"GROUNDBREAKING" OR BROKEN? AN ANALYSIS OF SEC CYBERSECURITY DISCLOSURE GUIDANCE, ITS EFFECTIVENESS, AND IMPLICATIONS

*Matthew F. Ferraro**

ABSTRACT

In October 2011, the Securities and Exchange Commission (SEC) responded to mounting concern about the threat of cyber-attacks on corporate America by issuing staff guidance on when publicly traded companies should disclose information about cybersecurity vulnerabilities and attacks in their annual public filings. This SEC cybersecurity disclosure guidance has escaped serious analysis until now. Using case studies and paying particular attention to the comment letters sent by the SEC to registrants to prompt greater disclosure, this article concludes that the guidance both procedurally overreaches and substantively underachieves.

It overreaches because, while it is facially a nonlegislative rule, it has had the practical effect of binding private conduct as if it were a legislative one, violating the Administrative Procedure Act. It underachieves because the disclosures it requires are vague, similar across industries and companies, and bring little information to the marketplace. In particular, it fails to resolve an information asymmetry problem—between corporate managers and stockholders—that the disclosure laws are meant to address. To resolve these defects, the SEC should elevate cybersecurity disclosure guidance and issue it as a legislative rule, after a notice and comment period. Notice and comment rulemaking would contribute to sounder policy by allowing stakeholders to offer their expertise and experience at the front-end of the rulemaking process, improving the rule and its acceptability among the public.

This guidance offers a counterexample to those who say that

* J.D., Stanford Law School, 2013. I thank Professor Mariano-Florentino Cuéllar for supervising the directed research that became this article and for his mentorship during law school, Keri L. Vanderwarker and the other editors of the *Albany Law Review* for their careful review, and my family for their love and support. Of course, all errors are mine alone.

agencies do not commonly use guidance documents to make important policy decisions outside of the notice and comment process. The experience with this guidance also suggests the limits of agency creativity during periods of political ossification, and it challenges the simple verity that economic security and national security have merged.

I. INTRODUCTION

It has been said that history repeats itself, first as tragedy and then as farce[1]—and sometimes there is a thin line between the two. In May of 2013, a group loyal to the embattled Syrian President Bashar Al-Assad, known as the Syrian Electronic Army, hacked into the Twitter account of the satirical newspaper and website *The Onion* and sent out a series of inflammatory messages to the publication's five million Twitter followers.[2] The culprits reportedly were angered by what they considered the satirists' bias against the Syrian regime,[3] evidenced by a facetious column the paper published supposedly authored by Al-Assad, in which he boasted of killing 70,000 people.[4] After the attack, *The Onion*—which had been accustomed to skewering the news instead of being the subject of it—did something serious for a change.[5] It disclosed on its website a detailed account of how its Twitter account was compromised and suggested steps other websites could take to prevent similar attacks.[6]

What is remarkable about *The Onion* pulling back the layers of its cyber-attack is that the satirical newspaper took steps that many more sober organizations—fearful of admitting digital weaknesses

---

[1] *See* KARL MARX, *The Eighteenth Brumaire of Louis Bonaparte*, *in* THE PORTABLE KARL MARX 287, 287 (Eugene Kamenka trans., Penguin Books 1983) (1852).

[2] Nicole Perlroth, *No Joke: Syrians Hack The Onion*, N.Y. TIMES (May 6, 2013, 5:11 PM), http://bits.blogs.nytimes.com/2013/05/06/no-joke-syrians-hack-the-onion/.

[3] Dell Cameron & Oz Katerji, *Speaking With an Alleged Member of the SEA About Hacking The Onion's Twitter Account*, VICE (May 8, 2013), http://www.vice.com/en_ca/read/speaking-with-the-sea-about-hacking-the-onions-twitter-account (discussing an interview with a self-proclaimed Syrian hacker with the *nom de guerre* "The3 Pr0").

[4] "Bashar Al-Assad," (Fake) Op-Ed., *Hi, In The Past 2 Years, You Have Allowed Me to Kill 70,000 People*, THE ONION (Mar. 25, 2013), http://www.theonion.com/articles/hi-in-the-past-2-years-you-have-allowed-me-to-kill,31805/ (joke column supposedly written by Syria's embattled president).

[5] *See How the Syrian Electronic Army Hacked The Onion*, ONION INC.'S TECH TEAM (May 8, 2013), http://theonion.github.io/blog/2013/05/08/how-the-syrian-electronic-army-hacked-the-onion/.

[6] *See id.*

that may either invite future attacks or shake investor confidence—are reluctant to take.[7]

Such reluctance has persisted, even though the ubiquity of digital systems in modern society is matched only by their vulnerability to disruption.[8] In one survey, ninety percent of organizations reported having suffered at least one cybersecurity breach over a twelve-month period.[9] Seemingly every day, news breaks of yet another bank heist, espionage operation, or data theft accomplished not with masks and guns, but with clicks of a mouse and taps of a keyboard.[10] The U.S. government has spoken darkly of such cyber risks.[11] In his February 2013 State of the Union address, for instance, President Barack Obama warned of the "the rapidly growing threat [of] cyber-attacks."[12] He said that "hackers steal people's identities and infiltrate private e-mails [and] foreign countries and companies swipe our corporate secrets [while others seek] the ability to sabotage our power grid, our financial institutions, [and] our air traffic control systems."[13] He declared,

---

[7] Nick Bilton & Nicole Perlroth, *Details Emerge About Syrian Electronic Army's Recent Exploits*, N.Y. TIMES (May 10, 2013, 5:40 PM), http://bits.blogs.nytimes.com/2013/05/10/details-emerge-about-syrian-electronic-armys-recent-exploits/ ("Exposing details about an attack is not the normal approach companies take after they are hacked.").

[8] *See generally* Michael Bachmann, *Deciphering the Hacker Underground: First Quantitative Insights*, *in* CORPORATE HACKING AND TECHNOLOGY-DRIVEN CRIME 105, 105 (Thomas J. Holt & Bernadette H. Schell eds., 2011) ("The increasing dependence of modern societies . . . on information technology and computer networks renders them ever more vulnerable to attacks.").

[9] PONEMON INST. LLC, PERCEPTIONS ABOUT NETWORK SECURITY: SURVEY OF IT & IT SECURITY PRACTITIONERS IN THE U.S. 2 (2011), *available at* http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf; *see also* David E. Sanger & Eric Schmitt, *Rise is Seen in Cyberattacks Targeting U.S. Infrastructure*, N.Y. TIMES, July 27, 2012, at A8 (citing U.S. government estimate that there was a seventeen-fold increase in computer attacks on American infrastructure between 2009 and 2011).

[10] *See, e.g.*, Marc Santora et al., *In Hours, Thieves Took $45 Million in A.T.M. Scheme*, N.Y. TIMES, May 10, 2013, at A1 (reporting that a worldwide heist was facilitated by digital sleight-of-hand); Craig Timberg, *Report: China is Top Source of Cyber-Spying*, WASH. POST, Apr. 23, 2013, at A12 ("[H]ackers affiliated with the Chinese government were by far the most energetic and successful cyberspies in the world last year . . . . dominat[ing] the category of state-affiliated cyber-espionage of intellectual property."); Nicole Perlroth, *Twitter Hacked: Data for 250,000 Users May Be Stolen*, N.Y. TIMES (Feb. 1, 2013, 7:49 PM), http://bits.blogs.nytimes.com/2013/02/01/twitter-hacked-data-for-250000-users-stolen/ (discussing theft and possible sale of twitter passwords). By the time this article is published, there will no doubt be many more examples that could be added to this list.

[11] *See* Barack Obama, U.S. President, Address Before a Joint Session of Congress on the State of the Union 9 (Feb. 12, 2013), *available at* http://www.gpo.gov/fdsys/pkg/DCPD-201300088/pdf/DCPD-201300088.pdf.

[12] *Id.*

[13] *Id.*

"[w]e cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[14]

In light of these threats, the Executive branch has taken action to address cybersecurity, recently through an Executive order meant to strengthen public-private cooperation on electronic infrastructure protection,[15] but broader legislation intended to bolster cybersecurity has failed, due to disagreements among the U.S. House, Senate, and White House, and privacy advocates, business interests, and security specialists.[16]

In October of 2011, another branch of the federal government sought to promote security in the digital domain.[17] In response to pressure from the Senate Commerce Committee and a spate of highly publicized attacks on public companies,[18] the Division of Corporation Finance of the Securities and Exchange Commission (SEC) issued a staff document called "Disclosure Guidance Topic No. 2—Cybersecurity" (hereinafter referred to as CF DG 2), which set forth the SEC staff's views on the disclosure obligations of public companies related to cybersecurity risks and cyber-attacks.[19] Under the Securities Acts of 1933 and 1934,[20] companies registered with the SEC are required to disclose material information, for the benefit of investors, in their registration statements and in periodic reports.[21] For the first time, CF DG 2 established that the SEC considered information related to cybersecurity "material" and

---

[14] *Id.*

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

[16] *See* Gerry Smith, *Senate Won't Vote on CISPA, Deals Blow to Controversial Cyber Bill*, HUFFINGTON POST (Apr. 25, 2013, 7:13 PM), http://www.huffingtonpost.com/2013/04/25/cispa-cyber-bill_n_3158221.html/. Another highly anticipated cybersecurity bill that would have asked key infrastructure assets to submit voluntarily their computer networks to security testing failed to pass the U.S. Senate in 2012 over similar concerns. *See* Mark Clayton, *Senate Cybersecurity Bill Fails, So Obama Could Take Charge*, CHRISTIAN SCI. MONITOR (Nov. 16, 2012, 5:45 PM), http://www.csmonitor.com/USA/Politics/2012/1116/Senate-cybersecurity-bill-fails-so-Obama-could-take-charge. *See generally* MICHAEL E. BLEIER ET AL., REED SMITH LLP, THE CURRENT STATE IN FINANCIAL SERVICES CYBERSECURITY 4 (2013), *available at* http://www.reedsmith.com/The-Current-State-in-Financial-Services-Cybersecurity-07-22-2013/ (providing an overview of proposed cybersecurity legislation).

[17] *See CF Disclosure Guidance: Topic No. 2—Cybersecurity*, DIV. OF CORP. FIN., U.S. SEC. & EXCH. COMM'N (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [hereinafter CF DG 2].

[18] *See infra* Part III.A.

[19] *See* CF DG 2, *supra* note 17.

[20] Securities Act of 1933, 15 U.S.C. § 77a–77bbbb (2012); Securities Exchange Act of 1934, 15 U.S.C. § 78a–78oo (2012).

[21] *See* 15 U.S.C. § 77g; *Id.* § 78l–m. For the canonical U.S. Supreme Court case that established the modern doctrine of materiality, see TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).

requiring disclosure.[22] In essence, the SEC sought to encourage public companies to act more like *The Onion*—to disclose in their required filings information about their cyber vulnerabilities and cyber-attacks. At the time, policymakers hailed the SEC guidance as "groundbreaking" and "a critical step toward improving U.S. cybersecurity," since it was expected to bring such vulnerabilities—which firms have an inherent disincentive to publicize, lest their stock prices fall—to light, "allow[ing] market participants to weigh cybersecurity as an investment factor" and prompting the private sector to bolster cyber defense and mitigation measures.[23]

Almost two years after its initial issuance, policymakers expressed keen interest in revisiting the guidance.[24] In April of 2013, Senator John D. (Jay) Rockefeller IV, who, as discussed *infra*, played a key role in calling for cyber disclosure guidance, wrote to the SEC Chairwoman Mary Jo White to praise the effectiveness of CF DG 2, but also to ask that she "elevate [CF DG 2] and issue it at the Commission level," so as to send "a strong signal to the market that companies need to take their cybersecurity efforts seriously."[25] In response, Chairwoman White said she would review "current disclosure practices and overall compliance with the guidance [and] recommendations . . . [for] further action in this area."[26]

Despite the fanfare that heralded the release of CF DG 2 and the recent interest in revising it, scholars have written little about the topic.[27] The analysis that does exist consists largely of newsletters propagated by law firms, articles in the popular press, and

---

[22] *See* CF DG 2, *supra* note 17.

[23] *See* Jay Rockefeller & Michael Chertoff, Op-Ed., *A Step Toward Improving Cybersecurity*, WASH. POST, Nov. 18, 2011, at A19.

[24] *See* Letter from John D. Rockefeller IV, Chairman, U.S. Senate Comm. on Commerce, Sci., & Transp., to Mary Jo White, Chairman, Sec. & Exch. Comm'n (Apr. 9, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51 [hereinafter Rockefeller Letter 2013]; *see also* 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. ONLINE 257, 279–82 (2012) (discussing critiques of CF DG 2 by various authorities on cybersecurity).

[25] *See* Rockefeller Letter 2013, *supra* note 24.

[26] Letter from Mary Jo White, Chairman, Sec. & Exch. Comm'n, to John D. Rockefeller IV, Chairman, U.S. Senate Comm. on Commerce, Sci. & Transp. (May 1, 2013), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-97qfyd [hereinafter White Letter]; *see* Phyllis Diamond, *White Says SEC Staff is Reviewing Adequacy of Cybersecurity Risk Disclosures*, BLOOMBERG BNA DAILY REPORT FOR EXECUTIVES 6 (May 15, 2013).

[27] For two short law journal pieces written by students that are notable exceptions, see Bronstein, *supra* note 24, at 257–61 and Sam Young, Note, *Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches*, 38 J. CORP. L. 659, 660–62 (2013).

practitioner alerts.[28] Even less work has looked at the effect the guidance has had on corporate behavior, analyzed the disclosures themselves, or questioned whether the policymaking form the SEC utilized—staff policy guidance issued without a vote of the presidentially appointed SEC Commissioners and released without a notice and comment process—is permissible under the Administrative Procedure Act (APA).[29] Generally, administrative rulemaking falls into two categories: "legislative rules" that carry the force of law, are authorized pursuant to a Congressional statute, and are subject to public notice and comment before becoming final,[30] and "nonlegislative rules" (typically categorized into subgroups, interpretive rules, or guidance documents) that lack legal force and are not subject to the notice and comment requirements of legislative rules.[31] On its face, CF DG 2 is a nonlegislative rule.[32] Finally, little has been said about whether CF DG 2, whatever its policymaking form, makes for good policy, informing investors and promoting greater cybersecurity.

This article adds to the existing literature by addressing those gaps. Using case studies, it is the first piece to evaluate the cyber disclosures of SEC-registered companies themselves since CF DG 2's issuance, and it particularly analyzes SEC-issued comment letters that invoked CF DG 2 to prompt greater disclosures.

Based on that evidence, this article concludes that CF DG 2 is both procedurally and substantively flawed. It argues that the

---

[28] *See, e.g.*, Ernest E. Badway & Daniel A. Schnapp, *Protecting Intellectual Property from Cyber Crime: A Common Sense Approach*, N.Y.L.J., Nov. 5, 2012, at 9, col. 1 (describing "the current state of significant cyber dangers, regulatory efforts to protect intellectual property and cyber systems, and the consideration and implementation of policies and procedures for businesses."); Roland L. Trope, *"There's No App for That": Calibrating Cybersecurity Safeguards and Disclosures*, 68 BUS. LAW 183, 184 (2012) (detailing a 2011–2012 survey of the law related to cybersecurity); RICHARD E. BALTZ ET AL., ARNOLD PORTER LLP, SEC CYBERSECURITY DISCLOSURE FOR PUBLICLY TRADED COMPANIES, INCLUDING GOVERNMENT CONTRACTORS 1–4 (2011) (discussing how CF DG 2 affects companies holding government contracts); Vince Crisler, *New Cyber Security Disclosure Guidance from the SEC*, EMERGING ISSUES, Jan. 24, 2012, 2012 EMERGING ISSUES 6186 (Lexis) (discussing CF DG 2 and how it will affect SEC disclosures).

