SEC CYBERSECURITY GUIDELINES:
INSIGHTS INTO THE UTILITY OF RISK FACTOR DISCLOSURES FOR INVESTORS

Edward A. Morse, Vasant Raval, John R. Wingender
Creighton University
Omaha, Nebraska

ABSTRACT

In October 2011, the SEC issued new guidelines for disclosure of cybersecurity risks. Some firms responded to these guidelines by issuing new risk factor disclosures. This paper examines the guidelines and cybersecurity disclosures in the context of existing laws governing securities regulation. It then examines empirical results from firm disclosures following the new guidelines. Evidence shows a relatively small proportion of firms chose to modify their risk factor disclosures, with most firms choosing not to disclose any specific cybersecurity risk. Moreover, disclosing firms generally experienced significant negative stock market price effects on account of new disclosures. Rather than viewing disclosure a positive signal of management attentiveness, investors apparently viewed it as a cautionary sign.

Contents

I. Introduction.

Business information (including customer data, proprietary information, or other sensitive financial information) is an attractive target for malefactors seeking to exploit its value or inflict economic harm through inappropriate access, use or disclosure. Corporate managers are expected to consider cybersecurity risks as part of their duty to secure business assets.[1]

Previous research has demonstrated that *ex post* disclosures of data security breaches correlate strongly to negative stock price movements and that these effects can linger over reasonably long-term time horizons.[2] A breach disclosure likely represents new information entering the marketplace that could cast a shadow on the firm's economic prospects. Factors such as erosion of customer goodwill, reduced investor confidence in management's ability to secure the firm's assets, and exposure to transaction costs associated with resolving claims may explain negative effects on stock prices.[3]

This article considers a distinct but related issue: whether *ex ante* disclosures of cybersecurity risks can also impact stock prices. On October 13, 2011, the Division of Corporation Finance of the U.S. Securities and Exchange Commission issued guidance expressing the Division's views on "disclosure obligations relating to cybersecurity risks and cyber incidents". [4] That guidance, which is neither a rule, regulation or statement of the SEC,[5] was intended to "assist[] registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant's specific facts and circumstances." [6]

Although other rules may obligate firms to disclose material cybersecurity risks in particular contexts,[7] some publicly traded companies added new disclosures following the issuance of this new guidance.[8] This change in reporting practices provides an opportunity to assess the impact of new voluntary disclosures on the disclosing firms.

---

[1] Of course, non-electronic data storage media can also present security concerns. See, e.g., Peter Sloan, The Reasonable Information Security Program, 21 RICH J. L. & TECH 2, 11 (2014) (noting federal laws requiring protection against unauthorized access in connection with the disposal of consumer information). However, the ubiquity of electronic information storage has created special concerns that have dominated the discussion of information security. On the matter of securing business assets, see, e.g., 15 U.S.C.A. § 78m(b)(2) (requiring that "access to assets is permitted only in accordance with management's general or specific authorization")

[2] See Edward Morse, Vasant Raval, & John Wingender, Market Price Effects of Data Security Breaches, 20 INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE 263 (Taylor & Francis 2011).

[3] See id.

[4] Division of Corporation Finance, U.S. Securities & Exchange Commission, CF Disclosure guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (last visited August 4, 2015) [Hereinafter 2011 Cybersecurity Guidance].

[5] See id. As will be discussed below (see notes 66-67, *infra*), this qualification is significant because of the fact that silence is an option under federal securities laws unless disclosure is required.

[6] Id.

[7] See id. at note 3 (citing SEC rules and case law).

[8] As discussed in part III.C., below, while a significant number of firms issued new disclosure, such firms reflect only a small fraction of the total firm population in any given industry. Disclosing firms thus appear to be outliers in this sense.

We examined Form 10-K, Form 10-Q, and Form 8-K disclosures of publicly traded companies from the year preceding and following October 13, 2011, in order to identify companies that issued new cybersecurity risk disclosures following the SEC guidance. We catalogued the language used to make this disclosure, along with the date that it was first published, in order to perform an event study to investigate whether any market price effects could be discerned on account of this new disclosure. As discussed below, we found a significant negative impact on market price associated with the disclosing event.

We also examined SEC comment letters related to its October 13, 2011 guidance, which were issued to registrants or prospective registrants between February 2012 and August 2014. We reviewed 68 letters from firms that responded to SEC questions concerning their compliance with the guidance. Most of these letters (54 or about 79.4%) addressed either Form 10-K disclosures or Form 20-F disclosures, which are required annually. Other responses (13 or about 19%) addressed forms for registering new securities, including Form DRS and Forms S-1 or S-1A; one response involved Form DEF 14A, which is connected to proxy solicitation.

These exchanges between the SEC and registered firms provide additional insights into the kind of information that the SEC is seeking from registered firms. While most firms have chosen to remain silent because of the absence of any perceived material impact from cybersecurity problems, other firms appear to be moving toward including bland, boilerplate discussion of such risks as a means to avoid controversy with the SEC. If this path is followed, it does not bode well for the utility of the current disclosure framework. Bland disclosures could also enhance risks for firms, to the extent that such disclosures may arguably provide fuel for investor claims of material misrepresentation based on changing conditions within the firm.

This discussion is organized as follows. Part II provides an overview of the role of disclosure in federal securities law and the parameters for disclosure in the October 13, 2011 guidance. Part III looks at the legal consequences for errors and omissions in disclosure and their effects upon disclosure behavior, including the potential for over-disclosure in a manner that, ultimately, may provide limited or no utility for the investing community. Part IV provides a more detailed look at empirical results from our examination of company disclosures and the associated effects on stock price. Finally, part V provides concluding comments about disclosures in this context.

II. Cybersecurity Disclosure Requirements

Federal securities laws are rooted in the efficacy of disclosure. Requiring the timely disclosure of relevant information presumably allows investors to make informed decisions about their investments and induces confidence in the investment community.[9] However, an effective disclosure regime requires a winnowing process, so that investors can sort ~~our~~ out

[9] As the Supreme Court has stated,

> Disclosure, and not paternalistic withholding of accurate information, is the policy chosen and expressed by Congress. We have recognized time and again, a "fundamental purpose" of the various Securities Acts, "was to substitute a philosophy of full disclosure for the philosophy of caveat emptor and thus to achieve a high standard of business ethics in the securities industry." [Citations omitted.]

Basic Inc. v. Levinson, 485 U.S. 224, 234 (1988).

relevant information from the trivial and insignificant. A materiality screen is thus designed to "filter out essentially useless information that a reasonable investor would not consider significant, even as part of a larger 'mix' of factors to consider in making his investment decision."[10]

As a leading treatise has observed, "Materiality is highly factual and thus defies a bright line definition."[11] Further, "[m]ateriality depends not upon the literal truth of statements, but upon the ability of reasonable investors to become accurately informed."[12] This amorphous character of the materiality standard has often generated controversy as registrants, regulators, and rule makers all seek to provide and/or insure that compliant content is accessible to investors. Part A provides background discussion of disclosure requirements generally, while Part B examines requirements of the 2011 Cybersecurity guidance.

A. Disclosure Rules: Generally.

Statutes enacted by Congress prescribe only a skeletal framework for disclosure, leaving the task of promulgating detailed rules to the SEC. For example, provisions of the Securities Exchange Act require periodical reporting "in accordance with such rules and regulations as the Commission may prescribe as necessary or appropriate for the proper protection of investors and to insure fair dealing in the security …."[13] For domestic registrants, the SEC has promulgated Form 10-K as the prescribed form for annual reports pursuant to this provision.[14] Quarterly reports are required on Form 10-Q following the end of the first three fiscal quarters of each year.[15] Current reporting may also be required or permitted on Form 8-K.[16] Although various other forms may be used to address registrants with other particular characteristics, these forms provide the foundation for periodic reporting by domestic registrants, thereby providing the vehicle for delivering information to investors.

Compliance with periodic reporting obligations imposes significant burdens on registrants. The Government estimates that compliance with Form 10-K imposes an average burden per response of 1,998.78 hours.[17] Form 10-Q, which must be filed three times per year,

---

[10] See id. at 233 (noting that management disclosure of an "overabundance of information" that might result in burying shareholders in "an avalanche of trivial information" is "hardly conducive to informed decisionmaking" [internal quotations and citations omitted]". The perspective of the reasonable investor has also been embraced in regulations. See, for example, 17 CFR § 230.405, which defines "material" for purposes of registration under the 1933 Act: "The term material … limits the information required to those matters to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered."

[11] Thomas Lee Hazen, 2 Law Sec. Reg. § 9.3[0] (Jan. 2015).

[12] Id.

[13] 15 U.S.C. § 78m(a). For a general discussion of the framework for reporting under federal securities laws, see Hazen, supra note 11, at § 9.3.

[14] See 17 CFR § 249.310 (directing use of Form); https://www.sec.gov/about/forms/form10-k.pdf (Form 10-K with general instructions).

[15] See 17 CFR § 249.308a (directing use of Form); https://www.sec.gov/about/forms/form10-q.pdf (Form 10-Q with general instructions).

[16] See 17 CFR § 249.308 (Form 8-K required pursuant to 17 CFR § 240.13a-11 and 17 CFR § 240.15d-11); http://www.sec.gov/about/forms/form8-k.pdf (Form 8-K with general instructions).

