Journal of Business Ethics (2023) 187:199–224
https://doi.org/10.1007/s10551-022-05107-z

REVIEW PAPER

Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach

Jing Chen[1] · Elaine Henry[2] · Xi Jiang[3]

Received: 9 July 2021 / Accepted: 20 February 2022 / Published online: 19 April 2022

Abstract

By examining managers' decisions about disclosing updated assessments of firms' risks, we present evidence that the risk factor disclosures are informative. We use the setting of cybersecurity risk factor disclosures after a data breach because data breaches, especially severe breaches, serve as a natural experiment where an exogenous shock to managers' assessment of their firm's cybersecurity risks occurs. We analyze the topic from the perspective of two different theoretical lenses: the economic lens of optimal risk exposure and the ethical lens of stakeholder theory. Using a sample of firms experiencing data breaches, we find that firms experiencing a data breach increase the amount of cybersecurity risk factor disclosures compared to matched firms with no data breach. Further investigation reveals that the severity of data breaches affects the results; cybersecurity risk factor disclosures increase only after severe data breaches. While there is no significant market reaction if breached firms' subsequent annual reports include increased cybersecurity risk factor disclosures, a significant negative market reaction occurs if breached firms decrease cybersecurity risk factor disclosures, regardless of the severity of the breach, implying that the market anticipates increased disclosures after data breaches.

Keywords Cybersecurity risk factor disclosures · Cyber business ethics · Data breach

Introduction

Beginning in 2005, the US Securities and Exchange Commission (SEC) required all firms (other than asset-backed issuers) to include a risk factor section in their periodic filings to discuss the most significant factors that make an investment in the company risky (Regulation S-K, Item 105, SEC, 2005). Risk factor disclosures inform market participants of the risks that a firm faces, consistent with the SEC's objectives (Campbell et al., 2014, 2019; Chiu et al., 2018; Hope et al., 2016; Li et al., 2018). However, doubts about the informativeness of risk factor disclosures still linger among practitioners, researchers, and regulators (Berkman, 2018; Johnson, 2010; Malone, 2005; SEC, 2016). Critics argue that firms may simply disclose all the possible risks using generic and repetitive language (i.e., boilerplate) and risk factor disclosures have become less reflective of firms' underlying economic risks in the post financial crisis period (Beatty et al., 2019). The SEC has repeatedly reminded firms to avoid generic risk factor disclosures (SEC, 2010, 2011, 2019).[1]

Understanding the informativeness of risk factor disclosures is important as these disclosures represent an average of 11.0% of the total words in firms' 10-K filings (Campbell et al., 2014). Among risk factor disclosures, cybersecurity risk disclosures are particularly important. The importance of these disclosure decisions is intensified by an ever-growing number of data breaches raising serious concerns

✉ Jing Chen
jchen4@stevens.edu

Elaine Henry
ehenry1@stevens.edu

Xi Jiang
xjiang12@stevens.edu

[1] School of Business, Stevens Institute of Technology, 414 Babbio Center, Hoboken, NJ 07030, USA

[2] School of Business, Stevens Institute of Technology, 408 Babbio Center, Hoboken, NJ 07030, USA

[3] School of Business, Stevens Institute of Technology, 220 North Building, Hoboken, NJ 07030, USA

[1] More recently, the SEC has undertaken efforts to improve risk factor disclosures by mandating a summary risk factor disclosure of no more than two pages if the risk factor section exceeds 15 pages, replacing the requirement to discuss the "most significant" risks with "material" risks, and requiring filers to organize their risk factor disclosure under relevant headings (SEC, 2019).

about corporate cybersecurity. Costs of data breaches can be significant. For example, the 2017 Equifax data breach affected as many as 143 million consumers in the USA and cost Equifax over $650 million on information technology and data security recovery, legal and investigation fees, and product liability (Cowley, 2019). In August 2019, the hotel giant Marriott booked a $126 million charge tied to a data breach that compromised up to 327 million guest records of passport and credit card information (Armental, 2019). While the ethics literature mentions the responsibilities of breached firms to disclose data breach information when a breach occurs (Morgan & Gordijn, 2020), we focus on firms' responsibilities for changing risk factor disclosures following a breach. In our study, we investigate whether risk factors disclosures are used to inform investors about the changes in managers' assessments of firms' risks. In particular, we focus on the setting of cybersecurity risk factor disclosures after a data breach because data breaches, especially severe breaches, serve as a natural experiment where an exogenous shock to managers' assessment of their firm's cybersecurity risks occurs.

We analyze the topic from the perspective of two different theoretical lenses: the economic lens of optimal risk exposure and the ethical lens of stakeholder theory. In the context of economic theory of cost/benefit-based risk optimization, Kamiya et al. (2021)'s model assumes a firm with optimal exposure to cyber risk in which pre-attack risk exposures are optimally managed and fully priced by capital providers. The model's implications are that a cyberattack would result in a change in post-attack policies (including risk disclosure) of a firm with an optimal exposure to cyber risk only if the cyberattack caused managers to alter their assessment of the loss distribution for cyberattacks. In other words, as managers learn from the attack that the loss distribution is different from what they believed it to be, they will adjust the firm's disclosures and policies to reflect their new understanding of the loss distribution (Kamiya et al., 2021).[2] An increase in cybersecurity risk disclosures resulting from a material change in risk assessments would also be consistent with the SEC risk factor disclosure mandate.

We argue, however, that a reassessment of loss distribution following a cyberattack is a necessary but not sufficient condition for an increase in post-attack cyber risk disclosure because managers face competing incentives. On one hand, managers face business and career incentives to suppress negative information, including concerns about the negative impact on firm valuation, cost of capital, debt contract negotiations, and executive compensation and career opportunities (Fields et al., 2001; Hermalin & Weisbach, 2012; Kothari et al., 2009; Nagar et al., 2003; Watts & Zimmerman, 1986). Following a security breach, managers could elect to leave risk disclosures unchanged or issue noninformative boilerplate disclosures. On the other hand, they also face competing motivations to provide at least some meaningful cybersecurity risk factor disclosures updates, including motivations such as mitigating litigation risk should the firm and its securities not perform as expected (Nelson & Pritchard, 2016; Skinner, 1994), responding to public scrutiny, and/or deterring potential future cyberattacks by signaling raised costs to penetrate cyber-defenses (Schechter & Smith, 2003).