[29] *See infra* Parts III.B, IV, V.A.

[30] *See* William Funk, *A Primer on Nonlegislative Rules*, 53 ADMIN. L. REV. 1321, 1322 (2001); Connor N. Raso, Note, *Strategic or Sincere? Analyzing Agency Use of Guidance Documents*, 119 YALE L.J. 782, 788 (2010).

[31] *See* 5 U.S.C. § 553 (2006) ("General notice of proposed rule making . . . does not apply[] to interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice."); *see also* Funk, *supra* note 30, at 1322 (providing overview of differences between legislative and nonlegislative rules); Raso, *supra* note 30, at 788 (introducing the differences between guidance documents and legislative rules).

[32] CF DG 2, *supra* note 17 ("This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission.").

guidance both *overreaches* and *underachieves*. First, it overreaches because, as implemented, it has had the practical effect of binding company behavior in a way that violates traditional limits on nonlegislative rules. While it is a close call given: (1) the warnings CF DG 2 carries that it is merely advisory,[33] (2) the SEC's authority under the securities laws to regulate registered companies' disclosures,[34] (3) the SEC staff's routine practice of communicating with registrants to provide feedback on their filings,[35] and (4) the difficulty courts have had distinguishing between legislative and nonlegislative rules,[36] an analysis of the letters the SEC sent to registrants and the registrants' subsequent actions strongly suggest that CF DG 2 has been given the de facto effect of law. Research presented here shows, in short, that the registrants did not have a choice; they did essentially what the SEC asked of them, disclosing more information about cyber-attacks than they wished, even after the registrants objected in writing to the SEC's interpretation of the governing law or averred that the information was not "material" and requiring of disclosure. Since the SEC can bring an enforcement action if a company fails to disclose material information, and shareholders can file suit for similar claims,[37] failing to adhere to CF DG 2 could potentially carry significant dangers.[38]

This article also argues that CF DG 2 underachieves for, even though the guidance overreaches, the disclosures it has prompted do little to bring valuable information about corporate cyber vulnerabilities or attacks to light. An analysis of case studies across industries shows that, most often, even after the SEC's prodding, companies have inserted essentially boilerplate disclosures that

---

[33] *See id.*

[34] *See generally* 1 THOMAS LEE HAZEN, TREATISE ON THE LAW OF SECURITIES REGULATION § 1.4 (6th ed. 2009 & Supp. 2013) (providing overview of SEC authority).

[35] *See The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, U.S. SEC. & EXCH. COMM'N, http://www.sec.gov/about/whatwedo.shtml (last modified June 10, 2013) [hereinafter *The Investor's Advocate*] ("Through the Division's review process, the staff checks to see if publicly-held companies are meeting their disclosure requirements and seeks to improve the quality of the disclosure."). For ease, this article uses the words "company," "corporation," and "registrant" (that is, a company registered with the SEC) interchangeably.

[36] *See, e.g.*, Gen. Motors Corp. v. Ruckelshaus, 742 F.2d 1561, 1565 (D.C. Cir. 1984) ("[T]he distinction between legislative and nonlegislative rules has been described as 'enshrouded in considerable smog.'") (internal citation omitted).

[37] *See* 15 U.S.C. § 78u (2013) (establishing SEC enforcement authorities); HAZEN, *supra* note 34, § 1.4[6] (describing SEC enforcement activity).

[38] The SEC has not brought suit against any company for failing to make a cybersecurity disclosure.

speak vaguely about past or future cyber-attacks and their preparedness for them.[39] If the goal of the guidance was to prompt registrants to make *some* mention of cybersecurity, CF DG 2 has succeeded; if the goal was to "change[] everything [to] allow the market to evaluate companies in part based on their ability to keep their networks secure," as Senator Rockefeller said,[40] or "create the demand curve for cybersecurity," as the former White House cyber coordinator said,[41] results have disappointed. As discussed more in Part VI, this reticence stems partly from a muddied understanding of what kind of cyber-attacks qualify as "material" under the securities laws and from a concern with revealing too much information publicly that could provide would-be hackers with a roadmap for successful attacks—a concern CF DG 2 recognizes but does little to resolve.[42] Ironically, if the SEC utilizes CF DG 2 to achieve its desired policy ends—by forcing greater and more detailed disclosures about potential and past cyber-attacks—it will compound its violations of the APA by giving the guidance an even greater binding effect.

In light of these procedural and substantive shortcomings, this article makes one concrete recommendation and addresses three doctrinal implications. Primarily, the SEC should rescind CF DG 2 and issue stronger cybersecurity disclosure directives, not as staff guidance but as a legislative rule approved by the SEC Commissioners after a period of notice and comment. Issuing cyber disclosure guidance as a rule in this manner would not simply resolve the procedural flaw, but also likely result in sounder policy. The rule would carry greater legitimacy among the public, improve transparency, and—with the input of regulated entities, security professionals, and other interested parties—benefit from outside expertise in resolving the hard questions surrounding when a cyber-attack would be material and where to strike the balance between releasing appropriate information about a breach and compromising

[39] As noted below, on a few occasions, companies have inserted more specific information about particular cyber breaches or pending litigation, but even that information has been minimal. *See infra* Part V.A.

[40] Ellen Nakashima & David S. Hilzenrath, *SEC: Firms Must Report Cyberattacks*, WASH. POST, Oct. 15, 2011, at A10.

[41] *Id.*

[42] CF DG 2, *supra* note 17 ("We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security—and we emphasize that disclosures of that nature are not required under the federal securities laws.").

security by saying too much.[43]

In addition to this specific recommendation, this article discusses three doctrinal implications that go beyond the issues of the SEC and corporate disclosure to larger questions of administrative rulemaking, economic security, and national security. First, the findings here offer an example of a recently studied phenomenon—how agencies issue guidance documents to make important policy decisions outside the formal legislative rulemaking system.[44] This case buttresses the claim that agencies pursue guidance documents to further policy outside of notice and comment, especially during periods of divided government, when political inaction places administrative agencies in the position of trying to please both the President and Congress without having consensus direction from both.

Second, the findings demonstrate how political paralysis opens up space for agency creativity when trying to solve public policy problems, but also how those efforts can fall short, procedurally and substantively. In an era of legislative ossification, one sympathizes with the SEC staff that is trying to address a major security threat. Here, that pressure led to a creative approach to an intractable problem, but with mixed results.

Finally, while many argue that "[n]ational security and economic security have converged,"[45] the experience with the SEC's cybersecurity disclosure guidance suggests the limits of that union when it comes to administrative regulation. Without greater legislative changes, the New Deal-era organization developed to meet the economic security threats of the twentieth century is ill-suited to meet the high-tech security threats of the twenty-first century. Congress and the public should moderate their expectations of what the SEC can accomplish to promote more cybersecurity, specifically, and national security goals, more generally.

---

[43] *See* Nat'l Tour Brokers Ass'n v. United States, 591 F.2d 896, 902 (D.C. Cir. 1978) (describing the purpose of notice and comment procedures); *see also* Chocolate Mfrs. Ass'n of the U.S. v. Block, 755 F.2d 1098, 1103 (4th Cir. 1985) ("The notice-and-comment procedure encourages public participation in the administrative process and educates the agency, thereby helping to ensure informed agency decisionmaking.").

[44] *See generally* Raso, *supra* note 30, at 786 (assessing when agencies use guidance documents rather than formal rules).

[45] *See* Joel Brenner, *The Calm Before the Storm*, FOREIGN POL'Y (Sept. 6, 2011), http://www.foreignpolicy.com/articles/2011/09/06/the_calm_before_the_storm; *see also* Aaron L. Friedberg, *The Changing Relationship Between Economics and National Security*, 106 POL. SCI. Q. 265, 265 (1991) ("[E]conomics and national security are and will continue to be intimately intertwined.").

In Part II, this article explains cyber-attacks, describes their growing threat to the private sector, and corporations' traditional disincentives to disclose them. Part III describes CF DG 2, its history, its relationship to the securities laws, and its structure. Part IV discusses the difference between legislative and nonlegislative rules and between interpretive rules and guidance documents, and explains how this article applies that taxonomy to CF DG 2. Part V reviews ten case studies where the SEC invoked CF DG 2 to prompt companies to expand their cybersecurity disclosures. Part VI analyzes those case studies to argue that the guidance both overreaches procedurally and underachieves substantively. Part VII offers recommendations and implications, and Part VIII concludes.

II. CYBER-ATTACKS, CYBER THREATS, AND THE CORPORATE INCENTIVE AGAINST DISCLOSURE

A. Defining a Cyber-attack

The SEC defines "cybersecurity" as "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access."[46] However, the SEC does not define a "cyber-attack."[47] The U.S. Department of Defense distinguishes between three different kinds of so-called computer network operations[48]: (1) computer network defense (CND), which encompasses actions taken "to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks,"[49] (2) computer network attacks (CNA), which are "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves,"[50] and (3) computer network exploitations (CNE), which are "[e]nabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or

[46] CF DG 2, *supra* note 17.

[47] *See id.*

[48] AIR UNIV., *Computer Network Operations & Network Warfare Operations*, U.S. AIR FORCE, http://www.au.af.mil/info-ops/netops.htm (last updated July 24, 2010).

[49] *Id.*

[50] *Id.*

networks."[51] Legal scholarship tends to focus on computer network attacks (often calling them "cyber-attacks") while ignoring what the military considers computer network defense or computer network exploitations.[52]

This article adopts an expansive definition of "cyber-attack" that includes both computer network attacks and computer network exploitations. Herein, a "cyber-attack" is: a "deliberate action[] to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks"[53] as well as any unauthorized "intelligence-gathering activity"—including "the monitoring or copying of data"[54]—conducted on those systems or networks.[55]

To effectuate a successful cyber-attack, an attacker needs access to a target's computer or network—gained either from afar (through the Internet) or up close (through a thumb drive, for instance)—that allows the exploitation of a "vulnerability"—such as altered software or hardware—to deliver a "payload"—usually a piece of software that, once entered into a targeted computer, performs any number of insidious actions, such as "reproducing and retransmitting itself, destroying files on the system, or altering files."[56] The weakest link in computer network protection remains the people themselves—innocent computer users who download malicious software, lose hardware, or witlessly post proprietary

---

[51] *Id.*

[52] *See* Aaron P. Brecher, Note, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations*, 111 MICH. L. REV. 423, 424–25 (2012) (citing NAT'L RESEARCH COUNCIL OF THE NATI'L ACADS, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009), *available at* http://www.carlisle.army.mil/DIME/documents/2Cyberattack%20Brochure_FINAL.pdf [hereinafter NRC REPORT]); Hannah Lobel, Note, *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, 47 TEX. INT'L L.J. 617, 622–23 (2012) (same). For a broader definition, see Marc J. Lederer, *Obligations of Public Companies to Disclose Cybersecurity Risks and Attacks*, EMERGING ISSUES, Feb. 2, 2012, 2012 EMERGING ISSUES 6204 (Lexis), at n.3. For a narrower interpretation, see Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 826 (2012); *cf.* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422 (2011) (describing the difficulty of defining terms in this field).

[53] NRC REPORT, *supra* note 52, at 1.

[54] Brecher, *supra* note 52, at 425.

[55] NRC REPORT, *supra* note 52, at 1.

[56] *Id.* at 3; *see also* Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR, Apr. 2011, at 152 (describing how a thumb drive provides access to a computer network); Cindy Vanegas, *Types of Cyber-attacks and How to Recognize Them*, FOXBUSINESS (Jan. 26, 2011), http://smallbusiness.foxbusiness.com/technology-web/2011/01/26/types-cyber-attacks-recognize/ (summarizing different kinds of common cyber-attacks from "bots" to "worms").

information on the Internet.[57] Some cyber-attacks, like denial-of-service attacks, do not even require the unauthorized access of a computer system, since they operate by merely overwhelming a computer website with redundant requests until the site crashes.[58]

B. The Growing Danger of Cyber-attacks on Corporations

Attacks themselves run the gamut from bank thefts[59] to intellectual property thefts[60] to military attacks,[61] and the cyber-attackers themselves range from foreign intelligence services[62] to crime syndicates to individuals motivated by avarice or ideology.[63]

The effects of cyber-attacks on private companies can be stark. "Attacks may result in disruptions to corporate networks and the compromise of trade secrets, intellectual property, and financial and confidential data."[64] One report estimated that in 2011, the average cost of a data breach that resulted in the "loss or theft of protected personal data was $5.5 million, or an average of $194 per

---

[57] Rene Siemens & David L. Beck, *Siemens and Beck on Obtaining Optimal Cyber Insurance*, EMERGING ISSUES, Sept. 4, 2012, 2012 EMERGING ISSUES 6613 (Lexis) (providing examples of such human foibles).

[58] *See* Bronstein, *supra* note 24, at 264 & n.41; Joshua McLaurin, *Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks*, 30 YALE L. & POL'Y REV. 211, 216 (2011) (describing denial-of-service attacks). A detailed description of cyber-attacks and corresponding defenses falls outside the scope of this paper. For more on such specifics, see SANS INST., CRITICAL CONTROLS FOR EFFECTIVE CYBER DEFENSE (2013), *available at* http://www.sans.org/critical-security-controls/cag4-1.pdf.

[59] *See* Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2011 U.S. Dist. LEXIS 62677, at *17–18 (E.D. Mich. June 13, 2011) (plaintiff was tricked by bogus email claiming to originate from defendant into providing a third-party with online access to plaintiff's bank accounts, resulting in ninety-three fraudulent money transfers totaling over $1.9 million to the third-party, which was based in either Russia or Estonia).

[60] *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009-2011, at i–ii (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf ("[F]oreign collectors will remain interested in all aspects of US economic activity and technology [in the near-term].").

[61] *See* Gross, *supra* note 56, at 152 (describing "Stuxnet" worm, likely a covert attack by the U.S. and Israel, which infected Iranian military computers and sabotaged Iranian uranium centrifuges).

[62] *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the S. Select Comm. on Intelligence*, 112th Cong. 8 (2012) (statement of James R. Clapper, Director of National Intelligence) [hearinafter *Worldwide Threat Assessment*] ("We assess that foreign intelligence services (FIS) are constantly developing methods and technologies that challenge the ability of the US Government and private sector to protect US national security and economic information.").

[63] *See generally* Bronstein, *supra* note 24, at 262 (discussing financial and ideological motives); Brenner, *supra* note 45 (discussing use of cyber-attacks by crime syndicates).

[64] Crisler, *supra* note 28.

compromised record."[65] Some cyber-attacks cost much more; a 2011 attack on Sony, Corp. likely cost the company in excess of $170 million.[66] Such thefts can form "the basis for a new breed of lawsuits," in which plaintiffs allege that the attacked corporation was negligent in protecting its customers' personal information, allowing for the increased potential for identity theft.[67] Concerns over such litigation costs and settlements are prompting the growth of a new market for cyber insurance, now a $1 billion industry.[68] Given the wide-ranging threats cyber-attacks pose to corporations, "the World Economic Forum ranked cyberattacks on businesses and governments as the fourth greatest threat to global stability."[69]

There has been no shortage of cybersecurity Cassandras pronouncing upon the fundamental vulnerabilities of the modern, wired world for national security interests, public utilities, and private firms.[70] For instance, the former Chairman of the U.S. Joint Chiefs of Staff, Admiral Michael Mullen, called cyber-attacks one of only "two existential threats to the United States"—on par with nuclear proliferation.[71] The theft of intellectual property through cyber espionage amounts to "probably the biggest transfer of wealth through theft and piracy in the history of mankind," according to one U.S. Senator.[72] The number and success rate of cybersecurity attacks on private companies reportedly increase with each passing year.[73]

The U.S. Director of National Intelligence, James R. Clapper, Jr., has called cyber threats "a critical national and economic security concern."[74] In Congressional testimony, he "underscore[d] the

---

[65] Siemens & Beck, *supra* note 57 (citing PONEMON INST. LLC, 2011 COST OF DATA BREACH STUDY: UNITED STATES 1 (2012), *available at* http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf).