[17] See Form 10-K, supra note 13 (providing OMB Approval with estimated average burden hours per response).

requires 187.43 hours per response,[18] while Form 8-K, which is filed only when certain material events occur, requires 5.71 hours per response.[19]

Disclosure obligations also accompany the registration of securities prior to sale under applicable provisions of the Securities Act of 1933.[20] Notably, when the SEC is engaged in rulemaking, the statute requires that it "shall also consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation."[21]

Concerns about efficiency, effectiveness, and compliance burdens ultimately led the SEC to develop an integrated framework for disclosures affecting both registration and ongoing reporting obligations, which is known as Regulation S-K.[22] In December 2013 the SEC Staff completed a study of disclosure requirements under Regulation S-K.[23] Although that study was prompted by congressional desire to simplify disclosure by so-called "emerging growth companies",[24] the study ultimately explored the broader scheme of disclosure requirements for public companies generally.[25] The study's comments on two areas for disclosure guidance are particularly relevant to cybersecurity threats: risk factor disclosure in Item 503(c) of Regulation S-K and the potentially related matter of the management's discussion and analysis of financial condition and the results of operations in Item 303 of Regulation S-K.[26]

1. Risk factor disclosure (Item 503).

Section 503(c) of Regulation S-K addresses the matter of discussing risk factors in the content of a prospectus offered in connection with a registrant's securities. [27] That provision states in relevant part:

> (c) Risk factors. Where appropriate, provide under the caption "Risk Factors" a discussion of the most significant factors that make the offering speculative or risky. This discussion must be concise and organized logically. Do not present risks that could apply to any issuer or any offering. Explain how the risk affects the issuer or the securities being offered. Set forth each risk factor under a subcaption that adequately describes the risk. ….The risk factors may include, among other things, the following:
>
> (1) Your lack of an operating history;
>
> (2) Your lack of profitable operations in recent periods;

---

[18] See Form 10-Q, supra note 14 (providing OMB Approval with estimated average burden hours per response).
[19] See Form 8-K, supra note 15 (providing OMB Approval with estimated average burden hours per response).
[20] See 15 U.S.C. § 77g (referring to detailed specifications in 15 U.S.C. §§ 77aa).
[21] 15 U.S.C. § 77b(b).
[22] See SEC Staff, Report on Review of Disclosure Requirements of Regulation S-K 8-10 (December 2013), https://www.sec.gov/news/studies/2013/reg-sk-disclosure-requirements-review.pdf ; see also Hazen, *supra* note 11, at § 9.4.
[23] See SEC Staff, supra note 22, at 2. Regulation S-K is found at 17 CFR Part 229.
[24] See id. at 2.
[25] See id. at 3-4 ("The disclosure requirements in Regulation S-K have an impact on the costs and burdens of conducting registered offerings, including IPOs by emerging growth companies, but also have an impact on the ongoing compliance burden associated with public company status. A review of all requirements of Regulation S-K would have a benefit for issuers beyond the period that they may qualify for emerging growth company status. Therefore, in conducting its review of the requirements of Regulation S-K, the staff evaluated the requirements for public companies generally …."). As the staff also noted, "[t]he staff is not aware of a single source that presents a clear picture of the scope, frequency, and purpose of past revisions to the disclosure requirements." Id. at 7.
[26] See id. at 30, n. 80.
[27] See 17 CFR 229.503(c).

(3) Your financial position;
(4) Your business or proposed business; or
(5) The lack of a market for your common equity securities or securities convertible into or exercisable for common equity securities.[28]

As this text from Regulation S-K shows, concise discussion is required. The factors disclosed should not include risks that "could apply to any issuer or offering". The risk factor should also explain how the risk affects the particular issuer or securities. The listed examples are not designed to be exhaustive, but it is easy to see how the items listed – e.g., a lack of an operating history or profitable operations in recent periods – would logically fit these requirements of relevance and materiality. Reasonable investors would want to know such things, and apart from disclosure, they may have limited access to acquiring that information in an efficient manner.

The 2013 Study explains that the risk factor disclosure requirement in Item 503(c) was originally consolidated into Regulation S-K in 1982 from guidance originally issued in 1968 in connection with completing securities registration statements.[29] Minor changes occurred in 1995 and 1998, including adding the "risk factors" heading and implementing plain English disclosure requirements.[30] But risk factor disclosure requirements applied to only to issuing securities until the SEC announced a rule change in 2005, which extended risk factor disclosures to annual and quarterly periodical reporting.[31]

As the SEC explained in comments accompanying this 2005 announcement, the same standards in Item 503(c) apply in both registration statements and annual reports.[32] However, disclosure is quarterly reports should be limited to "material changes" to annual disclosures, with the SEC stating: "The amendments do not otherwise require, and we discourage, unnecessary restatement or repetition of risk factors in quarterly reports."[33] Thus, in order for disclosure to be meaningful, it need not be repetitive. Imposing a materiality requirement and focusing upon changes from annual disclosures likely improves the utility of disclosure, but it achieves that increased utility by reducing the volume of verbiage disclosed. Indeed, sometimes less is more.

2. MD&A Disclosure (Item 303).

The second area of Regulation S-K which may be particularly relevant to cybersecurity risk involves the management discussion and analysis requirement ("MD&A") in Item 303.[34] Item 303 generally requires that the registrant "discuss [its] financial condition, changes in financial condition and results of operations" in order to provide information that would assist investors in understanding its financial statements.[35] This provision was added to regulation S-K

[28] Id.
[29] See SEC Staff, *supra* note 22, at 75.
[30] See id.
[31] See id. (citing 70 Fed. Reg. 44722).
[32] See 70 Fed. Reg. 44722, 44786 (Aug. 5, 2005).
[33] Id. As the SEC also noted, "We are adopting the proposed requirements for updated risk factor disclosure in quarterly reports because we believe that issuers who are required to file quarterly reports already need to undertake a review of changes in their operations, financial results, financial condition, and other circumstances in order to prepare other portions of the quarterly report, including the financial statements and MD&A." Id. at 44787.
[34] See 17 CFR 229.303.
[35] See 2013 Staff, *supra* note 22, at 41.

in 1980, incorporating prior guidance calling for narrative explanations to allow investors to appraise the quality of earnings and operating results. [36] As the SEC Staff explains, "Rather than focusing on prescriptive, line-item disclosure requirements, MD&A requirements were intended to function as principles-based requirements, in order to elicit meaningful, company-specific disclosure."[37] According to the SEC Staff,

> The MD&A requirements are intended to satisfy three principal objectives: (1) to provide a narrative explanation of a company's financial statements that enables investors to see the company through the eyes of management, (2) to enhance the overall financial disclosure and provide the context within which financial information should be analyzed, and (3) to provide information about the quality of, and potential variability of, a company's earnings and cash flow, so that investors can ascertain the likelihood that past performance is indicative of future performance.[38]

In particular, Item 303 requires that a registrant to "[d]escribe any unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income from continuing operations and, in each case, indicate the extent to which income was so affected."[39] Similarly, it requires the registrant to "[d]escribe any known trends or uncertainties that have had or that the registrant reasonably expects will have a material favorable or unfavorable impact on net sales or revenues or income from continuing operations."[40] Materiality is also a condition for these disclosures, and the rules presuppose some expected level of knowledge on behalf of those speaking for the firm.

Item 303 also provides instructions to guide registrants in fulfilling these disclosure requirements. That guidance includes the general purpose, which is "to provide investors and other users information relevant to an assessment of the financial condition and results of operations of the registrant as determined by evaluating the amounts and certainty of cash flows from operations and from outside sources."[41] Registrants are also directed to focus on both events and uncertainties that are known to management that could affect either past or future operations.[42] Fortunately for registrants, a safe harbor rule for projections potentially covers forward-looking information, thereby insulating them from liability for an inaccurate prediction.[43] As might be expected, errors and omissions in applying these provisions are often the subject of litigation by investors.[44]

As explained by the SEC Staff, the SEC has also issued other guidance from time to time on the matter of compliance with MD&A requirements.[45] For example, this includes 2010 guidance issued to address disclosures relating to climate change.[46] Notably, the 2011

---

[36] See id.
[37] Id at 41-42 (citing 68 Fed. Reg. 75056).
[38] Id. at 42, n. 125.
[39] 17 CFR § 229.303(a)(3)(i).
[40] 17 CFR § 229.303(a)(3)(ii).
[41] 17 CFR § 229.303 (Instructions to Paragraph 303(a), ¶ 2)
[42] See id. at ¶ 3.
[43] See id. at ¶ 7. These safe-harbor protections from liability are discussed in part III, below.***[Add cite.]***
[44] See part III, below.
[45] See 2013 Staff, *supra* note 22, at 42-43, n.129.
[46] See id. (citing 75 Fed. Reg. 6290).

Cybersecurity guidance is not cited among these official pronouncements. However, as discussed below, that guidance does indeed draw upon these general principles in advising registrants upon the matter of incorporating cybersecurity risks relevant to investors.