Given management's competing motivations, an ethical lens complements the economic analysis. In the context of stakeholder theory as articulated in Wickset al. (1994), corporate cybersecurity and related risk disclosures are critical topics because they impact capital providers, managers and employees, and society as a whole.[3] The cyber environment's trust-dependent interconnectedness arguably epitomizes the essence of stakeholder theory's interconnected relationships within which managers must act. Moreover, the cyber environment is a common good, the protection of which is as much a shared responsibility as is the protection of the physical environment. Cybersecurity involves taking appropriate actions and making ethical decisions to mitigate cyber risks, and increasing cybersecurity risk disclosures can be viewed as an ethical decision (Radu & Smaili, 2021). The argument in Morgan and Gordijn (2020), namely that "non-disclosure [of a breach] contributes to the weakening of an already fragile cyber environment" is also applicable to decisions about risk disclosures following a breach. An increase in the risk disclosure following a breach event can be viewed as a signal of a more ethical corporate response.[4]

[2] Indeed, the SEC views information related to cybersecurity risks and incidents as material nonpublic information and encourages the companies to take codes of ethics into account to prevent trading on the basis of such information (SEC, 2018). A related recent study by Berkman et al. (2021) finds that for firms that are less protected from digital insiders– hackers who target corporations to obtain nonpublic corporate information for illegal trading– a larger share of new earnings information is incorporated into prices prior to earnings announcements and pre-announcement trading by short sellers is more predictive of earnings surprises for these firms, suggestive of informed trading.

[3] As explained in Morgan and Gordijn (2020, p. 124), the original tenets of stakeholder theory were later reinterpreted by the original authors in Wicks et al. (1994), a work that incorporates principles of care ethics and "considers corporations as webs of relations among stakeholders whose interests need to be at the core of decision-making processes." In *The Ethics of Cybersecurity*, Morgan and Gordijn (2020) apply principles from this care-based stakeholder theory as articulated in Engster (2011) to address businesses' responsibilities when confronting ransomware attacks.

[4] According to Lewis (1985, p. 383), "business ethics involves the application of one's understanding of what is morally right and truthful at a time of ethical dilemma." Given information disclosed about cybersecurity risks is informative and useful for investors when assessing the probability of future incidents, Radu and Smaili (2021)

Despite numerous reasons to expect an increase in firms' cybersecurity risk factor disclosures following a data breach, the evidence in prior accounting research on this subject is mixed. In a study most closely related to ours, Hilary et al. (2016) find no significant increase in the amount of combined disclosure about cybersecurity risks in the risk factor section and management discussion and analysis (MD&A) section in firms' annual reports following a data breach. They conclude that such breaches are not especially relevant, titling their work "Who cares?". Are we to conclude that, on average, managers do not change their cybersecurity risk assessments following a breach and/or if they do, they fail to behave ethically by updating disclosures? We hypothesize instead that the approach to identify cybersecurity risk disclosures in Hilary et al. (2016) is deficient as it employs a more limited keyword list compared with other cybersecurity risk-related keyword lists (Ghadge et al., 2019; Li et al., 2018.)[5] In this study, therefore, we utilize a more complete keyword list to measure cybersecurity risk factor disclosures.

Our work is also related to a study by Gao et al. (2020) which examines cybersecurity disclosures in various sections of annual reports for 112 representative sample firms from 2007 to 2018 and find that firms' cybersecurity risk disclosures are longer when the disclosures describe a prior cyber incident. Their study differs from our study in that it uses firms' self-reporting of cyber incidents within 10-Ks as the firm-specific indication of cybersecurity risk and relates the quantity of disclosure to a variable capturing whether the disclosure mentions a prior cyber incident.[6] We focus instead on the informativeness of firms' cybersecurity disclosures in the risk factor section of the 10-K filed after an announced data breach, whether or not such disclosures specifically mention the prior cyber incident. Moreover, to focus on the impact of the incident, we use a control sample of firms that did not experience a data breach.

Using a sample of 558 firm-years, representing 279 firm-years with data breaches and their matched control firm-years, we measure the amount of cybersecurity risk factor disclosures within the firms' annual reports issued before versus after the occurrence of a data breach. We find that while both breached and non-breached firms on average increase the amount of cybersecurity risk factor disclosures consistent with the secular trend of lengthening risk factor disclosures, the increase is significantly greater for breached firms compared to non-breached firms. We provide evidence suggesting that Hilary et al.'s (2016) lack of similar findings was likely due to measurement deficiencies. Further, we find that the increase in cybersecurity risk factor disclosures is present only when a firm has experienced a severe data breach, where the severity is measured based on the type of data breached, the amount of data breached, the source of the breach, and whether the hackers used the breached data. Our evidence that firms experiencing a data breach increase the amount of cybersecurity risk factor disclosures is consistent with management transparently providing information about their elevated assessment of the firm's cybersecurity risks after a data breach.

We further investigate how the stock market values managers' transparency. Our analysis of the market reaction to changes in firms' cybersecurity risk factor disclosures following a data breach focuses on the three-day abnormal returns around the filing date of the 10-K immediately after a data breach. Consistent with the market anticipating increased disclosures, no significant market reaction is observed if the amount breached firms' cybersecurity risk factor disclosure increases, while a negative market reaction is observed if the amount of disclosure instead decreases. Interestingly, our results also imply that while investors may be aware of the severity of a data breach at the announcement of the breach incident, investors penalize breached firms for subsequently decreasing cybersecurity risk factor disclosures regardless of the severity of the breach. One interpretation is that investors' concern over the firms' ethics is intensified when breached firms suppress their cybersecurity risk factor disclosures. Such finding supports the conjecture in Radu and Smaili (2021) that increasing cybersecurity risk disclosure after a data breach may be viewed as an ethical decision by managers.

In response to an increase in high-profile cyberattacks, the SEC enhanced its scrutiny of firm's disclosures of cybersecurity risks and their policies, procedures, and controls in place to address these risks. The staff of the SEC's Division of Corporation Finance issued *CF Disclosure Guidance: Topic No. 2*, which requires firms to disclose the risks of cyber incidents that "are among the most significant factors that make an investment in the company speculative or risky" (SEC, 2011). The amount of cybersecurity risk factor disclosures across all companies increased following

Footnote 4 (continued)

conjecture that, "increasing cybersecurity risk disclosure might be viewed as an ethical decision by organizations (managers and the board of directors)."

[5] Li et al.'s (2018) examination of the association between cybersecurity risk factor disclosure and subsequently reported cybersecurity incidents uses a keyword list to identify the presence of cybersecurity risk factor disclosure. Ghadge et al.'s (2019) literature review of cyber risk in supply chains uses a list of search strings to identify research papers in the relevant fields. Details on these keyword lists are in Sect. 3.2 and 3.4.

[6] In addition, Gao et al. (2020) examine the Form 10-K sections on business (Item 1), risk factors (Item 1A), MD&A (Item 7), and financial statement and supplementary data (Item 8), in contrast with our focus on risk factor disclosures.

the 2011 guidance.[7] Given our focus on the differential disclosures by breached versus non-breached firms, we examine whether cybersecurity risk factor disclosures following a data breach are affected by this SEC guidance.[8] We divide our sample period into the pre- and the post-2011 SEC guidance subperiods. In both subperiods, we find that the breached firms increase cybersecurity risk factor disclosures more than matched non-breached firms, and the magnitude of the relative increases in breached firms' cybersecurity risk factor disclosures does not change significantly from the pre- to the post-2011 period.