[66] Salvador Rodriguez, *Cyber Crimes Get More Costly*, L.A. TIMES, Aug. 3, 2011, at B4.

[67] Siemens & Beck, *supra* note 57 (quoting Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1050 (E.D. Mo. 2009)).

[68] Michael P. Voelker, *As Cyber Coverage Soars, Opportunity Clicks*, PROP.CASUALTY360° (Jan. 21, 2013), http://www.propertycasualty360.com/2013/01/21/as-cyber-coverage-soars-opportunity-clicks ("Cyber insurance[] business is booming.").

[69] *See* Bronstein, *supra* note 24, at 267.

[70] *See* Brenner, *supra* note 45 (listing various cyber threats).

[71] Karen Parrish, *Mullen Offers 40-year Perspective on Social, Military Issues*, AM. FORCES PRESS SERVICE (Sept. 20, 2011), http://www.defense.gov/news/newsarticle.aspx?id=65393.

[72] Scott J. Shackelford, *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012*, 64 STAN. L. REV. ONLINE 106, 107 (2012) (quoting Tim Starks, *Cybersecurity: Learning to Share*, CONG. Q WKLY., Aug. 2, 2010, at 1858).

[73] *See* Matt Liebowitz, *2011 Set to Be Worst Year Ever for Security Breaches*, TECH. NEWS DAILY (June 10, 2011, 10:47 AM), http://www.technewsdaily.com/2710-2011-worst-year-ever-security-breaches.html.

[74] *Worldwide Threat Assessment*, *supra* note 62, at 7.

vulnerability of key sectors of the US and global economy,"[75] noted that cyber-attacks are "likely to increase in coming years," and highlighted the challenge of protecting against threats given the difficulty in "identifying past or present security breaches."[76]

C. Traditional Disincentives for Disclosure of Cyber-attacks

Part of the difficulty in identifying cybersecurity breaches among private companies is the reluctance of such companies to disclose voluntarily when they have suffered attacks.[77] There are three main reasons why. First, most cyber-attacks are meant to remain covert; some victims are simply unaware that they have been victimized at all.[78] Second, victim corporations fear that disclosing information about a cyber-attack will provide other would-be attackers with a "road map" either for attacking their company again, or another similarly situated one.[79] This concern presents a notable inversion of a traditional argument for mandatory disclosure—that companies should be forced to disclose material information because of the benefits their disclosures will have on third-party companies.[80] Frank Easterbrook and Daniel Fischel have argued:

> The information produced by one firm for its investors may be valuable to investors in other firms. Firm A's statements may reveal something about the industry in which Firm A operates . . . that other participants in the industry can use . . . . Yet Firm A cannot charge the investors in these other firms for the benefits, although they would be willing to pay for them. Because they cannot be charged, the information will be underproduced.[81]

---

[75] *Id.*

[76] *Id.* at 8.

[77] *See* Nakashima & Hilzenrath, *supra* note 40; Nicole Perlroth, *Traveling Light in a Time of Digital Thievery*, N.Y. TIMES, Feb. 11, 2012, at A1.

[78] *See* Perlroth, *supra* note 77 ("Most breaches go unreported, security experts say, because corporate victims fear what disclosure might mean for their stock price, or because those affected never knew they were hacked in the first place.").

[79] *See* Interview by Jamie Reeves with John Reed Stark, Managing Dir., Stroz Friedberg, former Chief, SEC Office of Internet Enforcement (Nov. 7, 2011), *available at* https://www.boardmember.com/Article_Details.aspx?id=6937.

[80] *See* Frank H. Easterbrook & Daniel R. Fischel, *Mandatory Disclosure and the Protection of Investors*, 70 VA. L. REV. 669, 697–98 (1984) (justifying mandatory disclosure regulation at the federal rather than state level on the disclosures' third-party effects).

[81] *Id.* at 685. Easterbrook and Fischel's enthusiasm for SEC disclosure rules is tempered, though, as the best of bad options. *Id.* at 715 ("We cannot say that the existing securities laws are beneficial, but we also are not confident that their probable replacements would be

The experience with cyber-attacks suggests that mandatory disclosure actually may be inimical to the cybersecurity (and, thus, corporate well-being) of third-party firms, since detailed disclosures essentially share hacking best-practices.[82] In this line of thinking, third-parties would want targeted firms to "underproduce[]" information as a means of communal self-protection.[83] This may present corporations with a Hobson's choice: "If Registrants' disclosures contain sufficient information to be meaningful for investors, disclosures almost certainly will have to contain information of value to Adversaries seeking reconnaissance data that will facilitate a breach."[84]

Finally, firms are reluctant to publicize news of attempted or successful cyber-attacks for fear of the negative effects such disclosures could have on investor confidence, share price, litigation, and reputation.[85] In other words, firms are disincentivized to share full information with the market—a classic information asymmetry problem, which mandatory disclosure obligations are intended to address.[86]

III. EXPLAINING CF DG 2

A. History of CF DG 2

A series of high-profile cyber-attacks in 2011 drew increased attention to cyber threats and to the need for a policy response to resolve this information asymmetry.[87] In one particularly daring

better.").

[82] *See id.* at 686 (discussing how the disclosure of information by one party could give competitive information to another party); Ronald L. Trope & Sarah Jane Hughes, *The SEC Staff's "Cybersecurity Disclosure" Guidance: Will it Help Investors or Cyber-thieves More?*, BUS. L. TODAY, Dec. 2011, at 1.

[83] *See* Easterbrook & Fischel, *supra* note 80, at 685; Trope & Hughes, *supra* note 82, at 3.

[84] Trope & Hughes, *supra* note 82, at 4 (referring mistakenly to this situation as a "Hobbesian choice"); *see* Maria Lokshin, *With Cyber Threats to Financial Services, Questions Loom About Role of Regulation*, 45 Sec. Reg. & L. Rep. (BNA), 1544, 1544 (Aug. 19, 2013).

[85] *See* Nakashima & Hilzenrath, *supra* note 40; Perlroth, *supra* note 77; *see also* Brenner, *supra* note 45 (noting victims "rarely admit" corporate espionage). An exception to this occurred in early 2013, when several high-profile companies, including Twitter, Facebook, Apple, and the *New York Times* "announced that they were attacked by sophisticated cybercriminals." Nicole Perlroth, *Hacking Victims Edge Into Light*, N.Y. TIMES, Feb. 21, 2013, at A1. But nevertheless, "[a] majority of companies that have at one time or another been the subject of news reports of online attacks refuse to confirm them." *Id.*

[86] *See generally* ROBERTA ROMANO, FOUNDATIONS OF CORPORATE LAW 600 (2d ed. 2010) ("The federally mandated disclosure . . . aims to enhance shareholders' ability to monitor management as well as the quality of their investment decisions.").

[87] *See* Young, *supra* note 27, at 660–61.

example, in early 2011, hackers gained unauthorized access to the computers of EMC Corporation—a publicly traded corporation whose subsidiary, RSA, produces digital encryption systems—and subsequently compromised the computer systems of clients who used RSA products, including the aerospace company Lockheed Martin, "extracting data and information of untold value."[88] Also in early 2011, hackers made news by stealing the personal information of over 100 million PlayStation game console users through a digital attack on Sony, Inc.,[89] the account numbers of over 200,000 Citigroup banking customers through an attack on Citigroup,[90] and "crucial governmental and national security information" from NASA through a cyber-attack.[91]

With cyber-attacks in the news, on May 11, 2011, Senator Rockefeller and four other Democratic members of the Senate Commerce, Science, and Transportation Committee wrote to then-SEC Chairwoman Mary Schapiro expressing concern over "the growing threat and the national security and economic ramifications of successful attacks against American businesses" and noting that "it is essential that corporate leaders know their responsibility for managing and disclosing information security risk."[92] They cited a 2009 survey that "found that 38 percent of Fortune 500 companies made a 'significant oversight' by not mentioning privacy or data security exposures in their public filings"[93] and referenced their own review of disclosures that found that statements ranged "from boilerplate descriptions of risk to details of specific attacks; [they] did not, however, find information on steps taken by the corporation[s] to reduce risk exposure."[94] Accordingly, they asked the SEC to "develop and publish interpretive guidance clarifying existing disclosure requirements pertaining to information security risk, including material information security breaches involving intellectual property or trade secrets."[95]

---

[88] *Id.* at 662–63.

[89] Bronstein, *supra* note 24, at 261; Liebowitz, *supra* note 73.

[90] Bronstein, *supra* note 24, at 261.

[91] *See id.* at 261–62; Liebowitz, *supra* note 73.

[92] Letter from John D. Rockefeller IV, Chairman, U.S. Senate Comm. on Commerce, Sci., & Transp. et al., to Mary Schapiro, Chairman, Sec. & Exch. Comm'n (May 11, 2011), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e. The other signatories were Senators Richard Blumenthal (D-CT), Robert Menendez (D-NJ), Mark Warner (D-VA), and Sheldon Whitehouse (D-RI). *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

The next day, seemingly unrelatedly, the White House unveiled proposed legislation called the Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act of 2011, to "enhance the cybersecurity of infrastructures [and] establish workable frameworks for implementing cybersecurity minimum standards" among other goals.[96] If enacted, it would have required public companies designated as "covered critical infrastructure"—defined as those assets that, if incapacitated, "would have a debilitating impact on national security, national economic security, national public health or safety"[97]—to certify in their annual public SEC reports, their development and implementation of a cybersecurity plan. Such disclosures were not supposed to "include proprietary information or other information indicating a critical weakness of the covered critical infrastructure."[98] Congress never acted on the proposed bill,[99] but it is telling that in mid-2011 the administration was thinking of how it could leverage SEC disclosure obligations to pursue cybersecurity goals.

Then-Chairwoman Schapiro responded to Senator Rockefeller's letter on June 6, 2011.[100] She noted that "existing disclosure requirements under the federal securities laws impose an obligation on public companies to disclose risks and events that a reasonable investor would consider important to an investment decision."[101] On the specifics of cyber-attacks, she couched her language in hypotheticals, noting various regulations "may require . . .

---

[96] *See* Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act § 2 (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cybersecurity-regulatory-framework-for-covered-critical-infrastructure-act.pdf; Letter from Jacob J. Lew, Dir., Office of Mgmt. & Budget, to John Boehner, Speaker of the House of Representatives (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Cybersecurity-letters-to-congress-house-signed.pdf; *see also* Benjamin A. Powell & Randolph D. Moss, *Obama Administration Proposes Cybersecurity Legislation*, WILMERHALE (May 17, 2011), http://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=95364 (describing the Obama administration's proposed cybersecurity legislation).

[97] Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act § 3(b).

[98] *Id.* § 7(a)–(c).

[99] *See generally* ROB STRAYER & DAVID BEARDWOOD, BIPARTISAN POLICY CTR., CYBER SECURITY LEGISLATION PRIVACY PROTECTIONS ARE SUBSTANTIALLY SIMILAR (2012), *available at* http://bipartisanpolicy.org/sites/default/files/Cyber%20Privacy%20Paper.pdf (discussing the four competing cyber security proposals from the Obama Administration, the House of Representatives, and the Senate).

[100] Letter from Mary Schapiro, Chairman, Sec. & Exch. Comm'n, to Sen. John D. Rockefeller IV, Chairman, U.S. Senate Comm. on Commerce, Sci., & Transp., (June 6, 2011), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=abb71f29-9439-45e8-a366-b9d95d8027de.

[101] *Id.*

disclosure regarding a prior cyber attack, a potential cyber attack, or the effects of a cyber attack."[102] Accordingly, "a company should consider whether cyber attacks and vulnerabilities present specific and material risks and should avoid generic risk factor disclosure that could apply to any company."[103] She also emphasized that "the [SEC] relies on a general materiality analysis in seeking additional disclosure in appropriate cases."[104] While she was "not aware that investors have asked for more disclosure in this area," she said she would "seriously consider" issuing guidance, as requested.[105]

Four months later, as promised, the Commission staff issued CF DG 2.

B. SEC Disclosure Requirements, Materiality Doctrine, and SEC Regulatory Tools

Before reviewing the structure and content of the guidance itself, let us review SEC disclosure requirements in general, the doctrine of materiality, and the arsenal of SEC regulatory tools. Following the Great Depression, Congress created the SEC, which is composed of five presidentially appointed and Senate-confirmed commissioners who each hold office for five years and a staff,[106] "to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation."[107] To that end, "[t]he resulting body of securities law establishes an elaborate system of mandatory disclosure requirements."[108] Section 14(a) of the Securities Exchange Act of 1934 empowers the SEC to require proxy disclosure "as necessary or appropriate in the public interest or for the protection of investors."[109] Specifically, the securities laws require all issuers of equity securities, registered with the SEC, to file annual (Form 10-K) and quarterly (Form 10-Q) reports.[110] The SEC also requires registered companies to report "material events" to

[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *See* 15 U.S.C. § 78d(a)-(b) (2012).
[107] *The Investor's Advocate*, *supra* note 35.
[108] Amy Deen Westbrook, *Sunlight on Iran: How Reductive Standards of Materiality Excuse Incomplete Disclosure Under the Securities Laws*, 7 HASTINGS BUS. L.J. 13, 17 (2011).
[109] 15 U.S.C. § 78n(b)(1) (2012).
[110] *See* 2 THOMAS LEE HAZEN, TREATISE ON THE LAW OF SECURITIES REGULATION § 9.3[1][A] (6th ed. 2009 & Supp. 2013); *Form 10-K*, U.S. SEC. & EXCH. COMM'N, http://www.sec.gov/answers/form10k.htm (last modified June 26, 2009); *Form 10-Q*, U.S. SEC. & EXCH. COMM'N, http://www.sec.gov/answers/form10q.htm (last modified Sept. 2, 2011).

their shareholders with Form 8-K.[111] Material events that require mandatory disclosure include: "bankruptcy," entry into or termination of "material definitive" agreements, amendments to the articles of incorporation, and the catchall "other events."[112] Another regulation, Regulation S-K, Item 503, "contains perhaps the most important disclosure requirements[:] risk factors associated with the issuer's business or the securities being distributed."[113] Such risk factors should state clearly "the risk . . . in plain English and avoid 'boilerplate' risk factors" while specifying how the particular risk affects the company.[114] Other important subparts of Regulation S-K require disclosures regarding a company's financial condition and future prospects[115] and "material pending legal proceedings, other than ordinary routine litigation incidental to the business."[116]

But what counts as material? "The basic dividing line between what has to be disclosed and what information may be withheld is determined by the concept of materiality."[117] The U.S. Supreme Court has held that "[a]n omitted fact is material if there is a substantial likelihood that a reasonable shareholder would consider it important,"[118] emphasizing that the omitted fact's "significance" must be evaluated in context of the total mix of investor information.[119] "Though this guidance is somewhat helpful, the materiality standard remains inherently subjective."[120] Some argue that courts have, and should, interpret materiality broadly, giving

---

[111] *Form 8-K*, U.S. SEC. & EXCH. COMM'N, http://www.sec.gov/answers/form8k.htm (last modified Aug. 10, 2012).

[112] *Id.*; HAZEN, *supra* note 110, § 9.3[1][B].

[113] HAZEN, *supra* note 110, § 9.4[9][C][2].

[114] *Id.*

[115] *Id.* § 9.4[7][C] (discussing the Management's Discussion and Analysis requirement).

[116] *Id.* § 9.4[5][C] (quoting 17 C.F.R. § 229.103 (2013)) (discussing the Pending Legal Proceedings disclosure requirement of Regulation S-K, Item 103).

[117] *Id.* § 3.4[2].

[118] TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976) (defining materiality in the context of proxy violations).