B. 2011 Cybersecurity Disclosure Guidance.

In formulating its guidance, the Division of Corporate Finance has expressly stated its intention to be consistent with existing disclosure frameworks: "We prepared this guidance to be consistent with the relevant disclosure considerations that arise in connection with any business risks."[47] As for risk factor disclosures, the guidance states in part: "Registrants 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."[48] Both "severity and frequency of [past]incidents" as well as the probability of future events and the "quantitative and qualitative magnitude of those risks" should be considered in light of "the adequacy of preventive actions taken to reduce cybersecurity risks in the context of the industry in which they operate …."[49] Moreover, the guidance indicates that materiality of the risk should be an overarching consideration affecting disclosure. Indeed, the guidance mentions "material" or its derivations twenty-two times.[50]

The guidelines require that disclosure to be tailored to the particular circumstances of each registrant: "Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure."[51] Reiterating this point, the guidance also provides a significant limitation on particularity: "While registrants should provide disclosure tailored to their particular circumstances and avoid generic 'boilerplate' disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence."[52]

This expectation of avoiding cybersecurity compromise through disclosure does not excuse disclosure entirely, but it instead suggests that obfuscation through generalization is expected to avoid revealing vulnerability. However, since a registrant may take the "adequacy of preventing actions" into account in assessing the significance of cybersecurity risk, arguably only those who believe their own systems are inadequate would ultimately be responsible to disclose this information. As a result, even generalized disclosure may advertise to the dark world of the hacker that the firm is vulnerable.[53] It may also advertise to the investment

---

[47] See 2011 Cybersecurity Guidance, *supra* note 4.
[48] Id.
[49] Id.
[50] See id.
[51] Id.
[52] Id.
[53] See also Roland L. Trope and Sarah Jane Hughes, The SEC Staff's "Cybersecurity Disclosure" Guidance: Will It Help Investors or Cyber-thieves More?, BUSINESS LAW TODAY, December 19, 2011, http://apps.americanbar.org/buslaw/blt/content/2011/12/article-3-trope-hughes.shtml (arguing that a compliant disclosure that is specific to the registrant will likely be more valuable to Adversaries than to investors).

community, regulators, and potential plaintiffs, that the firm may not be securing its assets appropriately.[54]

Thus, it appears that firms seeking to follow the guidance face an uncomfortable choice. Those firms that carefully follow the guidance will be disclosing a firm-specific risk and admitting that such a risk is "among the most significant factors that make an investment in the company speculative or risky."[55] This is also an admission of vulnerability, which the firm may not be adequately addressing through preventive measures. The guidance suggests that appropriate disclosures may include: "Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences" and "[t]o the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks."[56] Providing detailed information on either of these items would not seem prudent from a security perspective.[57] Of course, the guidance expressly disclaims any intention that securities laws may require a compromise in the firm's cybersecurity, but presumably this is only true if the firm is taking appropriate measures. The real problem is that investors (and hackers) want to know exactly that kind of information.

In contrast, merely disclosing generalized risks that could apply to others in the same industry could be relatively harmless (assuming it is not signaling a bigger security problem). But this kind of disclosure would also be relatively useless, which is probably why the guidance advises against generic disclosure. Although a firm could plausibly send a favorable signal to investors that management takes cyber-risks seriously, such an approach does not conform to the requirement that the firm avoid generic boilerplate disclosures. For many firms, silence may be the most appropriate response, particularly when the firm is taking appropriate precautions to address known threats, thereby permitting such threats to be categorized below the materiality threshold.

If a firm has experienced a cyber incident and has already incurred or will likely incur costs, new compliance challenges are presented. For example, the guidance explains that "[c]yber incidents may result in losses from asserted and unasserted claims, including … indemnification of counterparty losses from their remediation efforts."[58] Material legal proceedings and financial statement effects are subject to disclosure.[59] These disclosure and compliance concerns are hardly unique to the cyber incident environment, but instead may be found in other common problems that registrants may face, including product defects, industrial accidents, or environmental harms that could potentially inflict costs or otherwise affect the economic wellbeing of the firm.

---

[54] See id.
[55] See note 49, supra.
[56] 2011 Cybersecurity Guidance, supra note 4.
[57] Moreover, it should also be noted that the federal government may also provide private sector firms with intelligence concerning threatened cyber attacks affecting key infrastructure, which might present additional foundation for concerns about potential risks. See generally Roland L. Trope, Bearings from the Southern Cross: Cybersecurity Decisions 2012-13, 69 BUSINESS LAWYER 189, 194-95 (2013) (discussing Executive Order No. 13636 (Feb. 12, 2013) which directs information sharing concerning infrastructure cyber threats)).
[58] See id. .
[59] See id.

The guidance recognizes that a firm "may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context."[60] In particular, it suggests that one who experienced a material cyber incident could not merely disclose a prospective risk that such an attack may occur.[61] Instead, the particulars of that incident, including material costs incurred to remediate these costs, as well as material increases in future cybersecurity expenses, should be disclosed.[62] Such discussion might also be appropriate in MD&A segments, but again, only to the extent that they reach the materiality threshold.[63]

The magnitude of these expenditures or expected future effects may not be expected to reach materiality thresholds in many firms. Indeed, as discussed in part IV, below, we find most firms who responded to SEC inquiries about cybersecurity disclosure reported no material impact. Moreover, the matter of security breaches affecting customer data may well become public information through other means, such as through breach disclosure laws.[64] While alternative disclosure media do not excuse required disclosures under the securities laws, they may well remove any significant new information value coming from compliance with SEC disclosure, thereby limiting market effects.

III. Legal Risks of Errors and Omissions.

Errors and omissions in company disclosures create potential liability for the company and for officers and directors who are responsible for disclosure. Moreover, a failure to appropriately monitor operations and secure assets from risk presents a liability risk for directors. The principal theories of liability include various forms of direct action under federal securities laws and derivative actions by shareholders based on a breach of a fiduciary duty. Significant liability threats and their potential effects on disclosure compliance efforts are outlined briefly below for the purpose of contextualizing risks presented in the cybersecurity context.

A. Rule 10b-5 and "fraud on the market".

Federal securities laws do not impose a general requirement that registered firms must disclose all material facts that shareholders would presumably like to know about. [65] As a leading treatise explains, "absent a statement or a separate SEC rule requiring disclosure, there is no affirmative duty to disclose facts simply because they are material."[66] In other words, absent a duty to disclose, "silence is golden."[67] Although rules enacted by public securities exchanges may require disclosure of material information despite the absence of a similar obligation under federal securities laws,[68] only private sanctions imposed by the exchange would attach to

[60] Id.
[61] See id.
[62] See id.
[63] See id.
[64] See generally Morse & Raval, Private Ordering in Light of the Law: Achieving Consumer Protection Through Payment Card Security Measures, 10 DePaul Bus. & Comm. L. J. 2013 (2012).
[65] See, e.g., In re BioScrip, Inc. Securities Litigation, __ F.Supp. 3d __, 2015 WL 1501620 (S.D. N.Y. March 31, 2015) ("Disclosure is not required simply because an investor might find the information relevant or of interest.")
[66] Hazen, supra note 11, at § 12.19[1].
[67] Id. (internal quotations omitted).
[68] See id. (citing, for example, NYSE Rule 202.05)

nondisclosure under these rules, rather than a legal remedy for shareholders.[69] Accordingly, the fact that the 2011 Cybersecurity Guidance does not rise to the level of a rule requiring disclosure is highly significant.[70]

Liability for a failure to disclose could nevertheless develop under section 10(b) of the Securities Exchange Act of 1934, which makes it unlawful to "use or employ, in connection with the purchase or sale of any security … any manipulative or deceptive device or contrivance in contravention of [SEC] rules and regulations".[71] Rule 10b-5, which implements this provision, states in relevant part:

> It shall be unlawful for any person … [t]o make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading …in connection with the purchase or sale of any security.[72]

Thus, the rule addresses untrue statements of a material fact, as well as omissions of material facts that are necessary to prevent other statements made from misleading investors. In other words, in order to violate Rule 10b-5, you have to speak (at one time or another). Although the rule merely proscribes such statements or omissions as unlawful, courts have recognized an implied private cause of action to enforce the rule.[73] Rule 10b-5 has become the primary source for damages paid out in settlement and judgments pursuant to private litigation under federal securities laws.[74]

A claim under Rule 10b-5 requires the plaintiff to prove these basic elements: "(1) a material misrepresentation or omission by the defendant; (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation."[75] A rebuttable presumption of reliance is available based on what is known as the "fraud-on-the-market" theory, which embodies the assumption underlying the efficient market hypothesis, i.e., that the market price reflects publicly available information, thereby incorporating any material misrepresentations.[76] Although the plaintiffs in *Halliburton* challenged the validity of this assumption, the Supreme Court sustained this approach to reliance, thereby permitting class action lawsuits to go forward without a requiring proof of individual reliance for each shareholder plaintiff.[77] The presumption of reliance is rebuttable, and courts will need to figure out exactly what standard will be applied to evidence sufficient to rebut that presumption.[78]

---

[69] See id. (noting that "sanctions by the exchange … have rarely been imposed for this type of violation alone.")
[70] See note 5, *supra*.
[71] 15 U.S.C.A. § 78j.
[72] 17 CFR § 240.10b-5.
[73] See Halliburton Co. v. Erica P. John Fund, Inc, 134 S.Ct 2398, 2407 (2014) (citing Blue Chip Stamps v. Manor Drug Stores, 421 U.S. 723, 730 (1975).
[74] See Merritt B. Fox, Halliburton II: It All Depends on What Defendants Need to Show to Establish No Impact on Price, 70 BUS. LAW. 437, 439 (2015).
[75] Halliburton, *supra* note 69, 134 S.Ct. at 2407 (internal quotations omitted).
[76] See id.
[77] See id. at 2407-13.
[78] See generally Fox, supra note 71.