Having presented evidence of increased cybersecurity risk factor disclosures following a severe data breach, we examine alternative motivations for this change. Specifically, we analyze reaction to public scrutiny, potential cyberattacks deterrence, and litigation risk mitigation as motivations for managers to increase cybersecurity risk factor disclosures after data breaches. Using media attention to cybersecurity issues of breached firms as our proxy for investors' scrutiny regarding the firm's cybersecurity risks, we find that firms increase cybersecurity risk factor disclosures after a severe data breach even more when the firm's cybersecurity issues receive greater media attention in the period between the announcement of a breach and the subsequent 10-K filing date. This finding suggests that responding to public scrutiny, i.e., attention from a broad array of stakeholders, is an important factor in managers' decisions to revise cybersecurity risk factor disclosures. We also find some evidence of a reduced likelihood of recurring data breaches to breached firms that increase cybersecurity risk factor disclosures, suggestive of disclosures having some deterrence effect. In contrast, our evidence suggests that prevention of litigation is not a dominant factor for increasing cybersecurity risk factor disclosures.

Our paper contributes to the literature on cybersecurity issues and cyber business ethics. This research stream provides much evidence of the negative market and economic consequences of cyber incidents (Campbell et al., 2003; Cavusoglu et al., 2004; Haislip et al., 2019; Kamiya et al., 2021; Spanos & Angelis, 2016), suggesting cybersecurity risk is significant for some firms. However, prior studies include limited and mixed results regarding the informativeness of cybersecurity risk factor disclosures. Hilary et al. (2016) find no significant increase in cybersecurity risk disclosures after a data breach, implying cybersecurity risk disclosures in the risk factor section and the MD&A are not informative while Li et al. (2018) find a positive association between cybersecurity risk factor disclosures and subsequently reported cyber incidents, implying the risk disclosures are informative, at least as predictors of future data breaches. Our study reconciles the contradicting results of those two studies by revisiting managers' disclosure decisions after data breaches and utilizing a more comprehensive keyword list to identify interested disclosures. Our study also complements Amir et al.'s (2018) examination of managers' decisions to withhold disclosures of the occurrence of a data breach. We extend the investigation to managers' decisions to update risk factor disclosures in annual filings after a data breach is known to have ocurred.

We extend the efforts by Radu and Smaili (2021) in studying cyber business ethics, the intersection of business ethics and cyber ethics, two ethical areas developed separately by researchers over time (Patrignani & Whitehouse, 2014).[9] We provide direct evidence consistent with management intent to inform investors and other stakeholders about increases in their assessments of a risk the firm faces by increasing risk factor disclosures. While economic theory provides a rational explanation for increases in post-attack cyber risk disclosures, applying a theoretical lens from ethical stakeholder theory enhances our understanding of the observed outcomes.

Our paper also adds to the literature on risk factor disclosure. Prior studies rely on investors' reactions to disclosed risk factors (Campbell et al., 2014; Chiu et al., 2018; Hope et al., 2016) or the realization of a specific type of risks (Campbell et al., 2019; Li et al., 2018) to infer the informativeness of risk factor disclosures. Our paper adopts the notion in Radu and Smaili's (2021) work that certain risk factor disclosures constitute an ethical issue. From a practical perspective, our work may be informative to firms' financial and investor relations management as they craft appropriate responses following cyber incidents.

Finally, our paper also contributes to the literature on computerized content analysis of disclosure narrative by highlighting the importance of comprehensive, yet targeted keyword lists in measuring the amount of a specific type of disclosure.

[7] "After the issuance of the guidance, many companies included additional cybersecurity disclosure, typically in the form of risk factors" (SEC, 2018, p. 6). See also Gordon et al. (2006), Morse et al. (2017), and Gao et al. (2020).

[8] In 2018, the SEC approved updated guidance on cybersecurity risk disclosures. Because 2018 is the end of our sample period, our analysis does not investigate any impact of this 2018 SEC guidance on disclosures.

[9] Cyber business ethics involves the study of the ethical decisions of firms (managers, boards of directors and employees) when dealing with information technology (Radu & Smaili, 2021). It is a combination of business ethics, as defined in business research, and cyber ethics, as viewed by engineering research.

Background, Literature Review, and Hypothesis Development

Risk Factor Disclosures

Disclosure of risk factors associated with securities offerings has long been required in Security Act registration statements. In 2005, the SEC extended risk factor disclosure requirements. Specifically, the SEC mandated that public firms (other than asset-backed issuers) must disclose the most significant risk factors in annual reports on Form 10-K in a new item (Item 1A risk factors) and update them quarterly for any material changes (Regulation S-K, Item 105, SEC, 2005). The SEC regulation states that the inclusion of a separate risk factor section "enhance[s] the contents of Exchange Act reports and their value in informing investors and the market" (SEC, 2005). Critics of the newly required risk factor disclosures contend that they are likely not as informative as the SEC expects. Although the risk factor section is mandatory, firms have a great degree of discretion over the disclosed content. Since the new rule does not require firms to estimate the likelihood that risks will be realized or to quantify the potential impact of the risks on their economic conditions, firms may simply disclose all the possible risks and uncertainties in a vague and boilerplate way (Ernst & Young LLP, 2005; IRRC, 2016; Johnson, 2010; Malone, 2005).[10]

Researchers respond to the debate and examine uses of the newly mandated risk factor disclosures by equity and debt market participants, mostly providing supporting evidence that the newly mandated disclosures are not boilerplate (Campbell et al., 2014, 2019; Chiu et al., 2018; Hope et al., 2016; Li et al., 2018).[11] Campbell et al. (2014) find that Item 1A risk factor disclosures increase investors' perceptions of the firm's risks proxied by stock return volatility and market beta, and reduce information asymmetry proxied by bid-ask spread. They further document a negative association between the disclosed risk factors and abnormal returns around the 10-K filing date, suggesting investors incorporate the information from risk factor disclosures into the stock price. Hope et al. (2016) find that more specific risk factor disclosures lead to larger stock price movement and trading volume around the 10-K filing date, indicating that more specific risk factor disclosures provide greater benefit to investors. Chiu et al. (2018) investigate the relevance of the newly mandated disclosures to creditors. They find credit default swap spreads decrease significantly after the SEC mandate of risk factor disclosures. Using settings of specific risk factors, Li et al. (2018) and Campbell et al. (2019) provide evidence that disclosures of specific risk factors inform investors about corresponding risks. Li et al. (2018) find a positive association between disclosed cybersecurity risk factors and future reported breach incidents. Campbell et al. (2019) find a negative association between disclosed tax risk factors and firms' tax-related cash payments over the subsequent years, implying tax risk factor disclosures relate to tax positions that are rewarded with future tax savings.