[119] Basic Inc. v. Levinson, 485 U.S. 224, 231–32 (1988) ("[The Court] now expressly adopt[s] the *TSC Industries* standard of materiality for the § 10(b) and Rule 10b-5 context."). This standard of materiality has been expanded to other sections of the securities laws. *See In re* Merck & Co., Inc. Sec. Litig., 432 F.3d 261, 274 (3d Cir. 2005) ("Sections 11 and 10(b) share the materiality element and the *TSC* [*Industries*] materiality definition."); Elfenbein v. Am. Fin. Corp., 487 F. Supp. 619, 627 (S.D.N.Y. 1980), *aff'd*, 652 F.2d 53 (2d Cir. 1981) ("[A] fact has been deemed material under sections 11 and 12(2) of the Securities Act when an investor would attach importance to it in making an investment decision.").

[120] Young, *supra* note 27, at 666. In 1999, the SEC tried to clarify materiality with "certain quantitative benchmarks" for those preparing financial statements and audits. SEC Staff Accounting Bulletin No. 99–Materiality, 64 Fed. Reg. 45150 (Aug. 19, 1999), *available at* http://www.sec.gov/interps/account/sab99.htm. Such a clarifying instruction has not been issued in the cybersecurity context.

the SEC a wide-ranging power to require disclosure, while others argue the materiality standard is "highly judgmental"[121] and its erosion deleterious.[122]

To exercise its legislative mandate to protect investors and maintain fair and orderly markets, including ensuring the disclosure of material information, the SEC can utilize a wide-range of policymaking tools. In an article on agency choice of policymaking form, M. Elizabeth Magill used the SEC's many options to illustrate the various instruments a typical administrative agency has to effectuate its policy ends.[123] If concerned about an illegal act, the SEC could, for example, "promulgate a legislative rule prohibiting the transaction. If valid, the rule would operate just like a statute; private parties would be required to refrain from engaging in the transaction or face sanctions."[124] Or, it could "bring an administrative enforcement action against an individual who has engaged in the transaction" that would bring the issue before an SEC adjudicator or a court.[125]

> Finally, the SEC might choose to provide guidance—for example, through congressional testimony, speeches, or a more formalized "release"—advising interested parties of its concerns about the transaction. Though it would surely influence the behavior of private actors, that guidance would be advisory only; it would not on its own have binding legal effect.[126]

With regard to legislative rules, the SEC follows a standard procedure for issuing such rules; typically, it first issues a concept release inviting public comment, then a proposed rule (also open for comment for one to two months), followed by a final rule after it is

---

[121] Richard C. Sauer, *The Erosion of the Materiality Standard in the Enforcement of the Federal Securities Laws*, 62 BUS. LAW. 317, 317 (2007).

[122] *Compare* Westbrook, *supra* note 108, at 37 ("[T]he SEC's statutory authority to require disclosure is broad."), *and* Cynthia A. Williams, *The Securities and Exchange Commission and Corporate Social Transparency*, 112 HARV. L. REV. 1197, 1207 (1999) (concluding that "the SEC has the authority to require expanded social disclosure under section 14(a) [and] should do so."), *with* Nicholas Kappas, Note, *A Question of Materiality: Why the Securities and Exchange Commission's Regulation Fair Disclosure is Unconstitutionally Vague*, 45 N.Y.L. SCH. L. REV. 651, 653 (2002) (arguing that Regulation Fair Disclosure is unconstitutionally vague), *and* Sauer, *supra* note 121, at 355 ("[M]ateriality . . . lies much in the eye of the beholder.").

[123] M. Elizabeth Magill, *Agency Choice of Policymaking Form*, 71 U. CHI. L. REV. 1383, 1384 (2004).

[124] *Id.*

[125] *Id.*

[126] *Id.*

approved by a majority of the Commission.[127]

Within the "guidance" category, the SEC issues a variety of documents under different titles that all essentially provide the staff's views of complex issues and carry a disclaimer that the information is advisory and not binding. For instance, Staff Accounting Bulletins provide the "staff's views regarding accounting-related disclosure practices."[128] Staff Legal Bulletins provide the "staff's views regarding various aspects of the federal securities laws and SEC regulations;"[129] furthermore, the SEC insists that "[b]ecause they represent the views of the staff, staff legal bulletins are not legally binding."[130] One scholar argues they "should be given deference when interpreting the law" although not "the precedential weight accorded to formal rulemaking."[131] The SEC staff also issues Compliance and Disclosure Interpretations that, it claims, are "not rules, regulations, or statements of the Commission."[132] Furthermore, "they are not binding due to their highly informal nature. Accordingly, these responses are intended as general guidance and should not be relied on as definitive."[133] The SEC also issues "No Action Letters" in response "to private requests for indication of whether certain contemplated conduct is in compliance with the appropriate statutory provisions and rules."[134] Like the other forms of guidance, such letters reflect staff interpretations and not action by the Commissioners,

> and thus have extremely limited, if any, precedential weight. The SEC staff position in a no action letter has been described as . . . "This is my view based on the facts as you describe them. You may not rely on it as if it were a Commission decision. If you don't like it, you are at liberty to disregard it . . . ."[135]

---

[127] *See The Investor's Advocate*, *supra* note 35 ("How the SEC Rulemaking Process Works.").

[128] *Selected Staff Accounting Bulletins*, U.S. SEC. & EXCH. COMM'N, http://www.sec.gov/interps/account.shtml (last modified Mar. 14, 2011).

[129] *Staff Legal Bulletins*, U.S. SEC. & EXCH. COMM'N, http://www.sec.gov/interps/legal.shtml (last modified Oct. 11, 2012).

[130] *Id.*

[131] HAZEN, *supra* note 34, § 1.4[3].

[132] *Compliance and Disclosure Interpretations*, U.S. SEC. & EXCH. COMM'N, http://www.sec.gov/divisions/corpfin/cfguidance.shtml (last modified May 30, 2013).

[133] *Id.*

[134] HAZEN, *supra* note 34, § 1.4[4].

[135] *Id.* (quoting Professional Care Services, Inc. [1973–74 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 79,770 at p. 84,080 (SEC No Action Letter March 15, 1974)).

C. The Structure of CF DG 2 Itself

Finally, in 2011, the SEC added to these many informal documents by releasing Corporation Finance Disclosure Guidance Topics, of which the cybersecurity disclosure guidance was only the second.[136] To date, the staff has issued only six such guidances;[137] the guidances are not published in the Federal Register. Nowhere has the SEC described the differences between a Disclosure Guidance Topic and the other litany of informal documents it issues to assist registrants in meeting their legal obligations.

CF DG 2 itself discusses six disclosure obligations: (1) Risk Factors; (2) Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A); (3) Description of Business; (4) Legal Proceedings; (5) Financial Statement Disclosures; and (6) Disclosure Controls and Procedures.[138]

Most corporate cyber disclosures discussed below fall under the "risk factors" obligation. The guidance states that a "registrant[] should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."[139] However, "registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure."[140] Recognizing the inherent tension in disclosing vulnerabilities, the guidance also notes that corporations should not disclose information that would "compromise" their cybersecurity.[141] Such disclosures may include "[d]iscussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks," corporate outsourcing that raises "material cybersecurity risks," descriptions of "cyber incidents experienced by the registrant," risks related to undetected cyber incidents, and descriptions of cyber insurance.[142]

Under MD&A, CF DG 2 advises registrants to disclose cyber-attacks if their costs or consequences "represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial

---

[136] *Division of Corporate Finance: Disclosure Guidance*, U.S. SEC. & EXCH. COMM'N, http://www.sec.gov/divisions/corpfin/cfdisclosure.shtml (last modified July 16, 2013).

[137] *Id.*

[138] CF DG 2, *supra* note 17.

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] *Id.*

condition. . . ."[143] For instance, "if material intellectual property is stolen in a cyber-attack, and the effects of the theft are reasonably likely to be material, the registrant should" disclose the attack and its financial effects.[144] CF DG 2 also recommends that registrants disclose cyber-attacks that "materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions," under the Description of Business obligation.[145] "[M]aterial pending legal proceeding[s]"[146] should be disclosed so long as a claim of damages exceeds "10 percent of the current assets of the registrant."[147]

Finally, CF DG 2 notes that "[c]ybersecurity risks and cyber incidents may have a broad impact on a registrant's financial statements, depending on the nature and severity of the potential or actual incident," and that registrants have a duty to report on the effectiveness of their disclosure procedures.[148]

At the top of the document, CF DG 2 carries an explicit disclaimer that it is not binding: "The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content."[149] Nevertheless, that distinction has been lost on some commentators who have described the guidance as "requiring public companies to disclose cybersecurity risks."[150]

Whether CF DG 2 imposes a requirement, instead of mere guidance, on registrants will be discussed in Parts V and VI. Next, we turn to why a requirement, instead of a simple statement by the SEC staff that "[t]his is my view," may run afoul of administrative law norms.

---

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] *Id.* & n.8.

[147] 17 C.F.R. § 229.103(5)(B) (2013). The CF DG 2 cross-references to Regulations S-K, Item 103, which includes the ten percent threshold. CF DG 2, *supra* note 17; Young, *supra* note 27, at 673.

[148] CF DG 2, *supra* note 17 ("For example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective.").

[149] *Id.*

[150] Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L. 313, 318 (2011); *see also* Reeves, *supra* note 79 (describing new SEC cybersecurity "requirements").

IV. LEGISLATIVE AND NONLEGISLATIVE RULES, INTERPRETIVE GUIDANCES, AND POLICY STATEMENTS

A federal regulation is a general statement issued by an administrative agency that has the force and effect of law, and the APA governs the rulemaking process through which such regulations are created.[151] Under the APA, a "rule" is any "agency statement of general or particular applicability and future effect designed to . . . interpret, or prescribe law or policy."[152] Rules themselves fall into two categories: "legislative rules" (occasionally referred to as "substantive rules") and "nonlegislative rules."[153] Legislative rules are "just like statutes passed by Congress" and "are legally binding on persons, and in many cases violations of these rules can subject a person to civil or criminal penalties."[154] "[A] legislative rule is the product of an exercise of delegated legislative power to make law through rules"[155] and must meet a number of requirements, including that it be developed through public notice and comment procedures[156] and published in the Federal Register.[157] Nonlegislative rules are any rules that do not conform to the requirements for legislative rules, and they in turn are classified as either "interpretive rules" (occasionally referred to as "interpretative rules") or "policy statements."[158] Whereas legislative rules "have the force and effect of law" interpretive rules "advise the public of the agency's construction of the statutes and rules which it administers," and policy statements "advise the

---

[151] *See generally* KEITH WERHAN, PRINCIPLES OF ADMINISTRATIVE LAW 158–65 (2008) (describing the function of the APA and how it differs from traditional rulemaking).

[152] 5 U.S.C. § 551(4) (2012).

[153] *See* Robert A. Anthony, *Interpretive Rules, Policy Statements, Guidances, Manuals, and the Like—Should Federal Agencies Use Them to Bind the Public?*, 41 DUKE L.J. 1311, 1321, 1321 n.37 (1992).

[154] Funk, *supra* note 30, at 1322.

[155] Anthony, *supra* note 153, at 1322 (internal citation omitted).

[156] 5 U.S.C. § 553(b–d).

[157] *Id.* §§ 552(a)(1), 553(b–d). Anthony has described the other requirements for a legislative rule as:

> 1) The agency must possess delegated statutory authority to act with respect to the subject matter of the rule. 2) Promulgation of the rule must be an intentional exercise of that delegated authority. 3) The agency must also possess delegated statutory authority to make rules with the force of law. 4) Promulgation of the rule must be an intentional exercise of the authority to make rules with the force of law. 5) Promulgation of the rule must be an effective exercise of that authority.

Anthony, *supra* note 153, at 1322.

[158] Anthony, *supra* note 153, at 1324; *see* Funk, *supra* note 30, at 1322.

public prospectively of the manner in which the agency proposes to exercise a discretionary power."[159]

Courts have had difficulty discriminating between legislative rules and interpretive rules or policy statements. The distinction "has been described at various times as 'tenuous,' 'fuzzy,' 'blurred,' and, perhaps most picturesquely, 'enshrouded in considerable smog.'"[160] For clarity, this article adopts the view of the late Robert A. Anthony, who looked to the rule's effect, not its title, when determining its nature.[161]

Under Anthony's framework, "[a]n interpretive rule is an agency statement that was not issued legislatively and that interprets language of a statute (or of an existing legislative rule) that has some tangible meaning."[162] To qualify as an interpretive rule, the issuance must not go "beyond a fair interpretation of existing legislation."[163] By contrast, "[a] policy statement is an agency statement of substantive law or policy, of general or particular applicability and future effect, that was not issued legislatively and is not an interpretive rule."[164] Regardless of "whether they are captioned . . . as policy statements or manuals or guidances or memoranda or circulars or press releases or even as interpretations," "[a]ll substantive nonlegislative issuances that are not interpretive rules are policy statements."[165]

Policy statements may look benign and cannot officially "bind," but "they may effectively coerce persons into compliance because of the fear of agency enforcement or adverse agency rulings in adjudications."[166] "[T]o an agency, if persons act on the basis of the general statements of policy, these statements may be almost as effective as legislative rules."[167] To judge whether a policy

---

[159] *See* Am. Mining Cong. v. Mine Safety & Health Admin., 995 F.2d 1106, 1109 (D.C. Cir. 1993) (quoting TOM C. CLARK, ATTORNEY GENERAL'S MANUAL ON THE ADMINISTRATIVE PROCEDURE ACT 30 n.3 (1947)).

[160] Cmty. Nutrition Inst. v. Young, 818 F.2d 943, 946 (D.C. Cir. 1987) (citations omitted); *see also Am. Mining Cong.*, 995 F.2d at 1108–10.

[161] Other scholars adopt different views. *See, e.g.*, E. Donald Elliott, *Re-Inventing Rulemaking*, 41 DUKE L.J. 1490, 1490 (1992) ("I believe that a court should not go behind the objective terms of a statement of agency policy to speculate about whether the statement was 'really intended' to bind the public.").

[162] Anthony, *supra* note 153, at 1325.

[163] *Id.* at 1326.

[164] *Id.* at 1325.

[165] *Id.* at 1326. Other sources have noted that policy statements are known as "'guidances,' 'memoranda,' 'manuals,' 'policy letters,' 'press releases,' 'staff instructions,' 'bulletins' and the like." WERHAN, *supra* note 151, at 253–54.

[166] Funk, *supra* note 30, at 1333.

[167] *Id.*

statement is being used as an impermissible legislative rule, courts ask: "Did the agency intend the document to bind? Has the agency given it binding effect? If the answer to either of these questions is 'yes,' the document should have been issued as a legislative rule."[168] To judge whether a document has had the practical effect of binding the public, courts look to see whether agencies have embarked on any enforcement action based on the document, whether the standards in the document have been regularly applied, or whether "private parties are reasonably *led to believe* that failure to conform will bring adverse consequences."[169] As the D.C. Circuit Court of Appeals held, "an agency pronouncement will be considered binding as a practical matter if it either appears on its face to be binding, or is applied by the agency in a way that indicates it is binding."[170]

Formally, CF DG 2 is a nonlegislative rule, not a legislative one; it claims not to bind the public, was not published in the Federal Register, and was not issued after a notice and comment period. Is it an interpretive rule or a policy statement? A policy statement "can look like an interpretive rule, and often agencies claim both exceptions when they are challenged for not having adopted a rule after notice and comment."[171] CF DG 2 states directly that it is "guidance" that provides the staff's "views regarding disclosure obligations," and it does not purport explicitly to "interpret" or construe the securities laws.[172] SEC and other government officials have continued to speak of it as guidance that informs the public of the SEC's views on important policy questions, like how to balance disclosure with necessary corporate secrecy.[173] In this way, CF DG

[168] Anthony, *supra* note 153, at 1327 (emphasis omitted). In *Pacific Gas & Electric v. Federal Power Commission*, a leading authority on the distinction between legislative rules and policy statements, the D.C. Circuit Court of Appeals looked at the intent of the agency when deciding how to classify its action. Pac. Gas & Elec. v. Fed. Power Comm'n, 506 F.2d 33, 39, 40 (D.C. Cir. 1974). While, in that case, the policy statement at issue was exempt from rule-making requirements, the court observed that if the agency had intended for it to "establish a binding rule of law not subject to challenge in particular cases," the policy statement would have been invalid as a non-legislative rule. *Id.* at 39.