Presumably, proof that the misrepresentation did not affect the market price will be sufficient for this purpose.[79]

The scienter requirement, which refers to a state of mind "embracing intent to deceive, manipulate, or defraud"[80], also presents a significant hurdle for plaintiffs. In 1995, Congress enacted the Private Securities Litigation Reform Act, which imposes more exacting pleading requirements upon private securities fraud plaintiffs for the purposes of preventing abusive claims.[81] According to the Supreme Court,

> Under the PSLRA's heightened pleading instructions, any private securities complaint alleging that the defendant made a false or misleading statement must: (1) "specify each statement alleged to have been misleading [and] the reason or reasons why the statement is misleading," 15 U.S.C. § 78u–4(b)(1); and (2) "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind," § 78u–4(b)(2).[82]

According to the Court, "an inference of scienter must be more than merely plausible or reasonable – it must be cogent and at least as compelling as any opposing inference of nonfraudulent intent."[83] The Supreme Court has assumed that "deliberate recklessness" was sufficient for this purpose, assuming that the pleading otherwise follows the PSLRA requirements.[84] Courts have viewed "conscious misbehavior or recklessness" as sufficient for scienter, as well as a "failure to check information that [defendants] has a duty to monitor".[85] However, a recklessness standard has also been characterized as a "high burden", which plaintiffs cannot easily satisfy.[86]

Despite these barriers to pleading, effective securities fraud claims have gone forward based on omissions, which are rooted in management's failure to correct generalized disclosures with specific information that could have impacted risk to the firm. For example, in *Matrixx Initiatives*,[87] the Supreme Court sustained a claim under Rule 10b-5 in the context of a pharmaceutical manufacturer who failed to disclose medical reports that consumers using its product, Zicam Cold Remedy, developed a condition called anosmia (losing the sense of smell). In response to medical studies that appeared to show anosmia in connection with the use of Zicam, the company issued Form 10-Q in November 2003 that included risk factor disclosures

[79] See Halliburton, supra note 70, at 2408.
[80] See Matrixx Initiatives, Inc. v. Siracusano, 131 S.Ct. 1309, 1323 (2011) (internal quotations omitted).
[81] See Tellabs, Inc. v. Makor Issues & Rights, Ltd., 551 U.S. 308, 313 (2007).
[82] Id. at 321.
[83] Id. at 314; see also id. at 324. As Justice Scalia points out in a concurring opinion, this effectively means that a plaintiff may get an edge in close cases. Id. at 329-30. He would prefer a test that required an inference of scienter to be "*more plausible* than the inference of innocence." Id. at 329.
[84] See Matrixx, supra note 77, at 1324.
[85] See in re Fairway Group Holding Corp. Securities Litigation, 2015 WL 249508 (S.D. N.Y. Jan. 20, 2015).
[86] See in re Molycorp. Inc. Securities Litigation, 2015 WL 1097355, at 10 (S.D. N.Y. Mar. 12, 2015).
[87] See Matrixx, supra note 77.

warning investors of potential "material adverse effect" that could result from product liability claims, "whether or not proven to be valid".[88]

Unfortunately, when the company issued its general Form 10-Q disclosure, the company failed to disclose that two plaintiffs had already sued the company for causing anosmia.[89] In January 2004, news outlets reported that the FDA was investigating complaints that Zicam users were losing their sense of smell, apparently causing a significant drop in the stock price. Three days after these reports, the company issued a press release that included a statement that "Matrixx believes statements alleging that intranasal Zicam products caused anosmia (loss of smell) are completely unfounded and misleading."[90] A few days later, the company filed a Form 8-K, in which it stated that a panel of physicians and scientists had concluded "there is insufficient scientific evidence at this time to determine if [Zicam], when used as recommended, affects a person's ability to smell."[91]

In this context, the Supreme Court ruled that the plaintiffs had sufficiently alleged both material misstatement and scienter for purposes of their Rule 10b-5 claim. Here, the Court found "[i]t is substantially likely that a reasonable investor would have viewed this information as having significantly altered the total mix of information made available".[92] In sustaining the materiality claim, the Court also specifically pointed to company statements about rising revenues in the face of a significant risk to its leading revenue-generating product, as well as evidence that the company characterized this risk as "unfounded and misleading" despite having no studies of its own to disprove the link to anosmia.[93] The company's actions also provided sufficient support for the scienter requirement, as they supported an inference that the company chose not to disclose risks because of their likely effect upon the market for the company's stock.[94]

The Court's decision in *Matrixx* reflects an assessment of cumulative effects of several actions by the defendant. The generalized risk factor disclosure was only a part of the story, albeit one that was mentioned by both the Supreme Court and the Ninth Circuit.[95] But this case shows how speaking can be riskier than silence: making an assertion that was arguably incomplete in light of other information available to the company provides a data point that can be used to construct the framework for a viable claim under Rule 10b-5. A disclosure duty can arise when a subsequent event makes a prior statement false or misleading in a material way.[96]

---

[88] Id. at 1314. The Ninth Circuit's decision below, which the Supreme Court affirmed, clarifies that this was part of a risk factor disclosure that included the heading "We may incur significant costs resulting from product liability claims", which was the basis for one of allegations of false and misleading statements by the company. See Siracusano v. Matrixx Initiatives, Inc., 585 F.3d 1168, 1174, 1179-80 (9th Cir. 2009).
[89] Matrixx, supra note 78, at 1314.
[90] Id. at 1316.
[91] Id.
[92] Id. at 1321 (internal quotations omitted).
[93] See id. at 1324.
[94] See id. at 1324-25.
[95] See note 86, supra.
[96] See, e.g., In re Time Warner Inc. Securities Litigation, 9 F.3d 259, 267-68 (2d Cir. 1993)("[A]n omission is actionable under the securities laws only when the corporation is subject to a duty to disclose the omitted facts; such duty can arise "from the combination of a prior statement and a subsequent event, which, if not disclosed, renders the prior statement false or misleading").

An earlier disclosure can arguably become misleading when it provides a false sense of reality based on the mix of information available to the investor. [97]

Indeed, the 2011 Cybersecurity Guidance warns that merely disclosing a risk of cyberattack may not be sufficient if a material attack that compromised customer data had actually occurred.[98] However, the guidance does not address whether materiality considerations underlying disclosure would differ in the event that the firm had previously issued a general risk factor disclosure. If a prior general risk factor disclosure has been made, with no mention of actual attacks, would that suggest to investors that no successful attacks had occurred, a fact that is now false? And is a successful attack affecting customer information a significant change in the mix of information available, even if viewed in isolation, it would not be likely to have a material financial impact on the firm? On the other hand, if the firm had said nothing, there is no false impression to correct and the cyber incident would be evaluated based on its own significance to the firm's economic and operational wellbeing. The firm's assessment could turn out to be incorrect, in that the impact may be greater than it appeared, but that would likely not create an actionable omission on account of the meet the scienter requirement.

Knowledge of actual breaches also presents other conundrums for the firm. When a firm discovers a security breach, the firm could face a continuing threat until it ascertains and eliminates the source of vulnerability. Risk factor disclosure in this context could provide useful information to an investor about a firm-specific risk. However, it would not likely be prudent for the firm to disclose that kind of information before the perpetrator is identified if company losses are to be avoided. This kind of situation clearly presents tension with the assertion that "federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity."[99] Investors interested in the longer-term horizon would likely prefer that the firm avoid any disclosures that increase costs to the firm, even if that means a less accurate price for its stock because some risks or threats remain hidden from the public. Unfortunately, this policy judgement has not been clearly announced in a rule. Here, too, silence on these matters likely enhances the firm's ability to avoid making corrective disclosures that could prove disadvantageous.

To the extent that the cause of a breach has been resolved and new security measures are put into place, it is entirely possible that a risk factor disclosure would not be necessary if the firm's security measures are likely to reduce the risks to the firm for a future breach below the materiality threshold. On the other hand, to the extent that a breach may impact the firm's financial or operational health, the firm must assess whether those impacts merit disclosure.

---

[97] See id. ("The undisclosed information is material if there is 'a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information available.' [Citation omitted.] If a reasonable investor would so regard the omitted fact, it is difficult to imagine a circumstance where the prior statement would not be rendered misleading in the absence of the disclosure.")

[98] See 2011 Cybersecurity Guidance, supra note 3 ("A registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context. For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences.")

[99] See note 53, supra.

However, this is not a disclosure peculiar to the realm of cybersecurity risk. The resulting financial and operational assessment is indeed similar to that which occurs in the context of assessing liability threats from litigation or known defects in a product, and may appropriately be addressed under Item 303 of Regulation S-K.[100]

The Second Circuit in *Stratte-McClure v. Morgan Stanley* has ruled that a public company's failure to disclose under Item 303 of Regulation S-K, which imposes an affirmative duty to disclose "any known trends or uncertainties … that the registrant reasonably expects will have a material … unfavorable impact on … revenues or income from continuing operations" can also provide a basis for a securities fraud claim under Rule 10b-5.[101] This ruling contradicts the Ninth Circuit, which has rejected Item 303 as the basis for an actionable claim under Rule 10b-5.[102]

However, a successful plaintiff still has to overcome both the materiality and scienter hurdles in this context. The Second Circuit found that the plaintiff had met its pleading requirement through alleging that defendant Morgan Stanley had failed to disclose potentially material effects on its financial condition on account of its participation in the subprime mortgage securities market.[103] But the plaintiff did not adequately plead facts to show scienter, which allowed the claim to be dismissed. Unlike the defendant in *Matrixx*, Morgan Stanley had not made any affirmative statements about risk exposure, which could have been viewed as misleading investors. [104] Moreover, Morgan Stanley had reported subprime risk exposure to investors less than a month after its third quarter 10-Q and a month before its next report was due.[105] The delay occurred because the company was engaged in internal deliberations about its exposure, which the court found was at worst negligent and thus below the higher standard of recklessness needed to show scienter.[106]

---

[100] Such matters may also be covered by Item 103 of Regulation S-K, which contains a 10 percent of current assets disclosure threshold for the amount of any damage claim in litigation. See generally Note, Contemplated Corporate Disclosure Obligations Arising from Cyubersecurity Breaches, 38 J. CORP. L. 659, 673 (2013).