Prior research mainly relies on investors' reactions to disclosed risk factors (Campbell et al., 2014; Chiu et al., 2018; Hope et al., 2016) or the realization of a specific type of risks (Campbell et al., 2019; Li et al., 2018) to infer the usefulness of risk factor disclosures. An exception is Campbell et al. (2014), in which they probe managers' decisions and provide direct evidence that managers use risk factor disclosures to reflect the risks their firm faces. They decompose risk factor disclosures into five subcategories based on the different types of risks including financial, tax, legal, other systematic, and other idiosyncratic risks. They document the extent of risk factor disclosures about each risk type is positively related to the extent of this type of risk measured prior to the disclosure. Our study is along this line; while Campbell et al. (2014) examine managers' decisions over the amount of risk factor disclosures to reflect the level of existing risks, we explore managers' decisions to change the amount of risk factor disclosures to reflect changes in their assessments of a risk that the firm faces. To enhance our understanding of managers' decisions, our paper adopts the notion in Radu and Smaili's (2021) work that certain risk factor disclosures constitute an ethical issue.

Data Breaches and Cybersecurity Risk Disclosures

Data breaches have become more frequent and salient in recent decades (Audit Analytics, 2020). Breached firms not only incur considerable direct costs for activities like technical investigations, public relation campaigns, and litigation, but also suffer from more substantial indirect costs for brand name devaluation, increased costs to raise capital, and damaged customer relationships (Deloitte, 2016). In a 2017 survey, 87% of consumers surveyed said they would

[10] Other practitioners claim that a new risk factors section is not necessary because firms already included risk disclosures in various sections of their annual reports. For example, Intel Corporation's comment letter on the proposed regulation stated that Item 101 of Regulation S-K (description of business) and Item 303 (management's discussion and analysis) are highly risk-oriented, so it would be "both duplicative and confusing" to add an item on risk factor disclosure (Intel, 2005).

[11] An earlier study Kravet and Muslu (2013) examine risk disclosures in the whole 10-K filings for a period of 1994 to 2007 that mostly precedes the SEC mandate of risk factor disclosures. They find increased qualitative risk disclosures in a firm's 10-K filing is associated with increased stock return volatility and more dispersed analyst forecast revisions around the filing date, suggesting that qualitative risk disclosures increase investors' perceived risks.

take their business elsewhere if they don't trust that a company is handling their data responsibly (PwC, 2017). Using individual customer transaction data from a publicly owned retailer headquartered in the USA, Janakiraman et al. (2018) find that affected customers decrease their spending level by 32% after an announced data breach. Equity and debt investors are aware of elevated cybersecurity risks and react to an announcement of data breaches. Equity investors react negatively to announcements of data breaches, especially to breaches that involve unauthorized access to confidential data (Campbell et al., 2003; Cavusoglu et al., 2004; Kamiya et al., 2021).[12] Breached firms face higher bank loan spreads and stricter collateral and covenants requirements (Huang & Wang, 2021).

The SEC's 2005 mandate requires disclosure of a firm's most significant risk factors. To the extent that a firm faces significant cybersecurity risks, these risks should be disclosed in the Item 1A risk factor section of Form 10-K. However, practitioners complain that firms' cybersecurity risk factor disclosures are boilerplate repeated year after year, a criticism common for risk factor disclosures in general, and one critic cited anecdotal evidence of a firm failing to update cybersecurity risk assessment even after experiencing cyber incidents (Bennett, 2015). In response to an increase in high-profile cyberattacks, the SEC enhanced its scrutiny of firm's disclosures of cybersecurity risks and their policies, procedures, and controls in place to address these risks. In 2011, the staff of the SEC's Division of Corporation Finance issued *CF Disclosure Guidance: Topic No. 2*, which requires firms to disclose the risks of cyber incidents that "are among the most significant factors that make an investment in the company speculative or risky" (SEC 2011). In addition to disclosing the risks of potential cyberattacks, companies need to disclose the known material cyber incidents that already happened and discuss the potential costs and consequences.

Following the 2017 Equifax breach and the SEC's 2017 own EDGAR database breach, the SEC approved updated guidance for firms to prepare cybersecurity risk disclosures in 2018 (SEC 2018), reemphasizing the importance of cybersecurity procedures with detailed guidance and encouraging firms to develop comprehensive cybersecurity policies and procedures to properly assess the cybersecurity risks and to periodically review the cybersecurity disclosure controls.[13] Although the 2018 Guidance was approved unanimously by the SEC commissioners, several commissioners felt that the new guidance did not go far enough. For example, the SEC Commissioner Kara Stein stated, "the guidance does not sufficiently advance the ball—even in the context of disclosure guidance" and questioned whether the Commission was essentially just "re-issuing staff guidance solely to lend it a Commission imprimatur" (Stein, 2018). The SEC's plans included continued evaluation of developments in cybersecurity disclosures and need for further guidance or rules (Clayton, 2018), and cybersecurity related disclosures continue to be a priority of the SEC (Gensler, 2021).

The debate on the need for further guidance on cybersecurity risk disclosures could be advanced by a clear understanding of the information content of the present cybersecurity risk disclosures. Gordon et al. (2006) and Wang et al. (2013) examine cybersecurity risk disclosures in periods mostly prior to the SEC 2005 mandate of risk factor disclosures. Gordon et al. (2006) find evidence of a positive impact of the Sarbanes–Oxley Act (SOX) on firms' voluntary disclosures of information security activities.[14] Wang et al. (2013) find when security risk factors involve risk-mitigating action terms, firms are less likely to be associated with future breaches, suggesting the nature of disclosures is important in predicting breaches. Berkman et al. (2018), Li et al. (2018), and Gao et al. (2020) examine firms' cybersecurity disclosures in periods after the SEC 2005 mandate. Berkman et al. (2018) construct a cybersecurity awareness index based on content in all sections of 10-K filings and find that firms that demonstrate cybersecurity awareness have higher market valuation. Li et al. (2018) focus on cybersecurity risk factor disclosures in Item 1A of 10-K filings and find a positive association between the disclosures and subsequently reported cyber incidents, implying cybersecurity risk factor disclosures are informative predictors of

[12] Hilary et al. (2016) find insignificant market reaction to the announcements of data breaches. Their study, however, does not distinguish different types of breaches.

[13] On September 20, 2017, the SEC announced that Electronic Data Gathering, Analysis, and Retrieval system (EDGAR), its on-line database for receiving, storing, and publishing corporate securities filings, had been compromised in 2016 by hackers who may have traded on material nonpublic information obtained. The SEC noted, "It is believed the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission, or result in systemic risk." (SEC, 2017) Nevertheless, it is reportedly working with relevant parties to determine if data from millions of corporate disclosures have been put to illegal use (Burns 2017).