[169] Anthony, *supra* note 153, at 1328; *see also* Chamber of Commerce of the United States v. OSHA, 636 F.2d 464, 468 n.7 (D.C. Cir. 1980) ("Courts often infer the intent behind an action from an action's foreseeable effects.") (vacating a practically binding OSHA rule for failing to follow notice and comment procedures) (citing Brown v. Califano, 627 F.2d 1221, 1234 n.79 (D.C. Cir. 1980) (citations omitted)).

[170] Gen. Elec. v. EPA, 290 F.3d 377, 383 (D.C. Cir. 2002) (referencing approvingly Anthony, *supra* note 153, at 1328–29) (citations omitted).

[171] Funk, *supra* note 30, at 1332.

[172] *See* CF DG 2, *supra* note 17.

[173] *See* Michael Bologna, *Official Urges Caution in Using Social Media to Disclose Material Data*, BNA, May 6, 2013, *available at* 45 SEC. REG. & L. REP. 819 (quoting May 2, 2013 speech by acting director of SEC's Division of Corporation Finance Lona Nallengara); Deputy Attorney

2 is similar to a speech an SEC staffer gave at a public conference about cybersecurity. Accordingly, this article concludes that CF DG 2 is a policy statement and analyzes it as such.[174]

V. THE IMPACT OF CF DG 2

In her response to Senator Rockefeller's April 2013 letter asking for the SEC to "elevate" the staff cybersecurity guidance, Chairwoman White defended the efficacy of CF DG 2 by noting that the SEC "staff issued comments addressing cybersecurity matters to approximately 50 public companies of varying size and in a wide variety of industries."[175] No law review article on CF DG 2 has critically analyzed those letters or the cyber disclosures they prompted.[176] This part attempts to address that lacuna through the analysis of ten case studies of corporate disclosures on cybersecurity, the ensuing SEC comments, and the subsequent corporate disclosures.[177] In *every* case, the target corporation altered the subsequent disclosure in a manner the SEC (acting with direct reference to CF DG 2) requested, even if the company protested initially that the disclosure was not material or necessary. Notably, even after the SEC prompted action, most of the disclosures themselves were general and vague.

General James M. Cole, Address at the Georgetown Cybersecurity Law Institute (May 23, 2013), *available at* http://www.justice.gov/iso/opa/dag/speeches/2013/dag-speech-130523.html (describing sensitivity of corporate information related to SEC cybersecurity "guidance").

[174] Interpretive rules are allowed greater latitude than policy statements "to make a substantive nonlegislative rulemaking document binding on private parties . . . so long as it stays within the fair intendment of the statute." Anthony, *supra* note 153, at 1313. While this article argues for the reasons described above that CF DG 2 is a policy statement and not an interpretive rule, even if it were the latter, there is reason to think it would be still be impermissible, since it does not "spell[] out a duty fairly encompassed within the [law or] regulation that the interpretation purports to construe [in this case, cyberattacks that are not material]." Paralyzed Veterans of Am. v. D.C. Arena L.P., 117 F.3d 579, 588 (D.C. Cir. 1997).

[175] White Letter, *supra* note 26.

[176] Two newswire stories deserve mention. One reviews two cyber disclosures and mentions several others, although it does not go into detail about them. Linda Sandler, *SEC Guidance on Cyber-Disclosure Becomes Rule for Google*, BLOOMBERG (Aug. 29 2012), http://www.bloomberg.com/news/2012-08-29/sec-guidance-on-cyber-disclosure-becomes-rule-for-google.html. Another news article, from early 2012, argues that many companies with known breaches "have said nothing about the incidents in their regulatory filings" but, again, does not describe such disclosures. Joseph Menn, *Exclusive: Hacked Companies Still Not Telling Investors*, REUTERS (Feb. 2, 2012), http://www.reuters.com/article/2012/02/02/us-hacking-disclosures-idUSTRE8110YW20120202.

[177] All the annual and quarterly reports and comment letters analyzed here are available through the SEC's website. *Reports*, U.S. SEC. & EXCH. COMM'N (Aug. 7, 2013), http://www.sec.gov/about/secreports.shtml.

A. Case Studies

This article reviews each case study in turn.

1. Amazon.com

A leader in Internet retail, Amazon.com has a market capitalization of about $170 billion, 117,000 employees, and 2012 revenues of over $60 billion.[178] The online shoe portal Zappos.com—dubbed a "shoe utopia" by the press[179]—is a subsidiary of Amazon's. Recently, there was trouble in paradise: in January 2012, an unknown perpetrator infiltrated Zappos' internal computer network through servers housed in Shepherdsville, Kentucky and may have had "illegal and unauthorized access" to customer account information, including customers' names, e-mail addresses, billing and shipping addresses, phone numbers, the last four digits of their credit card numbers, and their "cryptographically scrambled password[s]."[180] The episode garnered significant press and spurred class action suits for a litany of civil wrongs.[181]

A few weeks later, Amazon filed its standard Annual Report (Form 10-K) with the SEC. It made only vague references to the potential of cyber intrusions that "*could* expose us or our customers to a risk of loss or misuse of [personal] information, adversely affect our operating results, result in litigation or potential liability for us and otherwise harm our business."[182] The report made no mention of the intrusion that had just occurred and triggered lawsuits.

The SEC replied to Amazon's Annual Report and cited the recent news that, far from a mere hypothetical intrusion, a cyber-attack on its Zappos subsidiary had "occurred during which millions of user accounts were compromised"; accordingly, it asked the company to "please address whether disclosure" in its 10-K of such an attack

[178] *Amazon.com, Inc. Company Profile*, CNNMONEY, http://money.cnn.com/quote/profile/profile.html?symb=AMZN (last visited Mar. 6, 2014).

[179] Alexandra Jacobs, *Happy Feet*, NEW YORKER, SEPT. 14, 2009, at 66.

[180] Tony Hsieh, *Security Email*, ZAPPOS.COM (Jan. 15, 2012), http://blogs.zappos.com/securityemail (explaining cyberattack and company's immediate remediation measures to employees, including the email subsequently sent to customers).

[181] *See* David Goldman, *Zappos Hacked, 24 Million Accounts Accessed*, CNNMONEY (Jan. 16, 2012, 11:33 AM), http://money.cnn.com/2012/01/16/technology/zappos_hack/index.htm; Complaint at 1–2, 10–14, Stevens v. Amazon.com, Inc., No. 3:12-cv-00032 M (W.D. Ky. Jan. 16, 2012). In June 2012, a multi-district panel consolidated the Stevens case with similar litigation in the District of Nevada, where Zappos.com is headquartered. Transfer Order at 1357–59, *In re* Zappos.Com, Inc., Customer Data Security Breach Litigation, 867 F. Supp. 2d 1357 (June 13, 2012), MDL No. 2357.

[182] Amazon.com, Inc., Annual Report (Form 10-K), at 10 (Feb. 1, 2012) (emphasis added).

was necessary to advise possible investors of all potential harm to its business, including "reputational damage affecting customer or investor confidence."[183] To support its request for greater disclosure, the SEC cited CF DG 2.[184]

At first Amazon protested, claiming that "information on the specific incident would not provide investors with additional material information relating to the cyber-attack risks facing our business," that the attack had no material impact on Amazon, and that any impact on Zappos would be "transitory."[185] Undeterred, the SEC again pressed Amazon to "expand" its 10-K "to disclose that you have experienced cyber-attacks and breaches" in a second letter the following month.[186] This time, Amazon obliged. It wrote in its next filing that some of its subsidiaries "had past security breaches, and, although they did not have a material adverse effect on our operating results, there can be no assurance of a similar result in the future."[187] It is unclear what effect, if any, Amazon's subtle word change had on shareholders' investment decisions.

2. American International Group (AIG)

AIG was once the world's largest insurer[188] and has "customers in more than 130 countries."[189] In its 2011 Annual Report it wrote that its many data systems "could . . . be subject to unauthorized access, such as physical or electronic break-ins or unauthorized tampering." It also noted that "[i]n some cases, such unauthorized

[183] Letter from William H. Thompson, Accounting Branch Chief, Sec. & Exch. Comm'n, to Shelly Reynolds, Vice President and Worldwide Controller, Amazon.com, Inc. (Mar. 12, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1018724/000000000012012577/filename1.pdf.

[184] *Id.* ("Please tell us what consideration you gave to including expanded disclosure consistent with the guidance provided by the Division of Corporation Finance's Disclosure Guidance Topic No. 2.").

[185] Letter from Shelly Reynolds, Vice President and Worldwide Controller, Amazon.com, Inc., to William H. Thompson, Accounting Branch Chief, Sec. & Exch. Comm'n (Apr. 9, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1018724/000119312512155627/filename1.htm.

[186] Letter from William H. Thompson, Accounting Branch Chief, Sec. & Exch. Comm'n, to Shelly Reynolds, Vice President and Worldwide Controller, Amazon.com, Inc. (Apr. 18, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1018724/000000000012019757/filename1.pdf.

[187] Amazon.com, Inc., Quarterly Report (Form 10-Q), at 34 (July 27, 2012).

[188] *See* Reuters, *No Deposition of Bernanke in A.I.G. Lawsuit, Court Says*, N.Y. TIMES (Oct. 16, 2013), http://www.nytimes.com/2013/10/17/business/economy/no-deposition-of-bernanke-in-aig-lawsuit-court-says.html.

[189] *American International Group Inc.*, N.Y. TIMES, http://topics.nytimes.com/top/news/business/companies/american_international_group/index.html (last visited Mar. 6, 2014).

access may not be immediately detected. This may impede or interrupt our business operations and could adversely affect our consolidated financial condition or results of operations."[190]

The SEC responded several weeks later and asked directly "whether you have experienced attacks, unauthorized access, systems failures and disruptions in the past and, if so, whether disclosure of that fact would provide the proper context for your risk factor disclosures." It directed AIG to "[p]lease refer" to CF DG 2.[191]

AIG responded with an air of incredulity. "Like other global companies, AIG has experienced threats to its data and systems, including malware and computer virus attacks, unauthorized access, systems failures and disruptions. The nature of these incidents is not unique to AIG," it wrote.[192] But, "[n]one of the incidents to date, nor the costs or other consequences associated with such incidents, has *materially* affected AIG's business or consolidated financial position or results of operations."[193] It also had procedures in place to notify affected individuals and the government, when necessary, of the unauthorized access of personal information. "Based on these procedures and in light of its experience to date, AIG does not believe that disclosure of the specific facts and circumstances of the incidents to date would provide useful context to its risk factor disclosures."[194]

In a second letter, the SEC seized on AIG's admission—probably taken for granted by most major firms—that it had "experienced threats to [its] data and systems, including malware and computer virus attacks" and pressed again for greater disclosure.[195] "In order to place the risks described in this risk factor in an appropriate context, please expand your risk factor to state that you have experienced [such] threats . . . ."[196]

AIG subsequently relented. "Pursuant to the Staff's comment,

---

[190] Am. Int'l Grp., Inc., Annual Report (Form 10-K), at 41 (Feb. 23, 2012).

[191] Letter from Jim B. Rosenberg, Senior Assistant Chief Accountant, Sec. & Exch. Comm'n, to Robert H. Benmosche, President and Chief Exec. Officer, Am. Int'l Grp., Inc. (Apr. 5, 2012), *available at* http://www.sec.gov/Archives/edgar/data/5272/000000000012017580/filename1.pdf.

[192] Letter from Kathleen E. Shannon, Senior Vice President and Deputy Gen. Counsel, Am. Int'l Grp., Inc., to Jim B. Rosenberg, Senior Assistant Chief Accountant, Sec. & Exch. Comm'n (Apr. 18, 2012), *available at* http://www.sec.gov/Archives/edgar/data/5272/000119312512168967/filename1.htm.

[193] *Id.* (emphasis added).

[194] *Id.*

[195] Letter from Jeffrey P. Riedler, Assistant Dir., Sec. & Exch. Comm'n, to Robert H. Benmosche, President and Chief Exec. Officer, Am. Int'l Grp., Inc. (May 9, 2012), *available at* http://www.sec.gov/Archives/edgar/data/5272/000000000012024184/filename1.pdf.

[196] *Id.*

AIG will expand its risk factor on electronic data systems and the handling of confidential information in" future filings to include an expanded disclosure, it wrote.[197] The new language reads in its entirety: "Like other global companies, we have, from time to time, experienced threats to our data and systems, including malware and computer virus attacks, unauthorized access, systems failures and disruptions."[198] Upon review, the statement seems self-evident.

3. Anheuser-Busch InBev

Headquartered in Brussels, Belgium, Anheuser-Busch InBev is the world's largest brewing company.[199] As a foreign corporation, it files a Form 20-F with the SEC, which is functionally equivalent to a Form 10-K.[200] In the Form 20-F it filed in 2012, Anheuser-Busch spoke in the future subjunctive: "our information systems *may* be vulnerable to a variety of interruptions due to events beyond our control" which could "disrupt our business."[201] The SEC was not satisfied with such disclosures and asked that, "[i]f you have experienced any cyber-attacks, security breaches or other similar events in the past, in future filings, beginning with your next Form 20-F, please confirm that you will state that fact in order to provide the proper context for your risk factor disclosure."[202]

Anheuser-Busch pushed back in a response letter. As far as it knew, "the Company has not experienced any material breaches of cybersecurity . . . and believes its risk factors, as currently drafted, adequately describe the nature of the risks the Company faces relating to cybersecurity."[203] In reply, the SEC—not comfortable

---

[197] Letter from Kathleen E. Shannon, Senior Vice President, Am. Int'l Grp., Inc. to Jeffery P. Reidler, Assistant Dir., Sec. & Exch. Comm'n (May 21, 2012), *available at* http://www.sec.gov/Archives/edgar/data/5272/000119312512242072/filename1.htm.

[198] *Id.*; *see also* AIG, Quarterly Report (Form 10-Q), at 185 (Aug. 2, 2012).

[199] *Company Information: Anheuser-Busch InBev N.V.*, N.Y. TIMES, http://topics.nytimes.com/top/news/business/companies/anheuser-busch-inbev-nv/index.html (last visited Mar. 7, 2014); *About Anheuser-Busch*, ANHEUSER-BUSCH.COM, http://anheuser-busch.com/index.php/our-company/about-anheuser-busch/ (last visited Mar. 7, 2014).

[200] *SEC Form 20-F*, INVESTOPEDIA.COM, http://www.investopedia.com/terms/s/sec-form-20-f.asp (last visited Mar. 7, 2014).

[201] Anheuser-Busch InBev SA/NV, Annual Report (Form 20-F), at 16 (Apr. 13, 2012) (emphasis added).

[202] Letter from John Reynolds, Assistant Dir., Sec. & Exch. Comm'n, to Felipe Dutra, Chief Fin. Officer, Anheuser-Busch Inbev SA/NV (Aug. 17, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1140467/000000000012044902/filename1.pdf (advising the company to "[p]lease refer" to CF DG 2).