[101] See Stratte-McClure v. Morgan Stanley, 776 F.3d 94, 101 (2nd Cir. 2015). It should be noted that this context for liability differs from those involving Sections 11 and 12(a)(2) of the Securities Act, codified at 15 U.S.C. §§ 77k, 77l(a)(2), respectively, which apply to registration statements. Item 303 has previously been recognized as creating a duty to disclose giving rise to liability in that context. See Panther Partners Inc. V. Ikanos Communications, Inc., 681 F.3d 114, 119-22 (2d Cir. 2012) (finding "generic cautionary language" did not fulfill duty to inform of "particular, factually based uncertainties").

[102] See *Morgan Stanley*, 776 F.3d at 101 (citing as contrary authority In Re. NVIDIA Corp. Securities Litigation, 768 F.3d 1046 (9th Cir. 2014)). A district court in the Eighth Circuit has also followed *Morgan Stanley* in allowing a Rule 10b-5 claim to go forward based on Item 303. See Beaver County Employees' Retirement Fund v. Tile Shop Holdings, Inc., 94 F.Supp.3d 1035 (D. Minn. 2015). See generally Hazen, supra note 11, at § 3.9[7] note 164 (collecting cases showing inadequate MD&A disclosures giving rise to liability under Rule 10b-5).

[103] See *Morgan Stanley*, 776 F.3d at 105-06. See also In re Francesca's Holdings Corp. Sec. Litig., 2015 WL 1600464, at 18 (S.D.N.Y. Mar. 31, 2015) ("Moreover, in order for even a known trend or uncertainty to create a disclosure obligation, the [event] must have been significant enough that the Company should 'reasonably expect[ ]' it to have a material unfavorable impact on its financials. 17 C.F.R. § 229.303(a)(3)(ii)."

[104] See *Morgan Stanley*, 776 F.3d at 107.

[105] See id.

[106] See id.

A "trend or uncertainty" known to the company[107] that could have a material unfavorable effect could include data security breaches known to the company, which could unfavorably impact the company's revenues or income in a material sense. A liability threat in this context may induce companies to look carefully at data security protections, as well as breach events in order to assess whether disclosure is appropriate. However, *Morgan Stanley* also suggests that a company's conscious decision to delay disclosure when there is a need to assess the magnitude and effect of a risk exposure may be appropriate, nullifying a scienter requirement.

Finally, it should be noted that disclosures of trends or uncertainties also potentially intersect with protections that may be available for so-called "forward-looking statements". In the Private Securities Litigation Reform Act of 1995 (PSLRA), Congress added safe harbors for certain forward-looking statements to the Securities Act and the Securities Exchange Act.[108] However, in order to be protected, the statement must meet several requirements, including a requirement that it be "accompanied by meaningful cautionary statements."[109] A statement about future financial impacts of a data security breach might well be covered by the safe harbor, but those which combine misleading historical facts with future impacts would not be covered. As the District of Columbia Circuit recently explained,

> A warning that identifies a potential risk, but "impl[ies] that no such problems were on the horizon even if a precipice was in sight," would not meet the statutory standard for safe harbor protection. If a company were to warn of the potential deterioration of one line of its business, when in fact it was established that that line of business had already deteriorated, then, as the Second Circuit explained, its cautionary language would be inadequate to meet the safe harbor standard. By analogy, the safe harbor would not protect from liability a person "'who warns his hiking companion to walk slowly because there might be a ditch ahead when he knows with near certainty that the Grand Canyon lies one foot away.'" [T]here is an important difference between warning that something "*might*" occur and that something "*actually* had" occurred.[110]

Alternatively, courts may also apply some form of the common law "bespeaks caution" doctrine as a means of conferring some protection upon a forward-looking statement.[111] Through a common law approach, protection for a cybersecurity disclosure may be developed through case-by-case adjudication. But in the meantime, as noted above, silence is golden; less is more. Unless you must disclose, silence is the preferable course to avoid liability.

B. Fiduciary Duties under State Law.

[107] See Hazen, supra note 11, at § 3.9[7] ("The obligation [to disclose] extends to trends and uncertainties that are 'known' and thus it is not sufficient that they were simply 'knowable' or merely possibility." [footnotes omitted]).
[108] See generally Allan Horwich, Clearing the Murky Safe Harbor for Forward-Looking Statements: An Inquiry into Whether Actual Knowledge of Falsity Precludes the Meaningful Cautionary Statement Defense, 35 J. CORP. L. 519, 523-24 (2010) (citing 15 U.S.C. §§ 77z-2, 78u-5).
[109] 15 U.S.C. § 78u–5(c)(1)(A)(i).
[110] In re Harman Int'l Indus., Inc. Sec. Litig., No. 14-7017, 2015 WL 3852089, at *9 (D.C. Cir. June 23, 2015) (citations omitted).
[111] [Add citation]

State law may provide a distinct remedy for harms to investors that may not otherwise be actionable under federal securities laws.[112] Rather than a securities class action, a shareholder derivative claim might be used to seek a recovery for losses caused by an act or omission of the board of directors which constitutes a breach of fiduciary duty. As discussed below, the liability bar in this area is set high, making it difficult for shareholders to recover losses from directors. However, these legal theories merit brief discussion to explore the extent to which they may affect board decisions involving cybersecurity disclosures.

1. Good Process and Good Faith.

As noted in an influential decision of the Delaware Court of Chancery, *In re Caremark International Inc. Derivative Litigation*[113], it is difficult to charge directors with responsibility for corporate losses.[114] When a decision of the directors ultimately produces a loss, liability will typically be reviewed under "the director-protective business judgment rule, assuming the decision made was the product of a *process* that was *either* deliberately considered in good faith or was otherwise rational."[115] As the court explained, a rule that permitted an objective evaluation of the decision, rather than an examination of a process of decision making, would injure investor interests by exposing directors to second-guessing by judges or juries.[116] "Thus, the business judgment rule is process oriented and informed by a deep respect for all *good faith* board decisions."[117]

In a second category of cases, claims to recover losses are based not on particular decisions, but on "unconsidered inaction".[118] Corporate agents other than directors make many decisions that can affect the wellbeing of the enterprise, without specific director attention. [119] Liability based on lack of oversight is possible, but the court describes this theory as "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment."[120]

In *Caremark,* losses resulted from employees who violated federal laws. In order to impose liability on directors based on their failure to exercise oversight, the *Caremark* court found that "plaintiffs would have to show either (1) that the directors knew or (2) should have known that violations of law were occurring and, in either event, (3) that the directors took no steps in a good faith effort to prevent or remedy that situation, and (4) that such failure

[112] See, e.g., Minzer v. Keegan, 218 F.3d 144, 152 (2d Cir. 2000) ("It may also be that the allegations amount to a breach of fiduciary duties under state law, but such conduct, without an accompanying materially misleading disclosure, does not state a claim under the federal securities laws. See Santa Fe Indus., Inc. v. Green, 430 U.S. 462, 479, 474-80, 97 S.Ct. 1292, 51 L.Ed.2d 480 (1977) (refusing to extend federal securities laws to "overlap and quite possibly interfere with state corporate law")
[113] 698 A.2d 959 (Del. Ch. 1996).
[114] Id. at 967.
[115] Id. (emphasis in original).
[116] See id.
[117] Id. at 967-68 (emphasis in original).
[118] Id. at 968.
[119] See i.d
[120] Id. at 967.

proximately resulted in the losses complained of ….”[121] As the court explained, this test would be demanding, as it would essentially require a lack of good faith in exercising directorial duties:

> Such a test of liability—lack of good faith as evidenced by sustained or systematic failure of a director to exercise reasonable oversight—is quite high. But, a demanding test of liability in the oversight context is probably beneficial to corporate shareholders as a class, as it is in the board decision context, since it makes board service by qualified persons more likely, while continuing to act as a stimulus to *good faith performance of duty* by such directors. [122]

Subsequent cases have arguably made it even more difficult to pursue claims based on a failure to monitor or exercise oversight transforming the required lack of good faith into a breach of a duty of loyalty to the corporation, so that the plaintiff must allege that directors consciously disregarded their duties. For example, in *Stone ex. rel. AmSouth Bancorporation v. Ritter*,[123] the Supreme Court of Delaware stated:

> We hold that *Caremark* articulates the necessary conditions predicate for director oversight liability: (a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention. In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations. Where directors fail to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their responsibilities, they breach their duty of loyalty by failing to discharge that fiduciary obligation in good faith.[124]

While other courts have suggested the *Caremark* standard for liability did not require intentional harm, and potentially could include reckless behavior,[125] these requirements create formidable barriers to liability.

