies related to cybersecurity efforts. Similar SEC regulations, with the force of law, could be imposed on public companies to transform the 2011 Guidance into binding cybersecurity regulation. Such action is likely to assist companies in establishing clear and effective channels of information gathering and reporting while also ensuring that the reports of cybersecurity whistleblowers unquestionably constitute activities that are statutorily protected from retaliation.

The SEC may transform the 2011 Guidance into binding regulations pursuant to its general rulemaking authority under various provisions of the Securities Act of 1933 and the Exchange Act that allow the SEC to adopt regulations it deems "necessary or appropriate in the public interest or for the protection of investors."¹⁷² The SEC has considerable leeway in enacting

167. Privacy of Consumer Financial Information (Regulation S-P), Exchange Act Release No. 42,974, Investment Company Act Release No. 24,543, Investment Advisers Act Release No. 1883, 72 SEC Docket 1694 (Nov. 13, 2000) (implementing the requirements of the Gramm-Leach-Bliley Act).

168. *Id.*

169. Press Release, SEC Charges Investment Adviser, *supra* note 16.

170. *Id.*

171. *See id.*; SEC Announces First Cybersecurity Enforcement Action Against an Investment Adviser for Failure to Protect Client Data, NAT'L L. REV. (Oct. 6, 2015), <http://www.natlawreview.com/article/sec-announces-first-cybersecurity-enforcement-action-against-investment-adviser#sthash.BvPeWhCx.dpuf>.

172. *See, e.g.*, Exchange Act, Pub. L. No. 94-29, 89 Stat. 97 (1975) (codified as amended at 15 U.S.C. § 78m (2012)); 15 U.S.C. §§ 77g, 78j(b); *see also* Yoon-Ho Alex Lee, *The Efficiency Criterion for Securities Regulation: Investor Welfare or Total Surplus?*, 57 ARIZ. L. REV. 85, 94 n.37 (2015) (noting that "[t]his phrase appears very frequently and verbatim throughout the SEC's organic statutes); Lawrence J. Trautman & George P. Michaely, *The SEC & The Internet: Regulating the Web of Deceit*, 68 THE CONSUMER FIN. L. Q. REP. 262, 272 (2014) (discussing

regulations aimed at ensuring investor protection generally, which is ubiquitous among the various securities regulation statutes, including the general anti-fraud prohibition in Section 10(b) of the Exchange Act.¹⁷³ The SEC intended its 2011 Guidance to assist public companies in preparing disclosures in registration statements, periodic reports under the Exchange Act, and in ensuring that “statements and omissions both inside and outside of [SEC] filings” are compliant with “the antifraud provisions of the federal securities laws.”¹⁷⁴ As such, the SEC has expressed that the disclosures mandate compliance with a number of federal securities law provisions.¹⁷⁵

An additional source of SEC rulemaking authority for cybersecurity regulations may be found in the proxy disclosure provisions of Section 14(a) of the Exchange Act, which authorizes the SEC to broadly promulgate proxy disclosure regulations “in the public interest or for the protection of investors.”¹⁷⁶ As some scholars have noted, the authority of the SEC to promulgate proxy disclosure regulations in the “public interest” may be even more expansive than the authority to do so to ensure investor protection, as the former may be interpreted, through legislative history and examination of the federal securities laws, to authorize rulemaking efforts to promote social disclosures (as opposed to only financial disclosures) promoting corporate social transparency.¹⁷⁷ Social disclosures may include information such as the nature of the company’s products, the countries in which it conducts business, and the community and political effects of a company’s operations in the United States and abroad,¹⁷⁸ with the goal of making directors more responsive to the public interest and the promotion of effective corporate governance measures.¹⁷⁹ Given the importance of cybersecurity-related

authority of the SEC to regulate internet and cyber-related issues); Joseph A. Franco, *Why Antifraud Prohibitions Are Not Enough: The Significance of Opportunism, Candor and Signaling in the Economic Case for Mandatory Securities Disclosure*, 2002 COLUM. BUS. L. REV. 223, 362 n.39 (2002) (describing the various authority of the SEC to “craft rules ‘for the protection of investors’”).

173. See, e.g., 15 U.S.C. § 78j; Michael D. Guttentag, *Protection from What? Investor Protection and the Jobs Act*, 13 U.C. DAVIS BUS. L.J. 207, 212–13 (2013) (noting that “[t]he ubiquity of investor protection as a goal in securities regulation in the United States is evident from an inspection of the securities regulation statutes themselves,” including the Securities Act of 1933 and the Securities Exchange Act of 1934, the latter of which discusses “investor protection” over 200 times); see also Lee, *supra* note 172, at n.37 (discussing the SEC’s broad rulemaking authority).

174. *CF-2 Disclosure Guidance*, *supra* note 8, at n.2, 3.

175. See generally *CF-2 Disclosure Guidance*, *supra* note 8.

176. 15 U.S.C. § 78n.

177. Cynthia A. Williams, *The Securities and Exchange Commission and Corporate Social Transparency*, 112 HARV. L. REV. 1197, 1199, 1236–46, 1274 (1999) (discussing the SEC’s authority to require from public companies expanded social and corporate accountability disclosures).

178. *Id.*

179. See Roberta S. Karmel, *Qualitative Standards for ‘Qualified Securities’: Sec Regulation of Voting Rights*, 36 CATH. U. L. REV. 809, 824 (1987) (noting the SEC’s role in this arena); see also Philip C. Berg, *The Limits of Sec Authority Under Section 14(a) of the Exchange Act: Where Federal Disclosure Ends and State Corporate Governance Begins*, 17 J. CORP. L. 311, 323–24 (1992) (discussing academic commentary on the SEC’s broad rulemaking authority under Section 14(a)).

information to investors as material information and to the public at large, the promulgation of regulations specifically mandating cybersecurity disclosures is arguably well within the SEC's rulemaking mandate to enact regulations both for the protection of investors and in support of the public interest.

CONCLUSION

Cybersecurity whistleblowers help mitigate the harmful effects of cyber-breaches, cyber-risks and other related threats by contributing to a communication-intensive corporate culture that more effectively discovers and remediates these problems. The SEC is increasingly focused on soliciting disclosures from public companies about their cybersecurity threats and encouraging boards of directors and compliance officers to take on a heightened role in collecting and managing such information. Given the non-binding status of the SEC's 2011 Guidance and the narrow judicial interpretations of the retaliation protections available under the SOX and Dodd-Frank whistleblower programs, cybersecurity whistleblowers are likely to be excluded from these statutory protections due to their reports falling outside the realm of "protected activity" enumerated in these statutes. This gap in the law is likely to discourage cybersecurity whistleblowers from making the types of internal reports that are conducive to effective cybersecurity compliance. The transformation of the 2011 Guidance into binding regulation would ensure that cybersecurity whistleblowers are fully protected from any retaliation they may experience and that the value of the information they provide is fully appreciated by both regulated entities and the SEC.

and noting that Professor Louis Loss has also "characterize[d] the SEC's section 14(a) power as 'quasi-legislative'").