[203] Letter from Martim Della Valle, Legal Dir., Anheuser-Busch Inbev SA/NV, to John Reynolds, Assistant Dir. Sec. & Exch. Comm'n (Aug. 31, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1140467/000119312512376987/filename1.htm.

merely providing its view and letting the company determine for itself what to disclose—noted that, from the company's response, "it appears that you have experienced and expect to continue experiencing *attempted* breaches of your technology systems," and, if so, it asked the company to state as much in its next filing.[204] Anheuser-Busch then relented. Appended to the bottom of its next Form 20-F was a blanket statement that the company "experience[s] from time to time attempted breaches of our technology systems" and expected those to continue, although "[n]one of the attempted breaches on our systems (as a result of cyber-attacks, security breaches or similar events) had a material impact on our business . . . ."[205]

What is striking is that unlike AIG, which at least admitted that some cyber-attacks had been successful, Anheuser-Busch claimed that none had been and agreed to disclose—vaguely and nonspecifically—merely attempted attacks, even though the attacks themselves were purportedly not "material." In light of the depth and breadth of the global cyber-attacks discussed *supra* it strains one's imagination that no such attacks on Anheuser-Busch have been successful, but there is no admission in the disclaimer to the contrary.

4. ConocoPhillips, Inc.

ConocoPhillips is a global oil and gas company that in 2011 reported revenue of over $237 billion.[206] A company of such size and scope faces a number of exposures, and in the Annual Report it filed with the SEC in February 2012 it listed "cyber-attacks" as the last among many "hazards and risks that require significant and continuous oversight."[207] In response, the SEC wrote ConocoPhillips and asked it to "provide a separate discussion of the

[204] Letter from John Reynolds, Assistant Dir., Sec. & Exch. Comm'n, to Felipe Dutra, Chief Fin. Officer, Anheuser-Busch Inbev SA/NV (Sept. 11, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1140467/000000000012049546/filename1.pdf (emphasis added).

[205] Anheuser-Busch InBev SA/NV, Annual Report (Form 20-F), at 19 (Mar. 25, 2013); *see also* Anheuser-Busch InBev SA/NV Letter from Martim Della Valle, Legal Dir., Anheuser-Busch Inbev SA/NV, to John Reynolds, Assistant Dir. Sec. & Exch. Comm'n (Sept. 24, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1140467/000119312512401513/filename1.htm (relenting to SEC's request).

[206] *Fortune 500 Ranking: ConocoPhillips*, CNNMONEY, http://money.cnn.com/magazines/fortune/fortune500/2012/snapshots/327.html (May 21, 2012) (ranking it America's fourth largest corporation).

[207] ConocoPhillips, Annual Report (Form 10-K), at 33 (Feb. 21, 2012).

risks posed to your operations . . . by cyber-attacks" and pointed it to CF DG 2 "for additional information."[208]

Like AIG and Anheuser-Busch, ConocoPhillips at first resisted. "We have reviewed . . . [CF DG 2] and believe the Company's current disclosures regarding the risks relating to its cybersecurity are appropriate in light of the Company's business, size and experience with cybersecurity and cyber incidents." While, it has experienced "occasional" breaches, "none of those breaches has had a material effect on our business, operations or reputation."[209]

The SEC renewed its request in a subsequent letter, asking ConocoPhillips to describe "risks posed to your operations from your dependence upon technology . . . in order to provide the proper context for your risk factor disclosure" as well as the fact that it had experienced "occasional actual and attempted" cyber breaches.[210] ConocoPhillips capitulated a month later, agreeing to the SEC's request.[211] In its following quarterly filing, it added a sentence to its previous disclosure of hazards and risks to say that it had experienced occasional breaches but that none had "material effect on our business."[212]

5. Eastman Chemical

Eastman Chemical "is a global specialty chemicals company that produces a [broad] range of advanced materials, chemicals and fibers" in sixteen countries.[213] It has a market capitalization of about $13 billion and over $9 billion in annual revenue.[214] The Form 10-K it filed in 2012 was similar to other disclosures we have reviewed. It mentioned "cyber-attacks" among one of many

[208] Letter from H. Roger Schwall, Assistant Dir., Sec. & Exch. Comm'n, to Jeff W. Sheets, Chief Financial Officer, ConocoPhillips (July 20, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1163165/000000000012038537/filename1.pdf.

[209] Letter from Jeff W. Sheets, Chief Fin. Officer, ConocoPhillips, to H. Roger Schwall, Assistant Dir., Sec. & Exch. Comm'n (Aug 3, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1163165/000119312512333820/filename1.htm.

[210] Letter from H. Roger Schwall, Assistant Dir., Sec. & Exch. Comm'n, to Jeff W. Sheets, Chief Fin. Officer, ConocoPhillips (Sept. 26, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1163165/000000000012052931/filename1.pdf.

[211] Letter from Jeff W. Sheets, Chief Fin. Officer, ConocoPhillips, to H. Roger Schwall, Assistant Dir., Sec. & Exch. Comm'n (Oct. 10, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1163165/000119312512419596/filename1.htm.

[212] ConocoPhillips, Quarterly Report (Form 10-Q), at 56 (Oct. 20, 2012).

[213] *Business Day: Eastman Chemical Company*, N.Y. TIMES, http://topics.nytimes.com/top/news/business/companies/eastman_chemical_company/index.html (last visited Mar. 6, 2014).

[214] *Eastman Chemical Co.: Key Statistics*, YAHOO! FINANCE, http://finance.yahoo.com/q/ks?s=EMN (last visited Mar. 6, 2014).

potential "disruptions"—including "pandemic illness" and "terrorism"—that "*could* have a material adverse effect on the Company's sales revenue, costs, results of operations, and financial condition."[215]

In its comment letter, the SEC took the unusual step of referencing "recent public statements" by an information technology employee of the company discussing the importance of cybersecurity for the chemical sector.[216] It asked for more information on "what consideration you gave to tailoring your risk factor disclosure to more clearly address such threats" and asked, as it had with other companies, whether Eastman had suffered actual attacks, "and, if so, address whether disclosing that fact would provide the proper context for investors considering these risk disclosures."[217] In response, Eastman noted that the employee was "a non-management employee" and that it had "implemented and maintained systems to protect against cyber-attacks and cybersecurity breaches."[218] Any cyber breaches to date had not had "a material adverse effect" and, therefore, "the Company believes it has provided appropriate disclosure to investors of potential risks."[219]

The SEC disagreed, noting that it should acknowledge those attacks, even if they were not material.[220] Eastman relented and added a single sentence to its following quarterly report doing so.[221]

---

[215] Eastman Chem. Co., Annual Report (Form 10-K), at 63 (Feb. 22, 2012) (emphasis added).

[216] Letter from Pamela Long, Assistant Dir., Sec. & Exch. Comm'n, to Theresa K. Lee, Senior Vice President, Eastman Chem. Co. (May 2, 2012), *available at* http://www.sec.gov/Archives/edgar/data/915389/000000000012022648/filename1.pdf; Jim Montague, *Security Prevents Unauthorized Access*, CONTROL DESIGN (Feb. 9, 2012), http://www.controldesign.com/articles/2012/network-security-prevents-unauthorized-access.html (discussing speech by Mark Heard, "cybersecurity lead" for Eastman).

[217] Letter from Pamela Long, *supra* note 216.

[218] Letter from Scott V. King, Vice President, Controller & Chief Accounting Officer, Eastman Chem. to Pamela K. Long, Assistant Dir., Sec. & Exch. Comm'n (May 16, 2012) *available at* http://www.sec.gov/Archives/edgar/data/915389/000119312512236826/filename20.htm.

[219] *Id.*

[220] Letter from Pamela Long, Assistant Dir., Sec. & Exch. Comm'n, to Theresa K. Lee, Senior Vice President, Eastman Chem. Co. (May 21, 2012) *available at* http://www.sec.gov/Archives/edgar/data/915389/000000000012026294/filename1.pdf.

[221] Eastman Chem. Co., Quarterly Report (Form 10-Q), at 52 (Aug. 2, 2012) ("The Company has in the past had cyber attacks and breaches of its computer information systems, none of which has had a material adverse effect on the Company's operations."); *see also* Letter from Scott V. King, Vice President, Controller & Chief Accounting Officer, Eastman Chem. to Pamela K. Long, Assistant Dir., Sec. & Exch. Comm'n (May 22, 2012), *available at* http://www.sec.gov/Archives/edgar/data/915389/000119312512243687/filename1.htm.

6. Google

In January 2010, Google made news when it disclosed that hackers based in China had raided the company's networks.[222] It reported that breach to the SEC in a "Current Report" (Form 8-K) filed in January 2010, well before CF DG 2 was issued.[223] The Annual Report the company issued in January 2012 made only tentative statements about cybersecurity, referencing (as had the other companies here reviewed) what would happen "[i]f our security measures are breached."[224] The SEC invoked CF DG 2 when asking Google to revise its disclosure to reference the 2010 attack "to provide the proper context for your risk factor disclosures."[225] Google agreed, and in its subsequent disclosures, it noted that it "experience[s] cyber-attacks of varying degrees on a regular basis, and . . . unauthorized parties have obtained, and may in the future obtain, access to our data . . . [possibly resulting in] an adverse effect on our business."[226]

7. Hartford Financial Services Group

An insurance and financial services company, Hartford Financial Services Group has a market capitalization of about $16 billion.[227] In the Annual Report it filed in February 2012, it spoke of future, possible cyber "security incident[s]" that could "compromise[]" its ability to conduct business.[228] The SEC responded by asking whether it had ever been the subject of a cyber-attack and pointed to CF DG 2 for more information.[229] Hartford demurred, responding

---

[222] *See* Andrew Jacobs & Miguel Helft, *Google May End Venture in China Over Censorship*, N.Y. TIMES, Jan. 13, 2010, at A1. For general information on Google, the Internet services behemoth, see generally *Google Inc. (GOOG.O) Company Profile,* REUTERS, http://www.reuters.com/finance/stocks/companyProfile?symbol=GOOG.O (last visited Mar. 7, 2014) (describing, among other things, the company's products and services).

[223] Google Inc., Current Report (Form 8-K), at 2, ex. 99.1 (Jan. 13, 2010).

[224] Google Inc., Annual Report (Form 10-K), at 15 (Jan. 26, 2012).

[225] Letter from Maryse Mills-Apenteng, Special Counsel, Sec. & Exch. Comm'n, to Larry Page, Chief Exec. Officer, Google, Inc. (May 2, 2012) *available at* http://www.sec.gov/Archives/edgar/data/1288776/000000000012022687/filename1.pdf.

[226] Google, Inc., Quarterly Report (Form 10-Q), at 54–55 (July 24, 2012).

[227] *Hartford Financial Services Group–Company Information*, N.Y. TIMES, http://topics.nytimes.com/top/news/business/companies/hartford_financial_services_group_inc/index.html (last visited Mar. 6, 2014).

[228] Hartford Fin. Servs. Grp., Inc., Annual Report (Form 10-K), at 25 (Feb. 24, 2012).

[229] Letter from Jim B. Rosenberg, Senior Assistant Chief Counsel, Sec. & Exch. Comm'n, to Christopher J. Swift, Exec. Vice President & Chief Fin. Officer, Hartford Fin. Servs. Grp. (Apr. 5, 2012), *available at* http://www.sec.gov/Archives/edgar/data/874766/000000000012017492/filename1.pdf.

unequivocally that it had "not experienced a material breach of cybersecurity" and saying that its disclosures were consistent with CF DG 2.[230]

In another letter, the SEC pressed again: "[D]espite the fact you believe you have not experienced a material breach of your cybersecurity, are you currently experiencing attacks or threats to your systems?"[231] It also asked that Hartford expand on the risk factor if it had experienced "attacks" (the SEC did not say "material attacks") in the past.[232] Hartford subsequently yielded and expanded its filings to include reference to past and future cyber-attacks that could occur, while noting that it "has not experienced a material breach of cybersecurity."[233]

8. Quest Diagnostics

Quest Diagnostics is a medical testing company with a market capitalization of about $10 billion.[234] Its 2011 Annual Report made especially vague references to the vulnerabilities of its information technology, warning that, "despite the security measures we have implemented, our IT systems may be subject to physical or electronic intrusions, computer viruses, unauthorized tampering and similar disruptive problems."[235] The SEC responded, asking if the company had ever experienced a cyber-attack, "[g]iven your extensive use of information technology systems," and, "if so, whether disclosure of that fact would provide the proper context for your risk factor disclosures."[236]

Quest initially tried to argue with the SEC. "The Company

[230] Letter from Beth A. Bombara, Senior Vice President & Controller, Hartford Fin. Servs. Grp., Inc., to Jim B. Rosenberg, Senior Assistant Accountant, Sec. & Exch. Comm'n (Apr. 18, 2012), *available at* http://www.sec.gov/Archives/edgar/data/874766/000119312512168405/filename1.htm.

[231] Letter from Jeffrey Riedler, Assistant Dir., Sec. & Exch. Comm'n, to Christopher J. Swift, Exec. Vice President & Chief Fin. Officer, Hartford Fin. Servs. Grp. (May 7, 2012), *available at* http://www.sec.gov/Archives/edgar/data/874766/00000000012023723/filename1.pdf.

[232] *Id.*

[233] Letter from Beth A. Bombara, Senior Vice President & Controller, Hartford Fin. Servs. Grp., Inc., to Jeffrey Riedler, Assistant Dir., Sec. & Exch. Comm'n (May 16, 2012), *available at* http://www.sec.gov/Archives/edgar/data/874766/000119312512236210/filename1.htm.

[234] *Quest Diagnostics Inc.*, REUTERS, http://www.reuters.com/finance/stocks/overview?symbol=DGX (last visited Mar. 7, 2014).

[235] Quest Diagnostics Inc., Annual Report (Form 10-K), at 24 (Feb. 16, 2012).

[236] Letter from John Reynolds, Assistant Dir., Sec. & Exch. Comm'n, to William J. O'Shaughnessy, Jr., Assistant Gen. Counsel & Corporate Sec'y, Quest Diagnostics Inc. (Apr. 18, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1022079/00000000012019754/filename1.pdf.

respectfully advises the Staff that the Company's information technology systems have not sustained any attacks, viruses, intrusions or similar problems that have materially disrupted, interrupted, damaged or shutdown the Company's information technology systems,"[237] Quest wrote. It also quoted the language of CF DG 2 that directed registrants to "avoid generic risk factor disclosure."[238] In response, the SEC dispensed with the issue of materiality: "[P]lease tell us whether you have experienced any attacks, viruses, intrusions or similar problems in the past," they wrote.[239] And, if so, Quest should include language that the attacks were mitigated.[240]

Quest relented, and its later filings included the admission that, its "information technology systems from time to time have experienced minor attacks . . . but each was mitigated, and none materially disrupted . . . the Company's information technology systems . . . ."[241]

9. Verizon

"[A] provider of communications, information and entertainment products and services," Verizon Communications, Inc. has a market capitalization of about $140 billion.[242] In its 2011 filing, Verizon, like many other companies, listed cyber-attacks as one of many threats that "may . . . disrupt[ ] . . . our operations."[243] The SEC asked that Verizon disclose in its next quarterly filing if it ever

[237] Letter from William J. O'Shaughnessy, Jr., Assistant Gen. Counsel & Corporate Sec'y, Quest Diagnostics Inc., to John Reynolds, Assistant Dir., Sec. & Exch. Comm'n (Apr. 30, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1022079/000094787112000403/filename1.htm.

[238] *Id.* (quoting CF DG 2, *supra* note 17).

[239] Letter from John Reynolds, Assistant Dir., Sec. & Exch. Comm'n, to William J. O'Shaughnessy, Jr., Assistant Gen. Counsel & Corporate Sec'y, Quest Diagnostics Inc. (May 15, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1022079/00000000012025327/filename1.pdf.

[240] *Id.*

[241] Quest Diagnostics Inc., Annual Report (Form 10-K), at 26 (Feb. 27, 2013); *see also* Letter from William J. O'Shaughnessy, Jr., Assistant Gen. Counsel & Corporate Sec'y, Quest Diagnostics Inc., to John Reynolds, Assistant Dir., Sec. & Exch. Comm'n (May 25, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1022079/000094787112000461/filename1.htm (conceding to SEC direction).