2. Application to Cybersecurity.

Board decisions to employ personnel or technology to address cybersecurity risks are therefore likely to be protected from liability claims in shareholder derivative suits. Even if cybersecurity measures proved ineffective, the process-oriented business judgment rule analysis would appear to provide broad protection for actual board decisions. Likewise, claims based on a failure to monitor or exercise oversight over cybersecurity risks are unlikely to succeed when the directors can that they devoted attention to cybersecurity risks, thereby demonstrating good faith.

Formal disclosures to shareholders, including the identification of risk factors and sharing MD&A insights, may also provide a means to show that directors are paying attention to these

[121] Id. at 971.
[122] Id.
[123] 911 A.3d 362 (Del. 2006).
[124] Id. at 370.
[125] See, e.g., McCall v. Scott, 239 F.3d 808, 818-19 (6th Cir. 2001) (interpreting Delaware law).

concerns. But formal disclosures are hardly the only means of proving that directors were exercising their oversight responsibilities. In fact, including a generalized risk factor disclosure concerning cyberspace risks may suggest that such matters merit heightened attention. Could a generalized risk factor disclosure that accompanies a pattern of behavior that demonstrates a lack of director attention to cybersecurity matters suggest a lack of good faith?

Directors concerned about oversight liability will want to provide a record of actual oversight apart from risk disclosures in order to ensure that they are able to deter such claims. Although it is plausible that boards could view formal disclosures about cyberspace risks as a means to signal or advertise their attentiveness, the empirical results in part IV, below, suggest that the marketplace is not buying that message. Instead, it seems to be punishing those firms that chose to make risk factor disclosures about cybersecurity.

IV. Interpreting Disclosures of Cybersecurity Risk: Evidence from the Market

The SEC's October 13, 2011 guidance on cybersecurity risks has apparently produced new disclosures by firms, and the patterns and effects of these disclosures are analyzed below. Part A describes the number of disclosures in time periods before and after the guidance. Part B addresses market price effects from the disclosures in the first year following the guidance. Part C outlines some additional data from SEC comment letters regarding compliance with the guidance.

A. Firm Disclosure Patterns.

Table 1 below shows the number of 10Ks filed during relevant disclosure periods before and after the date of the guidance. No firm used the specific term "cybersecurity risks" in the year before the guidance was issued; the number of 10K reports using this specific terminology has gradually increased since then. Although examining only this narrow terminology taken from the guidance likely underreports the number of firms that address the matter of data security generally,[126] use of this specific term tracks the likely influence of the guidance upon firm behavior.

Remarkably, only a small percentage of firms are referring to "cybersecurity risks" in disclosures to investors. However, that percentage is growing, more than quadrupling in the four year period following the guidance, although some of that percentage growth is apparently being fueled by fewer 10K filings over this period.[127]

---

[126] For example, some firms may choose to use related terminology to describe similar risks, such as "data security", or they may choose to describe "risks related to cybersecurity" instead of a specific pairing. We also paired "risks" with "cybersecurity". If the singular "risk" is used, it may add up to three incidents, which does not materially impact the analysis.

[127] The declining total number of 10-Kfilings in the database may reflect trends of smaller firms "going dark" by eliminating public ownership and reporting requirements, but this trend could also be affected by acquisitions, mergers, or bankruptcies. Stock market listings actually rose slightly in 2013 from the prior year, but it would take an annual reporting period to see an impact on Form 10-K filings. See U.S. Public Companies Rise Again, WALL STREET JOURNAL, Feb. 5, 2014, available at

Table 1: 10K Disclosures with "Cybersecurity Risks" [128]

Date Range After – Before	10Ks with "Cybersecurity Risks"	Total 10Ks	% of Total
10/12/10-10/13/11	0	9,707	0.00%
10/12/11-10/13/12	55	8,958	0.61%
10/12/12-10/13/13	92	8,537	1.08%
10/12/13-10/13/14	114	8,255	1.38%
10/12/14- 8/13/15	193	7,453	2.59%

For the most recent full-year period (10/12/13 to 10/13/14), Table 2 below shows that firms from the following industry classifications filed Form 10K using "cybersecurity risks". Remarkably, the classified firms reflect a variety of industries, with no clear domination by any particular industry group.

Table 2: Thompson Reuters Industry Classifications (10/12/13 – 10/13/14)[129]

Classification:	# of Firms	% of Total
Basic Materials	6	6.19%
Consumer Cyclicals	24	24.74%
Consumer Non-Cyclicals	6	6.19%
Energy	17	17.53%
Financials	25	25.77%
Healthcare	3	3.09%
Industrials	9	9.28%
Technology	2	2.06%
Utilities	5	5.15%
Total	97	

If search terminology is expanded to include range of disclosures involving cybersecurity risks, [130] the results increase slightly in periods after the cybersecurity guidance, but remain effectively at zero during the prior year, as shown in Figure 3, below. Moreover, Table 4 shows that the industry classification experiences remain relatively dispersed, although financial firms seem to be gaining more firms discussing cybersecurity risks using expanded terminology:

---

http://www.wsj.com/articles/SB10001424052702304851104579363272107177430 (showing listings and delistings over time).

[128] These figures reflect searches in the Westlaw Edgar 10K database with the specific term "cybersecurity risks" for the first column and the common term "risks" for the second column in order to approximate the total Form 10K filings reflected in each period.

[129] These figures are drawn from Thompson Reuters Classifications available in the Westlaw Edgar databases. The total of 97 firms reflects the fact that some firms making filings are not classified in this system.

[130] This search used the Boolean search "cybersecurity /5 risk or incident or threat" in the Westlaw database for EDGAR Form 10K filings.

Table 3: 10K Disclosures with "Cybersecurity" in proximity to Risk, Threat, or Incident[131]

Date Range	10Ks with Cybersecurity Risk, Threat Or Incident	Total 10Ks	% of Total
10/13/10-10/13/11	2	9,707	0.02%
10/13/11-10/13/12	139	8,958	1.55%
10/13/12-10/13/13	206	8,537	2.41%
10/13/13-10/13/14	294	8,255	3.56%
10/13/14-8/13/15	493	7,453	6.61%

Table 4: Thompson Reuters Industry Classification for Firms in 10/13/13/-10/13/14 Period

Classification:	# of Firms	% of Total
Basic Materials	12	4.71%
Consumer Cyclicals	39	15.29%
Consumer Non-Cyclicals	14	5.49%
Energy	33	12.94%
Financials	74	29.02%
Healthcare	14	5.49%
Industrials	38	14.90%
Technology	23	9.02%
Telecommunications Services	1	0.39%
Utilities	7	2.75%
Total	255	

Table 5, below, shows the proportion of firms having a Thomson Reuters Industry classification that included cybersecurity risk disclosures in the period from October 13, 2013-October 13, 2014 (the latest full year for which data is available) in relation to all firms filing form 10K having an industry classification. The data suggests that participation rates vary across industries, and that those rates are quite low in relation to the entire classified population.

Table 5: Estimated Proportions of Industry Participation in Cybersecurity Disclosure in the period October 13, 2013-October 13, 2014.

Industry Classification	*# Reporting Cybersecurity Risk*	*Total Firms*	*% Reporting Cybersecurity*
Basic Materials	12	438	2.74%
Consumer Cyclicals	39	942	4.14%

[131] Neither of the two firms identified in the 10/13/10 – 10/13/11 time period had disclosures that were relevant to their own cybersecurity practices, although the terms appeared in their Form 10K.

Consumer Non-Cyclicals	14	370	3.78%
Energy	33	622	5.31%
Financials	74	1376	5.38%
Healthcare	14	949	1.48%
Industrials	38	948	4.01%
Technology	23	974	2.36%
Telecommunications Services	1	96	1.04%
Utilities	7	109	6.42%
Total	255	6824	3.74%

These quantitative measures of firm disclosure practices suggest that the vast majority of firms are choosing not to address cybersecurity risks in their annual disclosure documents. As discussed above, this likely reflects the view that "silence is golden" – when a disclosure rule is not requiring the firm to address this matter, firms may effectively lower their securities litigation risks by saying as little as possible about it, providing that a material incident has not already occurred in the firm.

B. Effects of Disclosure on Market Prices.

In order to examine the market impacts of new cybersecurity disclosures following the 2011 SEC guidance, we examined 10K and 10Q filings during the twelve-month period before and after October 13, 2011, in order to identify firms that chose to add disclosures during this period. We targeted the use of the term "cybersecurity" in the "risk factors" discussion of Form 10K using the EDGAR database, thus generating a slightly broader result than a more restrictive search term, such as "cybersecurity risk". Although this produced a total of 188 filings, some firms were rejected because "cybersecurity" was used to address matters such as product offerings that do not relate to firm-specific risks.

This inquiry ultimately generated 167 Form 10-K filings by firms with publicly traded common stock for which the Form 10-K represented their first disclosure of cybersecurity-related risk as a risk factor to be considered for that firm. We then identified 37 firms with publicly-traded common stock that had made cybersecurity disclosures on Form 10-Q, rather than Form 10K.[132] By identifying all of these firms and identifying the date on which disclosure was provided to the SEC, we were able to evaluate the impact of such disclosures on market prices.

Our null hypothesis – no statistically significant effect from expanding risk factor disclosures – reflected the expectation that the market likely reflected the risk profile of each firm. Therefore we test the following more formally stated hypothesis:

[132] Form 10K disclosure might follow the Form 10Q disclosure, but the Form 10Q disclosure was tracked separately as it was the earliest indication that the firm was making a new disclosure concerning cybersecurity risks. Our analysis focused on Risk Factor disclosures, although we also identified a few firms who included discussion other segments of Form 10K without adding risk factor disclosures.