[14] Although SOX does not explicitly address the issue of information security, the definition of internal control combined with the fact that the reporting systems in all firms required to comply with SOX are based on computer-based systems imply that more focus on information security is a necessary compliance requirement (Gao et al., 2020).

future data breaches. Gao et al. (2020), analyzing cybersecurity disclosures in various sections of Form 10-K, observe a significant increase in cybersecurity disclosures through time, with a noticeable spike following the 2011 SEC Guidance.[15] They find that Item 1A risk factor section is the most frequently used location for cybersecurity disclosures, except for disclosures about regulation risks and data breach incidents that are mostly detailed in Item 1 Business and Item 7 MD&A, respectively. Our study extends prior studies focusing on cybersecurity risk disclosures in the Item 1A risk factor section, which allows us to add evidence to the long lingering research question about the informativeness of risk factor disclosures. Further, our particular emphasis on managers' decision to change cybersecurity risk factor disclosures after data breaches informs the debate on the need for further guidance on cybersecurity risk disclosures.

Hypothesis Development

We focus on managers' decisions to change cybersecurity risk factor disclosures when they change their views of the firm's exposure to cybersecurity risks. The timing of any change in managers' assessments of cybersecurity risks is unobservable. But we expect the timing coincides with data breach incidents, given the considerable costs and the negative market consequence of data breaches that have been documented in prior literature.

We analyze the topic from the perspective of two different theoretical lenses: the economic lens of optimal risk exposure and the ethical lens of stakeholder theory as articulated in Wicks et al. (1994). In economics, Kamiya et al. (2021)'s model begins with a firm whose loss distribution of data breaches is known. Investors demand transaction terms commensurate with the firm's cybersecurity risk exposure, and in turn the firm spends more on actions that decrease the risk of attacks and thus improve the firm's transaction terms. In this scenario, a data breach provides a valuable signal to the firm and its investors about the cost of attacks and the likelihood of future attacks with the implication that managers will update their assessment of the loss distribution and thus increase expenditures to decrease the probability of an attack, invest more in risk management, and decrease willingness to take other risks (Kamiya et al., 2021). What about the firm's policy of risk factor disclosures? The SEC's 2005 mandate requires disclosure of a firm's most significant risk factors. To the extent that a data breach elevates the significance of cybersecurity risks such that managers of breached firms change their risk assessments, the risk factor disclosures should be updated. As emphasized in SEC guidance, firms should "provide [risk] disclosure tailored to their particular circumstances and avoid generic 'boilerplate' disclosure" (SEC, 2011).

[15] Gao et al. (2020) identify cybersecurity related disclosures using the NICCS glossary of cybersecurity terms and classify disclosures into content categories.

Although managers should update material changes in the firm's cybersecurity risk assessment when cybersecurity is among its most significant risk factors, managers face incentives that can create bias against providing unfavorable information such as information about cybersecurity risks. Incentives creating a bias against providing unfavorable information include concerns about the impact on firm valuation, cost of capital, debt contract negotiations, and executive compensation and career opportunities (Fields et al., 2001; Hermalin & Weisbach, 2012; Kothari et al., 2009; Nagar et al., 2003; Watts & Zimmerman, 1986). In our research setting, a data breach has previously been announced by the time when a firm files its 10-K. Decisions about risk factor disclosures thus go beyond the more temporal announcements of a breach incident, and avoidance of updated risk factor disclosures would serve to indicate that no material increase in assessed cybersecurity risks has occurred.

While managers face business and career incentives to suppress negative information, they also face competing motivations to provide at least some meaningful cybersecurity risk factor disclosures updates. A substantial literature connects firms' voluntary disclosure efforts with various benefits including decreased information asymmetry (Diamond & Verrecchia, 1991; Healy & Palepu, 2001), reduced litigation risk (Skinner, 1994), and increased analyst coverage and institutional investor ownership (Bushee & Miller, 2012; Lang & Lundholm, 1996). Managers may use risk factor disclosures to alleviate litigation risk (Nelson & Pritchard, 2016; Skinner, 1994), and mitigation of litigation risk could thus motivate disclosure of breach incidents and updates to the firm's cybersecurity risk factor disclosures. Gordon et al. (2010) and Berkman et al. (2018) find firms that disclose proactive security activities and demonstrate cybersecurity awareness have higher market valuation. Furthermore, the revised disclosures likely deter future cyberattacks since economically rational hackers may shy away from expending resources to attack systems in which the cost of a successful attack has increased (Schechter & Smith, 2003).

Given the competing motivations of managers, it is helpful to analyze the situation in light of ethical stakeholder theory. Absent consideration of any stakeholder beyond shareholders and managers themselves, an economically rational manager's decisions to increase risk disclosures following a data breach would require a change in risk assessment and secondly a greater balance of motivation to disclose than not disclose. Ethical stakeholder theory as articulated in Wicks et al. (1994, p. 483) considers the firm as constituting "the network of relationships which it is involved in with the employees, customers, suppliers, communities, businesses and other groups who interact with and give meaning and definition to the corporation" and emphasizes the need to

share information. Managers can also utilize disclosures to signal to the public that the firm is actively engaged in detecting and correcting security breaches to respond to public scrutiny.

The amount of risk factor disclosures is linked to the level of corresponding risks to which the firm is exposed (Campbell et al., 2014). If motivations to suppress bad news dominate such that managers choose not to reflect their assessed greater exposure to cybersecurity risks in the Item 1A risk factor section, no change in the amount of cybersecurity risk factor disclosures after a data breach would be observed. On the other hand, if managers choose to inform investors of their assessments of greater exposure to cybersecurity risks, then an increase in the amount of cybersecurity risk factor disclosures would be observed.

Ultimately, it is an empirical question whether managers increase the amount of cybersecurity risk factor disclosures or not. Accordingly, we test the following hypothesis stated in an alternative form:

H1: Firms increase the amount of cybersecurity risk factor disclosures after experiencing data breaches.

After an attack, if neither the manager nor the firm's investors learn that the loss distribution is different from what they believed it to be, a financially unconstrained firm should not suffer a reputation loss from the cyberattack, and thus firm policies should not change (Kamiya et al., 2021). In this case, the cyberattack is the realization of a risk of which managers and investors are fully aware. In other words, reassessment of loss distribution is a precondition of an increase in risk disclosure. We distinguish between data breaches that change the firm's and its investors' assessment of the firm's loss distribution of cyberattacks and those that have no such impact.

Categorizing breaches by their primary effect in terms of confidentiality, availability, and integrity, Gordon et al. (2011) find that attacks associated with breaches of availability have the greatest negative effect on stock market returns. Campbell et al. (2003) find a highly significant negative market reaction for data breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information. Kamiya et al. (2021) study cyberattacks on public corporations involving data breaches from 2005 to 2017. They find out of 91 public disclosure events of first-time attacks within three years, 58 events are associated with negative abnormal returns in the three days around the announcement date. The negative market reactions are documented after a subset of data breaches suggest that investors change their assessments of the firm's risk or its risk appetite after a subset of, not all cyber incidents. This likely holds true for managers. Indeed, managers consider the severity of a data breach in their decisions to withhold reports of its occurrence to investors (Amir et al., 2018).