[242] *Verizon Communications Inc., Company Information,* N.Y. TIMES, http://topics.nytimes.com/top/news/business/companies/verizon_communications_inc/index.html (last visited Mar. 7, 2014).

[243] Verizon Commc'ns Inc., Annual Report (Form 10-K), at 16 (Feb. 24, 2012).

actually experienced an attack.[244] Verizon objected, arguing that such a disclosure was more appropriate for a 10-K, Annual Report, since a 10-Q "requires the inclusion of 'any *material* changes from risk factors as previously disclosed.'"[245] The suggested revision, Verizon said, was not a material change, since the attacks were not material.[246] SEC pressed again, noting that Verizon had implicitly acknowledged that it had previously been the subject of cyber-attacks (even if they were unsuccessful) and they had not disclosed that to their investors, so a 10-Q filing was appropriate.

Verizon retracted its objections and included in its next 10-Q the admission, that "[w]hile, to date, we have not been subject to cyber-attacks or other cyber incidents which, individually or in the aggregate, have been material to our operations or financial condition, . . . [major cyber-attacks or similar] occurrences could result in a material adverse effect."[247]

10. Wyndham Worldwide

Wyndham is a hotel and hospitality company with a large international presence and a market capitalization of about $8 billion.[248] In June 2012, the U.S. Federal Trade Commission (FTC) sued the company in federal court alleging unfairness and deception-based violations of Section 5 of the FTC Act in connection with three data breach incidents involving a group of Wyndham brand hotels.[249] Wyndham noted the litigation, which it contested and claimed would be immaterial, in a 10-Q filed in July 2012.[250] In an August 2012 letter, the SEC asked the company to acknowledge that it had experienced successful data breaches in the past "to

[244] Letter from Larry Spirgel, Assistant Dir., Sec. & Exch. Comm'n, to Robert J. Barish, Senior Vice President and Controller, Verizon Commc'ns Inc. (Aug. 27, 2012), *available at* http://www.sec.gov/Archives/edgar/data/732712/000000000012046448/filename1.pdf.

[245] Letter from Robert J. Barish, Senior Vice President and Controller, Verizon Commc'ns Inc., to Larry Spirgel, Assistant Dir., Sec. & Exch. Comm'n (Sept. 10, 2012), *available at* http://www.sec.gov/Archives/edgar/data/732712/000119312512386470/filename1.htm.

[246] *Id.*

[247] Verizon Commc'ns Inc., Quarterly Report (Form 10-Q), at 42 (Oct. 25, 2012); *see also* Letter from Robert J. Barish, Senior Vice President and Controller, Verizon Commc'ns Inc. to Larry Spirgel, Assistant Dir., Sec. & Exch. Comm'n (Oct. 2, 2012) *available at* http://www.sec.gov/Archives/edgar/data/732712/000119312512412737/filename1.htm (agreeing to SEC's direction).

[248] *Wyndham Worldwide Corp.*, BLOOMBERG BUSINESSWEEK, http://investing.businessweek.com/research/stocks/snapshot/snapshot.asp?ticker=WYN (last visited Mar. 7, 2014).

[249] Wyndham Worldwide Corp., Quarterly Report (Form 10-Q), at 19 (July 25, 2012).

[250] *Id.*

provide the proper context for your risk factor disclosure."[251] Wyndham agreed without argument and inserted a sentence into its October 2012 10-Q noting that it did not think the data breach was "material."[252] The insertion of the clause about the immateriality of the data breach was the only substantive, cyber-related difference between the July 2012 10-Q and the October 2012 one.

B. General Observations

Several general themes arise from these case studies. First, every request for disclosure came with an explicit reference to CF DG 2. Second, the SEC found that subjunctive references to potential future attacks were insufficient when the company did not make some reference to past breaches. Third, the materiality limitation was of little concern to the SEC; even when firms claimed that they had suffered no material attack or seen any material adverse consequences, the SEC continued to insist on disclosure. Fourth, every company surveyed changed its disclosures at the SEC's prodding, usually following a kind of Kabuki exchange, in which the SEC would question the initial 10-K, the company would object to including more information because no attack has been material or materially adverse, the SEC would renew its request, and the company would concede, agreeing to include an additional sentence or two. Fifth, the disclosures that the SEC eventually found satisfactory are remarkably similar across industries and businesses—a typical one includes an acknowledgement of past breaches (even if they were not material), a reference to the potential for future ones, and some statement about efforts to mitigate or insure against the risk of greater threats.

VI. ANALYSIS

A. CF DG 2 Overreaches

The evidence presented above shows that, procedurally, CF DG 2

---

[251] Letter from Jennifer Gowetski, Senior Counsel, Sec. & Exch. Comm'n, to Thomas G. Conforti, Chief Fin. Officer, Wyndham Worldwide Corp. (Aug. 1, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1361658/000000000012041213/filename1.pdf.

[252] Wyndham Worldwide Corp., Quarterly Report (Form 10-Q), at 48 (Oct. 24, 2012); *see also* Letter from Thomas G. Conforti, Chief Fin. Officer, Wyndham Worldwide Corp., to Jennifer Gowetski, Senior Counsel, Sec. & Exch. Comm'n (Aug. 13, 2012) *available at* http://www.sec.gov/Archives/edgar/data/1361658/000119312512355506/filename1.htm (agreeing to follow SEC guidance).

overreaches. While it claims to be merely guidance, it functions much like a legislative rule, compelling the behavior of private entities. Four factors suggest strongly that CF DG 2 crosses the line from policy statement to legislative rule.

First and most important, CF DG 2 has the "effect of binding the public *as a practical matter*."[253] And "a binding policy is an oxymoron."[254] As shown in Part V, private companies could not say "no" to cybersecurity disclosure requests from the SEC. Even when they objected—as did ConocoPhillips, Eastman, Hartford Financial, and others—every firm eventually capitulated to the disclosure sought. The SEC did not merely offer its view and let the registrants decide for themselves what to say, but it insisted (repeatedly) that registrants "please expand" their discussions of cyber threats. In light of the SEC's enforcement power, "there are sinews of command beneath the velvet words of . . . the guidelines."[255] Regardless of the written niceties, corporations recognize that "[r]esisting a letter from the SEC can be costly."[256] Writing memos to argue the finer points of administrative regulation takes time and money in legal fees. "It's easier to put a line in your 10-Q, if you're told to disclose something," a former SEC lawyer and now professor said. "The SEC knows that's their power."[257]

Second, the SEC has used CF DG 2 in such a way as to expand the reach of the securities laws by essentially ignoring the materiality requirement. The SEC comment letters brushed aside questions of materiality; any real or potential attack (regardless of whether there was "a substantial likelihood that a reasonable shareholder would consider it important")[258] was reason enough for a disclosure, even if the disclosure itself was evasive.[259] As discussed below, the "anything qualifies" disclosure requirement led to overly vague disclosures. "[O]ver-disclosure also serves to reduce the transparency of corporate disclosure. As former SEC Chairman Harvey Pitt has complained, 'People have to wade through a morass of garbage to finally get to the few nuggets that are contained

---

[253] Anthony, *supra* note 153, at 1328.

[254] Viet. Veterans of Am. v. Sec'y of the Navy, 843 F.2d 528, 537 (D.C. Cir. 1988).

[255] Am. Trucking Assoc. v. Interstate Commerce Comm'n, 659 F.2d 452, 463 (5th Cir. 1981), *cert denied*, 460 U.S. 1022 (1983) (invalidating administrative rules).

[256] Sandler, *supra* note 176.

[257] *Id.*

[258] TSC Indus., v. Northway, Inc., 426 U.S. 438, 449 (1976) (defining materiality in the context of proxy violations).

[259] *See supra* Part V.A.

there . . . ."[260] Under this broad reading of materiality, whether information is objectively material no longer matters, since "perception of what is material becomes reality. As a result, public companies must be more transparent and share information with investors that they previously may not have felt it prudent to disclose or publicize in order to satisfy this broad definition."[261] A Microsoft attorney has opined that the ambiguous articulation of materiality "would likely continue to obscure compliance with the staff guidance" since materiality is always "contextual."[262] As discussed *infra*, the substantive disagreement about materiality is the kind of thing that a notice and comment process could help resolve.[263]

Third, the context in which the SEC issued CF DG 2 suggests that the SEC may have intended for the guidance to do the work of a legislative rule. As discussed in Part III, CF DG 2 was issued after a series of high-profile hacks, in response to Congressional inquiry, and after the White House had introduced a bill that would have mandated similar disclosures from certain companies.[264] While there is no evidence that the guidance was issued purposefully to dodge notice and comment rulemaking requirements, it stands to reason that CF DG 2 tried to do what a legislative rule would have done, had such rules materialized.

Fourth, after the SEC staff issued CF DG 2, private parties were "reasonably *led to believe* that failure to conform will bring adverse consequences."[265] As discussed, *supra*, backers of stronger cybersecurity trumpeted CF DG as "fundamentally alter[ing] th[e] equation" of security and corporate responsibility.[266] Even those who recognized that as staff guidance it was not formally binding

---

[260] Sauer, *supra* note 121, at 355.

[261] Crisler, *supra* note 28.

[262] John Curran, *Panelists Handicap Cyber Bill Pace, NIST Progress*, TR DAILY, May 23, 2013.

[263] Some argue that "materiality is not always needed" to force disclosure, especially when information is disclosed to satisfy Regulation S-K risk factors. Westbrook, *supra* note 108, at 24. But not only would such a view open the floodgates for meaningless disclosures, it is also contradicted by CF DG 2, which—when describing risk factors—says that "[c]onsistent" with Regulation S-K, the "cybersecurity risk disclosure provided must adequately describe the nature of the *material* risks and specify how each risk affects the registrant." CF DG 2, *supra* note 17 (emphasis added).

[264] *See supra* Part III.A.

[265] Anthony, *supra* note 153, at 1328; *see also* Chamber of Commerce of the United States v. Occupational Safety & Health Admin., 636 F.2d 464, 469 n.7 (D.C. Cir. 1980) ("Courts often infer the intent behind an action from an action's foreseeable effects."). The Court vacated a practically binding OSHA rule for failing to follow notice and comment procedures. *Id.*at 471.

[266] Rockefeller & Chertoff, *supra* note 23, at A19.

warned that it would impose requirements. For instance, one law firm noted that "contrary to many commentators' suggestions," the guidance was not mandatory, but still wrote that there was "no doubt" that the guidance would "be relied upon in enforcement proceedings and by plaintiffs' counsel in litigation."[267]

For these reasons, despite CF DG 2's formal label as "guidance," the lack of any SEC enforcement action based on noncompliance, and the SEC's broad authority to require disclosure of relevant information, CF DG 2 is properly understood as an impermissible legislative rule. In practical effect, it exceeds the bounds of policy guidance.

B. CF DG 2 Underachieves

Even though CF DG 2 crosses the boundary between nonlegislative and legislative rule by compelling private companies to disclose information, ironically, the resulting disclosures fail to meet the substantive policy goals underlying the guidance. CF DG 2 underachieves because the disclosures it prompts are essentially boilerplate descriptions of cyber-attacks that are likely already assumed by most educated investors aware of the news.[268] The guidance asks registrants to tailor their disclosures "to their particular circumstances and avoid generic 'boilerplate' disclosures,"[269] but that has turned out to be hollow aspiration, as Quest Diagnostics discovered while objecting to SEC requests that it discuss immaterial information.[270] CF DG 2 underachieves partly because of the nonspecific information the SEC requests, partly because of what companies are willing to disclose, and partly because of the out-sized expectations for what the SEC can do through its disclosure authority to prompt greater corporate cybersecurity. In short, it is far easier for a company to place formulaic language in its SEC filings about the generalized danger of a cyber-attack than to buttress IT systems or adopt best practices

---

[267] *SEC Issues Disclosure Guidance on Cybersecurity Matters and Cyber Incidents*, HUNTON & WILLIAMS 1 (Oct. 19, 2011), http://www.huntonprivacyblog.com/wp-content/uploads/2013/03/sec_issues_disclosure_guidance_on _cybersecurity.pdf (citing *In re* Heartland Payment Sys., Inc. Sec. Litig., Civ. No. 09-1043, 2009 U.S. Dist. LEXIS 114866, *3–4, *23 (D.N.J. Dec. 7, 2009)); *see* BALTZ ET AL., *supra* note 28, at 1, 4 (explaining CF DG 2 guidelines "do not create any new disclosure obligations" but "are [likely] only the beginning of a trend towards increased cybersecurity regulation"); *see also* Crisler, *supra* note 28 ("[CF DG 2] establishes new responsibilities for corporations").

[268] *See supra* Part V.A.

[269] CF DG 2, *supra* note 17.

[270] *See supra* Part V.A.8.

that could be costly and cumbersome from a user's perspective.

The guidance suffers from three main flaws. First, CF DG 2 fails to resolve the information asymmetry at which the disclosure laws are aimed. "In a well ordered society, or market, making information publicly available is the best way to ensure good behavior."[271] And yet, the nebulous cybersecurity disclosures may not be sufficient to promote "good" cybersecurity behavior. The cybersecurity disclosures prompted by the guidance are of such similarity across industries and corporations that they indicate little useful information is coming to the market. If the disclosure rules were generating valuable information, one would expect greater variance in the disclosures between, say, an Internet retailer, an insurance company, and a healthcare company—and yet the cybersecurity disclosures of Amazon, AIG, and Quest Diagnostics are strikingly similar.[272] As noted, this may be in part due to the ambiguity surrounding materiality, which complicates identifying what disclosures are appropriate. It may even make it easier for companies to skirt their responsibilities by making everything material, because then nothing is, and, as former SEC Chairman Pitt might say, it is hard to tell the wheat from the chaff.

Second, CF DG 2 fails to resolve the so-called "Hobson's choice"[273] of how much detail to disclose about past cyber-attacks without disclosing too much. If a company discloses too much, it risks inviting more attacks or weakening the protection of third-parties. If a company discloses too little, the SEC could use CF DG 2 to prompt more disclosure. The guidance lacks specifics on how to make that determination and, despite recent efforts to encourage registrants to "call" the SEC if they have questions about handling cyber disclosures,[274] such outreach is probably less effective than clear, prior direction. As the evidence shows, CF DG 2 incentivizes just enough disclosure to comply with the guidance but not enough

---

[271] Westbrook, *supra* note 108, at 17.

[272] Amazon.com, Inc., Quarterly Report (Form 10-Q), at 34 (July 27, 2012) ("Some subsidiaries had past security breaches, and, although they did not have a material adverse effect on our operating results, there can be no assurance of a similar result in the future."); Am. Int'l Grp., Inc., Quarterly Report (Form 10-Q), at 185 (Aug. 2, 2012) ("Like other global companies, we have, from time to time, experienced threats to our data and systems, including malware and computer virus attacks, unauthorized access, systems failures and disruptions."); Quest Diagnostics, Inc., Annual Report (Form 10-K), at 26 (Feb. 27, 2013) ("[F]rom time to time [our IT systems] have experienced minor attacks, minor viruses, attempted intrusions or similar problems, like other major companies, but each was mitigated, and none . . . materially disrupted the Company's performance").

[273] Trope & Hughes, *supra* note 82, at 4.