$H1_0$: The null hypothesis is that there is no effect on firm value from the voluntary disclosure of cybersecurity-related risk.

$H1_A$: The alternative hypothesis is that the voluntary disclosure of cybersecurity-related risk announces an increase in risk resulting in significant negative abnormal returns.

Given the ubiquity of data security breach discussions, the possibility of adverse effects would likely be generalized among all firms. However, the empirical results allowed us to reject this null hypothesis.

When 10-K disclosures are segregated, the outcome continued to reflect a significant and negative impact after disclosure. These results indicate that investors are assigning a negative value to the minority of firms that choose to report cybersecurity risk in their risk factors. Given that disclosure is not compelled, and that the relevant SEC guidance suggests that it should only be made when the risk is firm-specific and among the most significant sources of risk for investing in the firm,[133] it is plausible that investors believe that this risk could materialize in a manner adverse to the interests of the company. Given that only a small percentage of the firms choose to disclose, the differential result suggests that firms that are silent may be perceived in a better light. Silence is indeed golden – at least from the investor's perspective. This negative outcome for disclosure also casts doubt upon an alternative hypothesis – that disclosure might mean that management is particularly proactive about this kind of risk, rather than ignoring it.

We also noted an unusual phenomenon with regard to the segregated data for 10-Q disclosures to add a cybersecurity risk factor. Here, the adverse impact occurs on the day before the 10-Q is disclosed. Although this affected a relatively small population of 37 firms, this data might provide a basis for concern about the security of the content of 10-Q disclosures in advance of their publication. Further research is needed on this point.

1. Method of Analysis.

To study whether a voluntary disclosure of cybersecurity-related risk event has any impact on the market value of a firm, we measure event-day cumulative abnormal returns (CARs) and test their statistical significance. We focus primarily on whether or not there was a market price effect of the firm's voluntary disclosure of cybersecurity-related risk within a reasonable time period, called the event window. The event window is the amount of time, measured in the number of trading days, taken by investors to absorb the impact of a new event. According to the efficient market hypothesis, new information is incorporated very quickly into the stock price. Consequently, a short event window is likely to more reliably test the market effect of an event.

An event study methodology is used to determine the price effect of the firm's voluntary disclosure of cybersecurity-related risk. For similar event study methods, see for example Conrad (1989), Holland and Wingender (1997), Groff and Wingender (2010), and Park, Lee and

[133] See text at notes __, supra.

Song (2014).[134] Single factor market model parameters are calculated using the estimation period of trading days before the event date to approximate one year of stock returns. The estimation period begins 275 trading days before the event and ends 26 days before it. These dates are the same as those used by Park, Lee and Song (2014). Across the companies in our sample, these dates cover several market cycles. For this study, we use the market model event study method and test the results for significance with the standard residual method. The market model event study method uses a linear regression to predict stock returns; then it compares the predicted value to its actual return. To test whether the cumulative abnormal return is significantly different from zero, we use the standardized cross-sectional method. We use the equally-weighted CRSP (Center for Research in Security Prices) index for the model's market returns. We also employ a generalized sign test, which differs from the simple sign test in that the fractions of positive and negative returns under the null hypothesis are determined by the fractions observed in the estimation period, rather than fixed at 0.5. Betas in the market model are estimated using the method of Scholes and Williams (1977).[135] To statistically test the data, the null hypothesis that the introduction of the event has no effect on the returns of the underlying security will be rejected if the Z-statistic is significant at the 0.10 level or lower with a one-sided test.

The abnormal return (ABR_{jt}) is the difference between the actual return (R_{jt}) on a specific date and the expected return ($E(R_{jt})$) calculated for the firm on that specific date. The expected return is calculated using the parameters of a single index regression model during the pre-event estimation period. The regression model parameters are determined by the following equation:

$$R_{jt} = a_j + b_j R_{mt} + e_{jt}$$

where R_{jt} is the return on security j for period t, a_j is the intercept term, b_j is the covariance of the returns on the jth security with those of the market portfolio's returns, R_{mt} is the return on the CRSP value-weighted market portfolio for period t, and e_{jt} is the residual error term on security j for period t. Betas (β_j) in the market model are estimated using the method of Scholes and Williams (1977). Ordinary Least Squares (OLS) was used to estimate the slope and intercept parameters for each security in the data set. The market model estimation is adjusted for any first order autocorrelation with a GARCH(1,1) approach. These estimates were then used to calculate the expected return for the event window, from which the abnormal returns (AR_{jt}) can be calculated:

$$AR_{jt} = R_{jt} - \left(\alpha_j + \beta_j R_{mt}\right)$$

[134] Jennifer Conrad, "The Price Effect of Option Introduction," 44 JOURNAL OF FINANCE 487-498 (1989); L.C. Holland & J.R. Wingender, Jr., "The Price Effect of the Introduction of LEAPS," 32(2) THE FINANCIAL REVIEW __(1997); James E. Groff & John R. Wingender, Jr., "The Impact on Firm Value from Joining a B2B Sourcing Network," 16(1) THE BUSINESS REVIEW, CAMBRIDGE __ (2010); Tae-Jun Park, Youngjoo Lee, & Kyojik "Roy" Song, "Informed Trading before Positive vs. Negative Earnings Surprises," 49 JOURNAL OF BANKING AND FINANCE __ (2014).

[135] Myron Scholes and J. Williams, "Estimating Betas from Non-synchronous Data," 9 JOURNAL OF FINANCIAL ECONOMICS 309-327 (1977).

where the estimates of alpha and beta are those calculated above from the estimation period. The average abnormal return (AAR_t) is calculated as the mean AR_{jt} for all N securities:

$$AAR_t = \frac{\Sigma_{j=1}^{N} AR_{jt}}{N}$$

where t is the trading day relative to the event. The cumulative average abnormal return from Day T_1 to Day T_2 ($CAAR_{T_1,T_2}$) is calculated as follows:

$$CAAR_{T_1,T_2} = \sum_{t=T_1}^{T_2} AAR_t$$

Test statistics are calculated as in Patell (1976). Standardized abnormal returns (SAR_{jt}) are defined as follows:

$$SAR_{jt} = \frac{AR_{jt}}{S_{jt}}$$

S_{jt} is further defined as the square root of the security j estimated forecasted variance:

$$S_{jt}^2 = S_j^2(1 + \frac{1}{D_j} + \frac{(R_{mt} - R_m)^2}{\Sigma_{k=1}^{D_j}(R_{mk} - R_m)^2}$$

where D_j is the number of trading day returns (251) used to estimate the parameters for firm j, and S_j^2 is calculated
as follows:

$$S_j^2 = \frac{\Sigma_{k=1}^{D_j} AR_{jk}^2}{D_j - 2}$$

Finally, the test statistic Z_{T_1,T_2} for the null hypothesis that the $CAAR_{T_1,T_2}$ equals zero is defined as:

$$Z_{T_1,T_2} = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} Z_{T_1,T_2}^j$$

where

$$Z_{T_1,T_2}^j = \frac{1}{\sqrt{Q_{T_1,T_2}^j}} \sum_{t=T_1}^{T_2} SAR_{jt}$$

and

$$Q_{T_1,T_2}^j = (T_2 - T_1 + 1)\frac{D_j - 2}{D_j - 4}$$

To test the data, the null hypothesis that there is no effect on firm value from the voluntary disclosure of cybersecurity-related risk will be rejected if the Z-statistic is significant at the 0.10 level or less.

The generalized sign test is used as a nonparametric test of the impact of the announcements. For each trading day or month in the event periods the number of securities with positive and negative average abnormal returns (cumulative or compounded abnormal returns for windows) is calculated. The generalized sign test statistic controls for the normal asymmetry of positive and negative abnormal returns in the estimation period. The significance levels for the generalized sign test are calculated. The null hypothesis for the generalized sign test is that the fraction of positive returns is the same as in the estimation period. For example, if 46% of market adjusted returns are positive in the estimation period, while 60% of firms have positive market adjusted returns on event Day −1, then the test reports whether the difference between 60% and 46% is significant at the five percent, one percent, or one tenth of one percent level. The actual test uses the normal approximation to the binomial distribution. For examples of the generalized sign test in the literature, see Sanger and Peterson (1990), Singh, Cowan and Nayar (1991), and Chen, Hu and Shieh (1991).[136]

2. Results.

The exact date of the voluntary disclosure of cybersecurity-related risk, the date of the 10-K or 10-Q statement, is the event date in the empirical study (Day 0). The results for the event study on the date of the voluntary disclosure of cybersecurity-related risk are listed in Table 6 for various event periods. Given the null hypothesis that there is no impact on firm value from the voluntary disclosure of cybersecurity-related risk, the event day (Day 0) Average Abnormal Return is -0.23%, which is statistically different from zero at the .05 level of significance (Z = -2.195). Of the 184 observations, 108 had negative abnormal returns on Day 0 versus 76 with positive observations. This difference is statistically significant at the .05 level of significance (the generalized sign test statistic is -1.948). This result supports our $H1_A$ that the voluntary disclosure of cybersecurity-related risk announces an increase in risk resulting in significant negative abnormal returns on the event date.