After a severe data breach, managers are more likely to revise their assessments of cybersecurity risks upward or revise their assessments by a larger extent. In these cases of severe breaches, managers' competing incentives—to update subsequent risk disclosures and to suppress indications of upward risks—are both exacerbated. Our second hypothesis, stated in an alternative form, is as follows:

H2: Firms increase cybersecurity risk factor disclosures more after experiencing a severe data breach.

We examine the market reaction to firms' changes in risk factor disclosure after experiencing a data breach. Prior research provides pervasive evidence of the information content and value relevance of firms' risk factor disclosures. Campbell et al. (2014) document the market reaction to unexpected risk factor disclosures and Hope et al. (2016) find the market reacts positively to more specific risk factor disclosures. In the context of disclosure covering cybersecurity issues, Gordon et al. (2010) find voluntary disclosures about information security in annual reports, especially those about proactive security activities, are associated with the firm's valuation three months after the fiscal year end, and Berkman et al. (2018) show a positive association between their self-developed firm-specific measure of cybersecurity awareness and firms' share price three months after the fiscal year end.[16] No prior research of which we are aware studies the market reaction to the changes in breached firms' cybersecurity risk factor disclosures, the interest of our study.

Our focus is not on market reaction at the time a data breach is announced, about which prior literature offers pervasive evidence, but on investors' reactions to firms' changes in cybersecurity risk factor disclosure in subsequent 10-K filings. At the discovery of a breach, investors reassess the loss distribution of the breached firm's cybersecurity risk and react negatively, particularly when the breach is severe (Campbell et al., 2003; Cavusoglu et al., 2004; Kamiya et al., 2021). Given the updated belief of the elevated cybersecurity risk has already been incorporated into the stock price at the time the data breach is announced, how will investors respond when observing changes in a breached firm's cybersecurity risk factor disclosures in the subsequent 10-K filing?

[16] Berkman et al. (2018) do not disclose the exact keyword list used in their process of identifying cybersecurity disclosures and creating their cybersecurity awareness measure. They also examine the tone in cybersecurity disclosure and find a more negative tone is associated with lower market value.

We expect the market reaction to changes in cybersecurity risk factor disclosures after a data breach depends on the type of change, i.e., increase or decrease in disclosures. Investors' elevated assessment of cybersecurity risk incorporated into the stock price at the breach announcement would be accompanied by an expectation of some increase in the breached firms' subsequent related risk factor disclosures. Thus, a decrease in the breached firms' cybersecurity risk factor disclosures following a data breach would be inconsistent with expectations resulting in a negative market reaction. Moreover, since increasing cybersecurity risk disclosures after a data breach may be viewed as an ethical decision by managers (Radu & Smaili, 2021), suppressing cybersecurity risk factor disclosures after a data breach can be a red flag in the firm's ethical conduct. In contrast, an increase in cybersecurity risk factor disclosures would be consistent with investors' expectations, thus resulting in little or no market reaction unless the amount or content of increased disclosure deviates from expectations. For example, if the amount of increased disclosure is less than the investors' expectation, the market reaction could be negative, similar to the scenario in which a breached firm decreased disclosures. If the content of the increased disclosures includes expanded risks beyond investors' expectations, the market reaction could also be negative while if the content of the increased disclosures includes additional risk prevention measures, the market reaction would likely be positive. We therefore form a non-directional hypothesis about the market reaction to an increase in disclosures and a directional hypothesis for a decrease in disclosures.[17] Our fourth hypothesis considers the exacerbated effect of breach severity on the market reaction.

H3a: An increase in cybersecurity risk factor disclosures following a data breach is associated with a non-zero market reaction.

H3b: A decrease in cybersecurity risk factor disclosures following a data breach is associated with a negative market reaction.

H4: The market reaction to changes in cybersecurity risk factor disclosures following a data breach is stronger when the breach was severe.

[17] A directional hypothesis about the market reaction to an increase in cybersecurity risk factor disclosures after a data breach would require a prediction model of investors' expectations of the increase in disclosures after the data breach is announced and before the annual report is filed, which is beyond the scope of our study.

Methodology and Descriptive Statistics

Data and Sample

We start by obtaining data on reported data breach incidents from 2005 to 2018 from the Chronology of Data Breaches, a free database maintained by Privacy Rights Clearinghouse, a nonprofit organization focused on privacy protection (https://www.privacyrights.org/). This Chronology records all US data breaches reported by either government agencies or verifiable media sources from 2005 onward for both public and private firms. It defines a data breach as "a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual."[18] The Chronology lists 8,943 data breach incidents from 2005 to 2018, which correspond to 8,182 organization-year observations. We eliminate non-business organizations such as educational, medical, and nonprofit institutions. For the remaining observations, we use fuzzy matching to link the company name in the Chronology with the company name in SEC's EDGAR, manually validate the matches, and obtain CIK identifiers.[19]

We obtain firms' financial data from Compustat and stock return data from Center for Research in Security Prices (CRSP). Following the protocol in Campbell et al. (2014), we extract risk factor disclosures (Item 1A) in 10-K forms filed between 2006 and 2018 from SEC's EDGAR. We choose 2006 as the start year because the SEC requirements of adding Item 1A came into effect on December 1, 2005.

For each firm-year with data breach incidents, we match it with a control firm-year based on the 2-digit SIC industry code and total assets as of the end of the same fiscal year using a matching technique with replacement. We eliminate observations with missing financial or textual data and require an observation from the prior fiscal year for calculating change variables, yielding 279 breach-control pairs or 558 firm-years. This final sample consists of 279 unique breached firm-year observations and 277 unique non-breached firm-years.[20] The details of sample construction are shown in Table 1.

[18] See https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice.

[19] We keep only matched records with a similarity score of 80% or more in the fuzzing matching procedure.

[20] Matching with replacement results in two cases where a single non-breached firm-year was matched to two different breached firm-years. Our results are robust if these two pairs of treatment and control observations are dropped.