[274] Bologna, *supra* note 173.

to provide meaningful information to other firms hoping to secure their networks. It is curious that in the Zappos case more information about the hack was released online on the CEO's blog than in the 10-K filing. That suggests that something intervened between the initial company response and the filing the SEC prompted—perhaps jittery corporate counsel—that decided it was in the company's interest to address the attack vaguely in the 10-K.[275]

Third, and finally, despite the practically binding nature of the guidance, it is unclear how many companies are providing even these minimal cybersecurity disclosures in their releases. According to Chairwoman White, only fifty companies, of the thousands that the SEC regulates, have received comment letters.[276] A legislative rule—backed by the unequivocal threat of enforcement—could trigger more consistent and more uniform disclosure (even if the disclosures are suboptimal). For a counterexample, consider the reported success of a new disclosure rule regarding companies' Iran-related activities. Such disclosures are mandated by the 2012 Iran Threat Reduction and Syria Human Rights Act, which requires public companies to disclose in their annual and quarterly filings and in special notices if they "knowingly" engaged in certain activities or dealings with Iran.[277] According to the SEC, in less than two months, 168 companies issued the notices required by the rule, which, as a part of an act of Congress, is a formal, legislative rule.[278] CF DG 2 has achieved comparatively weak results.

For these reasons, CF DG 2 substantively underachieves.

VII. RECOMMENDATIONS AND IMPLICATIONS

In light of this evidence and analysis, the SEC should rescind CF DG 2 and issue stronger cybersecurity disclosure guidance not as staff guidance but as a legislative rule approved by the SEC Commissioners after a period of notice and comment. Not only would such a move address CF DG 2's procedural flaw, but it would also result in better policy, more likely bringing the right kind of information to the marketplace. Notice and comment rulemaking would primarily promote fact-finding that could inform the policy,

---

[275] *See supra* Part V.A.1 and accompanying notes.

[276] White Letter, *supra* note 26.

[277] Iran Threat Reduction and Syria Human Rights Act of 2012, Pub. L. No. 112-158, § 219, 126 Stat. 1214, 1235–36 (2012).

[278] Yin Wilczek, *Disclosure: SEC Offers Statistics on New Disclosures Relating to Issuers' Iran-Related Activities*, 45 SEC. REG. & L. REP. (BNA) 655 (Apr. 15, 2013).

especially around materiality and the balance of releasing not enough or too much information. It would also likely promote acceptability among regulated entities and greater consistency, much like the Iran-related disclosure rule.

The purpose of notice and comment "is both (1) to allow the agency to benefit from the expertise and input of the parties who file comments with regard to the proposed rule, and (2) to see to it that the agency maintains a flexible and open-minded attitude towards its own rules . . . ."[279] Mariano-Florentino Cuéllar has shown that agencies actually take into account public comments; in his studies, "[a]gencies made substantial modifications . . . in response to comments,"[280] and that informational benefit would be especially pronounced in a technologically new and evolving area like cybersecurity. For instance, other federal agencies have recently turned to notice and comment when developing proposed rules to enhance cybersecurity, recognizing the importance of soliciting public expertise in this field.[281]

The SEC has followed such an open process before when dealing with novel areas of disclosure. In one recent example, the SEC engaged in an extensive notice and comment period when developing a rule requiring companies to disclose their use of conflict minerals from central Africa; the Commission received over 250 comments and hosted a roundtable discussion with interested parties.[282] Comments concerned "the definition of 'conflict minerals' . . . the need for a *de minimus* exception, and the necessary due diligence required, among other matters."[283] The SEC "incorporated many changes from the proposal that are designed to address concerns about the costs,"[284] and even though some commentators criticized the rule,[285] it is worth contemplating how much "worse" the rule could have been if the SEC had not moderated it in response to public input.

---

[279] Nat'l Tour Brokers Ass'n, v. United States, 591 F.2d 896, 906 (D.C. Cir. 1978).

[280] Mariano-Florentino Cuéllar, *Rethinking Regulatory Democracy*, 57 ADMIN. L. REV. 411, 498 (2005) (describing findings on the impact of public comments on regulatory rulemaking from three case studies).

[281] *See, e.g.*, Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition, 78 Fed. Reg. 27966, 27967 (proposed May 7, 2013).

[282] Press Release, U.S. Sec. & Exch. Comm'n, SEC Adopts Rule for Disclosing Use of Conflict Minerals (Aug. 22, 2012), *available at* http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171484002.

[283] Celia R. Taylor, *Conflict Minerals and SEC Disclosure Regulation*, 2 HARV. BUS. L. REV. ONLINE 105, 108 n.18 (2012).

[284] Press Release, *supra* note 282.

[285] Taylor, *supra* note 283, at 105–06.

With regard to cybersecurity, comments from regulated entities could be especially useful when addressing the issues of materiality and the depth of appropriate disclosures. As for materiality, one proposal in the academic press is for the SEC to set "a dollar threshold for cyber-attack prevention costs, mitigation costs, and losses that, if individually or collectively exceeded, automatically requires disclosure."[286] Notice and comment would be a useful tool for determining where that threshold would be.

This article has been critical of milquetoast disclosures that speak so broadly of cyber-attacks so as to lose any real value. However, in fairness, it is difficult to determine if or how companies should report minor intrusions that may at some later date pose a material hazard. Consider the example of an intellectual property hack from a foreign country like China. Perhaps such a cyber-attack gained only limited access to a single computer and did not seem to steal anything of import. However, suppose the stolen data turns out to be much more valuable than previously thought and, a decade later with the proper development, the Chinese perpetrator is able to enter a U.S. market and drive out the American competition with technology derived from the small, immaterial hack years before. There is no easy answer to resolving such a quandary, but the collective knowledge of the private sector may help point to a solution.

It is also worth noting that the SEC is essentially asking for public comments now, but only after the issuance of the guidance. SEC officials have publicly encouraged registrants to give them feedback on CF DG 2, telephone them with questions,[287] and provide greater input on the "sources of cyber-attacks, and why some attacks go unnoticed . . . [in this] evolving area."[288] Such outreach is a sign of commendable bureaucratic openness, but it also suggests that some of these complex issues would be well addressed through public engagement before, and not after, the guidance's issuance.

With regard to acceptability, cybersecurity disclosure issues, like "[t]he vast majority of regulatory questions simply cannot be resolved without making value choices and policy trade-offs."[289] One way to build support for those trade-offs is to engage in an open

[286] Young, *supra* note 27, at 677 (also proposing a "'percentage of assets' threshold where disclosure is required").

[287] Bologna, *supra* note 173.

[288] Wilczek, *supra* note 278.

[289] Cuéllar, *supra* note 280, at 497–98.

and honest discourse with the public.[290] Anthony has asked: "Especially in view of the important values served by legislative rulemaking—enrichment of the agency's information and enhancement of the rule's acceptability, flowing from the public's opportunity to present facts and views—can it credibly be argued that unilaterally issued guidances or memoranda can possess the same force?"[291] The obvious answer is no.

In addition to this specific recommendation, the experience of CF DG 2 has three broader, doctrinal implications. First, the evidence here both supports, and provides a counterexample to, the work of Conor N. Raso.[292] While Raso uses empirical data to argue that "[a]gencies do not commonly use guidance to make important policy decisions outside of the notice and comment process,"[293] CF DG 2 provides an example of where an agency did use a guidance document to further an important policy end, even if it did so imperfectly. Raso also argues that the advantages of using guidance documents to further policy outside of notice and comment "increases when Congress and the President are divided."[294] The story of CF DG 2 supports that claim. Here, the SEC faced pressure from Congress (specifically Senator Rockefeller) and from the White House (whose 2011 bill would have demanded similar disclosures) but Congressional Republicans made consensus on cybersecurity legislation impossible.[295] Without a clear mandate, the SEC did the best it could. Further, Raso argues that "concern over agency abuse of guidance is overwrought."[296] While CF DG 2 provides a complicating case study, one could argue that the procedural overreach in CF DG 2 can be overstated. At the end of the day, perhaps all that the SEC guidance has prompted is a few more sentences in financial disclosure documents and a few more hours of billing time for corporate counsel. CF DG 2 may not have lived up to the high expectations of its policy champions, but neither has its practical binding effect lead to catastrophic ends for private sector

---

[290] *See, e.g.*, Natural Res. Def. Council, Inc. v. United States EPA, 824 F.2d 1258, 1285 (1st Cir. 1987) ("Had the EPA opened a new comment period when they promulgated this never before proposed or foreshadowed rule, a significant number of the complaints that are before us now could have been resolved by the Agency either by amending the rule or by adequately explaining why the commenters' suggestions were not adopted.").

[291] Anthony, *supra* note 153, at 1356.

[292] Raso, *supra* note 30, at 782.

[293] *Id.* at 821.

[294] *Id.* at 801.

[295] *See supra* Part III.A.

[296] Raso, *supra* note 30, at 822.

freedom.

Second, the experience with CF DG 2 demonstrates how political paralysis can lead to agency creativity. As noted above, the failure of the White House and the Congress to act coherently on cybersecurity legislation left the SEC at loose ends. It faced pressure from its Congressional overseers, the Senate Commerce Committee, to do something to promote corporate cybersecurity and inform investors of the risks. But it lacked the direction and (without legislative rulemaking) the authority to address the issue. As a result, the staff used a relatively new tool—CF DG 2 was only the second "Disclosure Guidance" the SEC had issued—to prompt action without requiring it. In short, the SEC tried to solve a policy problem by essentially pouring new wine (cybersecurity disclosures) into old bottles (disclosure rules based on "materiality"). As this analysis shows, CF DG 2 is an example of how "[p]olitical decision making has moved to peripheral public entitles" in the face of legislative gridlock.[297] But even if the SEC's policy was creative, it was procedurally and substantively lacking.

There are other examples of creative policymaking that have borne sweeter fruit. For instance, Senator Rockefeller, frustrated by what he considered continued corporate stonewalling on cybersecurity, simply wrote to the CEOs of the *Fortune* 500 companies and asked them to advise him of their cybersecurity efforts.[298] Reportedly, he received substantive responses from 300 companies,[299] making his effort at cybersecurity policymaking outside of the typical legislative process far more successful than the SEC staff's.

Third and finally, the experience with CF DG 2 suggests the limits of the convergence between economic security and national security. The literature on the intersection of these two concepts is large and growing,[300] and the ideas have permeated high-level

---

[297] Robert B. Reich, Op-Ed., *The Real Price of Congress's Gridlock*, N.Y. TIMES, Aug. 14, 2013, at A23.

[298] *See, e.g.*, Letter from Sen. John D. Rockefeller IV, Chairman, Senate Comm. on Commerce, Sci., & Transp., to Virginia M. Rometty, President. & Chief Exec. Officer, Int'l Bus. Mach. (Sept. 19, 2012), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=396eb5d5-23a4-4488-a67c-d45f62bbf9e5.

[299] Jennifer Martinez, *Rockefeller: Fortune 500 Companies Back Voluntary Cybersecurity Standards*, THE HILL (Jan. 30, 2013), http://thehill.com/blogs/hillicon-valley/technology/280085-rockefeller-staff-memo-finds-fortune-500-companies-ok-with-cybersecurity-best-practices#ixzz2Uu9Lk37e.

[300] *See generally* C. R. NEU & CHARLES WOLF, JR., THE ECONOMIC DIMENSIONS OF NATIONAL SECURITY, at xi (1994) ("Economic Security is the ability to protect or to advance

policymaking.[301] It is difficult to quibble with the underlying observation that economic strength leads to national strength.[302] But that insight does little to address the inherent, practical hurdles of trying to use institutions designed for one problem (in this case, financial risk associated with the Great Depression) to address another (maintaining American competitiveness in a world in which digital thieves can abscond with intellectual property that took generations to develop and milliseconds to lose).

This is not to say that corporations should not protect against cyber threats—indeed, they should. But relying on SEC disclosure authority to try to force them to do so has not been shown to be an effective method. Disclosure regulations deal with only one aspect of the problem (are companies acknowledging cyber-attacks that are evident to anyone who reads the news?), without addressing the heart of the matter: helping private sector companies develop the IT systems and best practices that will protect their data. The institutionally optimal way of addressing the cyber threat would rely upon the strengths of the more traditional security agencies—such as the Department of Homeland Security and the Federal Bureau of Investigation—and upon the technical and scientific expertise resident in organizations like the National Institute of Standards and Technology, among others. That Congress has failed to give those parts of the federal bureaucracy the direction and authority they need to address this policy goal is an unfortunate reminder that while some may recognize an intellectual truth (i.e., the merging of economic and national security) they may be unwilling to take the practical steps needed to align institutions to meet those new challenges.

Furthermore, heaping ever-growing requirements on the SEC dilutes its core mission. It is an increasingly common occurrence. Recently, either because of legislative direction or on its own, the

U.S. economic interests in the face of events, developments, or actions that may threaten or block these interests."); Mariano-Florentino Cuéllar, *"Securing" the Nation: Law, Politics, and Organization at the Federal Security Agency, 1939-1953*, 76 U. CHI. L. REV. 587, 708 (2009) (describing the history of a "thick" notion of security, noting it "finds resonance in the concerns of international organizations, advocates, and governance reformers with 'human security' as an alternative to narrowly tailored conceptions of physical security."); Jessica Tuchman Mathews, *Redefining Security*, 68 FOREIGN AFF. 162, 162–63 (1989) (describing evolution of definition of security from the late- to post-Cold War).

[301] *See generally* THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES 9 (2010) (describing overlap between national security and economic and domestic prosperity).

[302] *See generally* PAUL KENNEDY, THE RISE AND FALL OF THE GREAT POWERS: ECONOMIC CHANGE AND MILITARY CONFLICT FROM 1500 TO 2000, at xv, xxii (1987) (arguing this point).

SEC has weighed-in on disclosure responsibilities related to climate change, Iran, conflict minerals, and other issues.[303] As laudable as those policy goals are, policing disclosures of such a wide-range of issues brings the SEC further away from its traditional competencies. One reason notice and comment is important when the SEC seeks to regulate these kinds of behaviors is because so little of the staff knows anything about them, and it is difficult to offer sensible regulation in an unknown field. For instance, when developing the conflict minerals rule, the "SEC staff freely spoke of the SEC's lack of expertise regarding conflict minerals and other sustainability-related disclosures . . . ."[304]

Properly conceived, the SEC's authority is limited, tethered to requiring the disclosure of information that is "material," and extends only so far as the APA allows through the legislative rulemaking process. As the experience with cybersecurity disclosures demonstrates, efforts to leverage disclosure rules to further other public policy goals can meet with limited success, with uncertain benefits to both the markets and society.

VIII. CONCLUSION

The SEC's cybersecurity disclosure guidance has escaped serious analysis until now. Using case studies and paying particular attention to the comment letters that the SEC sent registrants to prompt greater disclosure, this article concludes that the guidance both procedurally overreaches and substantively underachieves.

It overreaches because, while it is facially a nonlegislative rule, it has had the practical effect of binding private conduct as if it were a legislative one. It underachieves because the disclosures it requires are vague, similar across industries and companies, and bring little information to the marketplace. In particular, it fails to resolve the information asymmetry problem at which the disclosure laws are aimed. To resolve these defects, the Commission should elevate cybersecurity disclosure guidance and issue it as a legislative rule, after a notice and comment period. Notice and comment rulemaking would contribute to sounder policy by allowing stakeholders to offer their expertise and experience at the front-end

[303] *See supra* Parts VI and VII; Press Release, U.S. Sec. & Exch. Comm'n, SEC Issues Interpretive Guidance on Disclosure Related to Business or Legal Developments Regarding Climate Change (Jan. 27, 2010), *available at* http://www.sec.gov/news/press/2010/2010-15.htm; Westbrook, *supra* note 108, at 26.

[304] Taylor, *supra* note 283, at 106 n.5.

of the rulemaking process, enriching the agency's information and enhancing the rule's acceptability, instead of after-the-fact, which is largely what is happening now, as the SEC staff elicits comments from registrants trying to comply with the guidance.

The experience with CF DG 2 offers a counterexample to those who say that agencies do not commonly use guidance documents to make important policy decisions outside of the notice and comment process. It also suggests the limits of agency creativity during periods of political ossification. Finally, it challenges the simple verity that economic security and national security have merged. While they may have joined in theory, in the practice of day-to-day governing, they have not, and, when it comes to cybersecurity, Congress and the public would do well to expect more from the traditional national security bureaucracy and less from the economic one.