As is clear from the results reported in Table 6, below, the most statistically significant dates for measuring the impact on firm value from the voluntary disclosure of cybersecurity-related risk announcements are the event date (Day 0) and the two-day interval including the event date and the previous trading day ($CAR_{-1,0}$). Many event studies, specifically accounting research that studies the impact of disclosure information in annual statements and/or quarterly statements, use a two-day event period. The $CAR_{-1,0}$ is a negative -0.30%, highly statistically significantly different from zero at the .05 level (the Patell Z statistic equals -2.051). In a manner consistent with Park, Lee and Song (2014) who reported statistical significance using the t statistic, we tested the standard error specified for each event interval across securities (as compared to the Patell method that computes portfolio standard errors from the time series of estimation period portfolio abnormal returns with autocorrelation adjustments). The t statistic of

[136] Gary C. Sanger & James D. Peterson, "An Empirical Analysis of Common Stock Delisting," 25(2) JOURNAL OF FINANCIAL AND QUANTITATIVE ANALYSIS __ (1990); Ajai Singh, Arnold R. Cowan & Nandkumar Nayar, "Underwriting Calls of Convertible Bonds," 29(1) JOURNAL OF FINANCIAL ECONOMICS __ (1991); Haiyang Chen, Michael Y. Hu & Joseph C.P. Shieh, "The Wealth Effect of International Joint Ventures: The Case of U.S. Investment in China," 20(4) FINANCIAL MANAGEMENT __ (1991). Chen, Hu and Shieh (1991) refer to the test as a binomial sign test. For a more detailed explanation of the generalized sign test, see Peter Sprent, APPLIED NONPARAMETRIC STATISTICAL METHODS ___ (1989), and Arnold Cowan, "Nonparametric Event Study Tests," 2(3) REVIEW OF QUANTITATIVE FINANCE AND ACCOUNTING __ (1992). Cowan (1992) reports that the generalized sign test is well specified for an event date variance increase and more powerful than the cross-sectional test.

1.400 is statistically significantly different than zero at the 10% level and conforms with the economic and statistical significance of the negative impact on securities prices from the voluntary disclosure of cybersecurity-related risk announcements on the event date. Of the 184 observations 106 had negative abnormal returns during Days (-1,0) versus 78 with positive observations. This difference is statistically significant at the 5% level of significance (the generalized sign test statistic is -1.505). This result supports our $H1_A$ that there is a statistically significant negative impact on firm value from the voluntary disclosure of cybersecurity-related risk announcements.

Table 6. The Event Study Results Using the Market Model with the CRSP Value Weighted Index

Days	N	Mean Cumulative Abnormal Return CAR	Wtd. CAAR	Positive: Negative	Patell Z	CSectErr t	Gen Sign Z
(-10,-1)	184	0.29%	-0.02%	84:100	-0.099	0.511	0.768
(-5, -1)	184	**0.60%**	0.29%	91:93	1.085	1.313$	0.265
(-1,0)	**184**	**-0.30%**	**-0.34%**	**78:106<**	**-2.051**	-1.400$	**-1.653***
(0)	**184**	**-0.23%**	**-0.26%**	**76:108<**	**-2.195***	-1.337$	**-1.948***
(0, +1)	184	-0.08%	-0.16%	87:97	-0.973	-0.278	-0.325
(-1, +1)	184	-0.16%	-0.24%	84:100	-1.218	-0.512	-0.768
(+1, +5)	184	0.30%	0.13%	98:86)	0.478	0.776	1.298$
(+1, +10)	184	0.21%	0.36%	95:89	0.896	0.403	0.855
(-5, +5)	184	0.68%	0.16%	85:99	0.363	1.104	-0.620
(-10, +10)	184	0.28%	0.09%	95:89	0.021	0.339	0.855
(-20, +20)	184	0.09%	-0.59%	79:105(	-0.816	0.084	1.505$

(Note: The symbols $,*,**, and *** denote statistical significance at the 0.10, 0.05, 0.01 and 0.001 levels, respectively, using a generic one-tail test. The symbols (,< or),> etc. correspond to $,* and show the direction and significance of the generalized sign test. Statistics at the .05 level of significance or lower are in bold.)

These results indicate a statistically and economically significant negative impact on firm value is perceived by investors with the voluntary disclosure of cybersecurity-related risk in a firm's 10-K and/or 10-Q statements. This outcome is consistent with investors believing that there is a significant increase in firm risk from the disclosure of the firm deciding that its cybersecurity exposure warrants a voluntary statement about this risk. With no change in future cash flows, an increase in cybersecurity risk would increase the discount rate, thus lowering the present value of the stock. On the other hand, the voluntary disclosure of cybersecurity-related risk could indicate that future cash flow estimates need to be adjusted to reflect increased costs of monitor the firm's information systems, or require additional expensive software versus

cyberattacks, or increased costs of losses from cyberattacks, etc. If the risk in terms of the discount rate stays the same, but future estimates of cash flows decrease from the voluntary disclosure of cybersecurity-related risk announcements, then the present value of the stock would decline. Of course, investors could consider that both of these factors may change, thus negatively impacting firm value. All these scenarios support the findings in this empirical research.

C. Follow-up to SEC Comment Letters.

In order to gain further insight on firm reasons for expanding cybersecurity risk factor disclosures, we also examined firm responses to SEC comment letters that referenced the October 13, 2011, guidance on cybersecurity risk. During the period from October 13, 2011 to May 16, 2015, we identified 68 responses through searching the Westlaw EDGAR database for comment letters. Of these 68, 54 responses addressed regular disclosures in Form 10K or 20-F (an annual reported filed by foreign firms), with the balance addressing registration statements filed on Form S-1 or other similar forms.

Focusing on regular annual disclosures, we found that a majority of responses (31/54 or 57.4%) affirmed the company's position that its disclosure was in compliance with the SEC guidance and made no offer to change future disclosures. Only five registrants (9.3%) affirmed their compliance with the guidance but nevertheless agreed to make changes in future regular disclosures. Thus, two-thirds of the responses (36/54 or 66.67%) reflected the registrant's belief that their disclosures were already in compliance with the SEC guidance. In eighteen cases (33.3%), firms responded with an agreement to augment, enhance, or revise a future disclosure, with a four responses agreeing to make a correcting disclosure on Form 10-Q, rather than waiting for the next 10-K.

Among the thirteen responses addressing registration of new securities, seven (53.8%) affirmed compliance and made no changes, while only one (7.7%) affirmed compliance while agreeing to make a revision. Five responses (38.5%) simply agreed to augment or revise their registration statement without asserting their compliance.

The SEC letter generally disclosed the reasons for initiating the inquiry. In fifty-eight cases, the registrant's affirmative statements concerning cybersecurity risks in the relevant disclosure triggered the SEC comment letter. Public statements by employees triggered two inquiries, while news accounts of cybersecurity incidents affecting the registrant or affiliated firms triggered five inquiries. It thus appears that the SEC is being proactive in reaching outside the scope of the particular disclosure. Registrants should thus be concerned about securities registrations whenever cybersecurity breaches are disclosed, and even when their employees talk about assessing cybersecurity risks at public events.

In some of these cases involving affirmative statements, the SEC asked firms to contextualize their risk factor disclosure by discussing past cybersecurity risks. The source of these inquiries is unclear, but could involve other disclosures or suspicion based on the experiences of others in the industry. Most registrants responding to this invitation declined to provide additional details, noting that any attacks had not been successful or if they had, the financial impact was not material to the firm. Extant risks were not perceived to be sufficient,

particularly when considered in the firm-specific context of risk, rather than a risk to the entire industry. Moreover, many firms also noted that the financial impact of any cybersecurity breaches or attacks had not been material.

Silence about cybersecurity risks appears to have triggered the SEC inquiry in only seven cases. For these firms, the SEC expected to see cybersecurity risk factors, and when it did not, it pushed firms to see if disclosure was warranted. In all but one of these seven cases, registrants ultimately agreed to make revisions or new disclosures. However, one firm resisted any changes based on its assessment of compliance with the guidance, including the absence of any firm-specific risk to disclose.[137] To the extent that some firms altered or expanded disclosures, further research may be in order to ascertain whether changes in reporting altered market perceptions about the firm.

V. Conclusions.

Firms seem to have responded cautiously to the SEC's guidance concerning cybersecurity risks. Despite the pervasive nature of cybersecurity risks across a broad range of industries, only a small percentage of firms potentially affected by such risks have undertaken affirmative risk factor disclosures in response to the guidance. While one might expect that adding yet another item to a list of risks affecting the firm in the annual Form 10-K would not trigger an adverse reaction from the marketplace, our empirical data suggest otherwise.

Firms that disclosed cybersecurity risks were indeed punished by investors. This adverse market reaction suggests that caution was indeed the appropriate response from the firm's perspective. Although some firms might have concluded that disclosures might provide a favorable outcome from signaling that management was attentive to concerns in the cybersecurity environment, the investor response suggests a different signaling function was operating here.

Given that the guidance did not contain any new rules requiring disclosure, firms could likely comply with the guidance without choosing to engage in additional disclosures. Those who chose not to disclose may be implying that their cybersecurity efforts are adequate to address the risks that their firms may be facing, but securities laws do not treat this as an affirmative and actionable statement. Unfortunately for those who do add cybersecurity risk factor disclosures, they may be unintentionally suggesting that they have firm-specific risk. When only some firms respond with disclosure, while others remain silent, the market appears to conclude that a disclosure suggests additional risks. The empirical data here suggest that the market is amenable to that suggestion through sending a negative impact on stock price in response to the firm's signal.

EM/VR/JW

[137] See Nucor Corp. (May 17, 2012).