Table 1 Sample construction

	# firm-years	# unique firms
Organizations in chronology of data breaches during 2005–2018	8,182	7,573
Less: non-business organizations	(5,796)	(5,333)
Less: firms without identifiable CIK	(1,792)	(1,747)
Less: duplicate CIK with different company name	(20)[a]	(96)
Less: firm-years with missing financial data	(230)	(160)
Less: firm-years missing data in the prior fiscal year	(47)	(25)
Less: firm-years for which no match can be found	(18)	(7)
Final treatment sample	**279**	**205**
Final matched sample (i.e., treatment and control firms)	**558**	**407**
Observations of treatment and control firms in pre- and post-breach periods	**1,116**	

This table reports the sample selection process. The final matched sample comprises 558 firm-years, representing 279 firm-years with data breaches (i.e., treatment firm-years) and their matched control firm-years. For analyses using separate pre- and post-specifications, $n = 1{,}116$. For analyses using change specifications, $n = 558$

[a]The decrease of the number of firms is greater than that of the number of firm-years. This is because a firm, without primary identifier like CIK, may be identified with different company names in different incidents. Therefore, before linking to CIK, the number of firms is overcounted

Variable Measurement

Our main variable of interest, measuring the amount of firms' cybersecurity risk factor disclosures, *CyberDisclose*, is a frequency count (i.e., number of occurrences) of cybersecurity risk-related keywords in Item 1A in firms' 10-K filings. Our primary keyword list begins with the list used in Li et al. (2018) and makes three specific augmentations to more thoroughly capture cybersecurity risk factor disclosures.[21] The first augmentation is to allow phrases combined with "cyber" and words like "attack|fraud|threat|risk|terrorist|incident|security" to be separated by a hyphen or a space, while Li et al. (2018) allow only a hyphen. Second, our primary keyword list replaces the phrases "data confidentiality," "confidentiality of data," and "confidential data" with the standalone words "confidential" and "confidentiality" because many firms use these standalone words when describing cybersecurity risks.[22] The third augmentation is to replace "information technology (security|attack)" with "information (technology|attack)" because the latter captures cybersecurity risks in a more generic way.

As noted previously, Hilary et al. (2016) conduct an analysis similar to ours but find no evidence that breached firms increase cybersecurity risk disclosures after data breaches. An important factor that potentially causes this non-result is the keyword list they employ to measure cybersecurity risk disclosure, which includes only the following phrases: "cyber risk," "cyber attack," "cybersecurity risk," "cybersecurity attack," "data breach," "information breach," and "network breach."[23] Examples of frequently occurring words included in our primary keyword list but not Hilary et al. (2016) are "unauthorized access" (16.5%), "hacking|hacker" (13.0%), and "encryption" (3.7%). It is important to include these additional keywords because a considerable number of cases of cybersecurity risk factor disclosures are identified using our primary keyword list but not by the alternative list. As an example, Appendix 2 presents excerpts from Item 1A of Gymboree Corp's 10-K filing before and after a data breach. Four phrases are identified with our primary keyword list before the breach and eight after the breach, highlighted in gray color. Notably, Gymboree adds two entire paragraphs on cybersecurity risk after its data breach, but its risk disclosures include none of the phrases in Hilary et al.'s (2016) keyword list either before or after the breach. In Appendix 3, an analysis of the entire corpus of

[21] Keywords in Li et al. (2018) are identified from prior research (Gordon et al., 2010; Wang et al., 2013) and have been refined to prevent misidentification.

[22] For example, out of 92,277 10-K filings during our sample period, there are only 9,356 (10.1%) documents identified by the phrases "cyberattack" or "cyber-attack" as in the original Li's list. After adding the phrase "cyber attack" to the search, we identify 13,485 (14.6%) documents. Another example, only 368 (0.4%) documents are identified by the phrases "cyberincident" or "cyber-incident" as in the original Li's list, while 3,091 (3.3%) are identified after adding the phrase "cyber incident."

[23] Hilary et al. (2016, p. 13) describe their approach as follows: "The expressions include permutations of cyber or cybersecurity risk or attack and data or information or network breach (hyphenated or spaced and case insensitive)."

10-K filings from the years 2005 to 2018 illustrates how our more comprehensive keyword list provides a better measure of the cybersecurity risk disclosures. In our investigation of the informativeness of cybersecurity risk factor disclosures, we utilize our primary keyword list.

We measure the severity of data breaches as an objective index similar to the index used in Amir et al. (2018). Specifically, we evaluate four attributes of a data breach including the type of data breached, the amount of data breached, the source of the breach, and whether the hackers used the breached data.[24] We obtain and manually read the description of the breach incidents from Privacy Rights Clearinghouse. For each of the four attributes mentioned above, we assign the value of 1 to more severe cases or 0 otherwise. In particular, a data breach is considered as a severe case when there are multiple types of data breached, when the number of records breached is greater than 10,000, when the source of the breach is either hacking or insiders,[25] and when there is evidence shows the breached information is used. Summing up the values of the four attributes, we create an index that ranges from 0 to 4 with 0 being the lowest severity and 4 being the highest. The variable *Severity* equals the natural logarithm of this index value.[26]

Models

Tests of our first hypothesis that the cybersecurity risk factor disclosures increase after a firm experienced a data breach utilize a difference-in-difference regression analysis (DiD) for the amount of cybersecurity risk factor disclosures. DiD is useful in this setting because examining the difference in average cybersecurity risk factor disclosure before and after a data breach of breached firms relative to non-breached firms provides an estimate of the effect of a data breach incident. Moreover, examining the difference-in-difference in disclosures mitigates one potential limitation of keyword-based measurements of disclosures, namely generic boilerplate that is repeated from period to period. We estimate the following equation:

$$\begin{aligned} CyberDisclose &= \alpha + \beta_1 Breach + \beta_2 Post + \beta_3 Breach \times Post \\ &\quad + \beta_4 Size + \beta_5 MTB + \beta_6 Leverage + \beta_7 Litigation \\ &\quad + \beta_8 \text{Post-2011} + \beta_9 Length + \varepsilon \end{aligned} \tag{1}$$

where *CyberDisclose* = the frequency of cybersecurity risk-related keywords; *Breach* = 1 for breached firms, and 0 for matched non-breached firms; and *Post* = 1 for the post period, i.e., years with data breach incidents for breached firms and the matched year for non-breached firms, and 0 otherwise. We control for the size of the firm (*Size*), the market-to-book ratio (*MTB*), and the leverage ratio (*Leverage*) because prior research suggests that while larger firms and firms with lower market-to-book ratios tend to have more cybersecurity risk disclosures, and levered firms are less likely to mention cybersecurity risks in their annual reports (Gao et al., 2020; Hilary et al., 2016). We also include *Litigation*, an indicator variable of high litigation risk industry membership, because firms with higher litigation risk are more likely to disclose information on cyber breaches (Amir et al., 2018; Skinner, 1994). To control for the potential confounding impact of the 2011 SEC Guidance (Gao et al., 2020; Morse et al., 2017), we include an indicator of fiscal years ended after 2011 (*Post-2011*).[27] In addition, since prior research suggests that the length of Item 1A risk factor disclosures is associated with firm risks (Campbell et al., 2014) and firms with higher risks may universally disclose more regarding all risk factors including cybersecurity, we control for the length of risk factor section in Form10-K (*Length*). Finally, to control for the stickiness in cybersecurity risk factor disclosures across time and across industry, we include both industry and year fixed effects. Appendix 4 presents the details of variable definitions.

In the second model, we examine whether the firms with severe data breaches increase the amount of cybersecurity risk factor disclosures more than those with less severe breaches. The following equation is used to test H2[28]:

$$\begin{aligned} CyberDisclose &= \alpha + \beta_1 Breach + \beta_2 Post + \beta_3 Breach \times Post \\ &\quad + \beta_4 Severity + \beta_5 Post \times Severity + \beta_6 Size \\ &\quad + \beta_7 MTB + \beta_8 Leverage + \beta_9 Litigation \\ &\quad + \beta_{10} \text{Post-2011} + \beta_{11} Length + \varepsilon \end{aligned} \tag{2}$$

where *CyberDisclose* = the frequency of cybersecurity risk-related keywords; *Breach* = 1 for breached firms and 0

[24] Amir et al. (2018) utilize a severity index obtained from Gemalto (an international digital security company which was subsequently acquired by Thales in 2019). We create a conceptually similar severity index utilizing the description in Amir et al. (2018, p. 1184) of the index as "based on the type of data breached, the number of records stolen, the source of the breach, and whether the hacker used the stolen data."

[25] Other sources deemed not as severe include the following: fraud involving debit and credit cards not via hacking; paper documents that are lost, discarded, or stolen; portable device lost; stationary computer loss; unintended disclosure of sensitive information; and not enough information about the breach to know how exactly the information was exposed.

[26] Our results are robust when we use a market-based measure of data breach severity that categorizes a data breach as severe if the cumulative Carhart four-factor abnormal return in the three-day window [− 1,1] around the announcement of the data breach is negative.

[27] In a later Sect. 4.4.2, we formally investigate whether managers' decision to update risk factor disclosures after data breaches is affected by the 2011 SEC Guidance.

[28] The variable *Breach* × *Severity* is excluded from Eq. (2) because it always takes the same value as *Severity*.

otherwise; *Post* = 1 for the post period and 0 otherwise; and *Severity* = the natural logarithm of one plus an index value ranging from 0 to 4 based on the severity of the data breach incident (0 = lowest severity and 4 = highest severity), and 0 for all remaining firm-year observations (including the matched non-breached firms). Control variables are the same as in Eq. (1).

In the third model, we examine how investors react to changes in firms' cybersecurity risk factor disclosures after a data breach. Our focus is not on investors' reaction to announcements of data breaches, about which prior literature offers pervasive evidence, but on investors' reactions to firms' changes in cybersecurity risk factor disclosure in subsequent 10-K filings. We use the following Eqs. (3) and (4) to test H3 and H4, respectively[29]:

$$\begin{aligned} CAR = {} & \alpha + \beta_1 Breach + \beta_2 NegDeltaCyberDisclose \\ & + \beta_3 Breach \times NegDeltaCybersclose \\ & + \beta_4 PosDeltaCyberDisclose + \beta_5 Breach \\ & \times PosDeltaCybersclose + \beta_6 Size + \varepsilon \end{aligned} \tag{3}$$

$$\begin{aligned} CAR = {} & \alpha + \beta_1 Breach + \beta_2 NegDeltaCyberDisclose \\ & + \beta_3 Breach \times NegDeltaCyberDisclose \\ & + \beta_4 PosDeltaCyberDisclose + \beta_5 Breach \\ & \times PosDeltaCyberDisclose + \beta_6 Severity \\ & + \beta_7 NegDeltaCyberdisclose \times Severity \\ & + \beta_8 PosDeltaCyberdisclose \times Severity + \beta_9 Size + \varepsilon \end{aligned} \tag{4}$$

where *CAR* = cumulative abnormal returns in the three days around the 10-K filing date, estimated based on Carhart four-factor model; *NegDeltaCyberDisclose* is a truncated variable taking the absolute value of the change in the frequency count of cybersecurity risk-related keywords in Item 1A of the 10-K filing using our primary keyword list from the pre- to the post-breach year, conditional on the change being negative (i.e., a decrease in the frequency count of keywords), and 0 otherwise; and *PosDeltaCyberDisclose* is a truncated variable taking the value of the change in the frequency count of cybersecurity risk-related keywords in Item 1A of the 10-K filing using our primary keyword list from the pre- to the post-breach year, conditional on the change being positive (i.e., an increase in the frequency count of keywords), and 0 otherwise. We control for firms' total assets (*Size*), industry and year fixed effects. The coefficients of interest to test H3a and H3b are β_1 and β_3 in Eq. (3), and the coefficients of interest to test H4 are β_4 and β_5 in Eq. (4).

Descriptive Statistics

Table 2 presents descriptive statistics for the firm characteristics and industry composition of our breached firm sample. Breached firms are larger (measured by either total assets or market value), more leveraged (measured by leverage ratio), and more concentrated in business and financial services, communications, restaurants, and retail industries than the Compustat–CRSP universe. The 279 breached firm-years represent 205 unique breached firms. Using a matched sample of treatment and control firms yields 558 firm-years. For analyses using separate pre- and post-breach observations, $n = 1116$, and for analyses using a change specification, $n = 558$. As shown in Panel C, of the 205 unique breached firms, 154 firms (75.1%) have only one data breach incident during the 13 years sample period, while 51 firms (24.9%) have multiple data breaches. Panel D reports the summary statistics for the variables used in our analyses. The values of *CyberDisclose* indicate that sample firms' risk factor disclosures included an average of 9.504 occurrences of cybersecurity risk expressions based on our primary keyword list. In contrast, the average number of the occurrences of the cybersecurity risk expressions in sample firms' risk factor disclosures based on the keyword list in Hilary et al. (2016), *CyberDisclose_HSZ*, is only 0.621. For selected comparative analysis discussed in a later section, we examine a cybersecurity risk-related keyword list Ghadge et al. (2019) developed for a different research purpose, *CyberDisclose_Ghadge,* the mean occurrence of which is 19.755. The value of *Severity* indicates that the breach incident severity of an average breached firm is 0.0.626 (calculated as $e^{0.486} - 1$) out of 4.

Table 3 reports the mean of cybersecurity risk factor disclosures measures separately for breached firms and control firms, in the pre- and the post-breach year, along with tests of difference-in-difference means. Panel A presents results based on our primary keyword list. The mean values for both the breached firms and control firms increase from the pre-breach to post-breach period, implying an overall increasing trend in the amount of cybersecurity risk factor disclosure.[30] The mean change in the frequency of cybersecurity risk-related keywords for breached firms following a breach is 2.240, while the mean change is only 1.584 for non-breached firms. The difference of 0.656 is significant at the 0.05 significance level. These univariate test results indicate that breached firms increase cybersecurity risk factor disclosures more than non-breached firms.

[29] The terms *Breach* × *Severity*, *Breach* × *Severity* × *NegDeltaCyberDisclose, Breach* × *Severity* × *PosDeltaCyberDisclose* are not included in Eq. (4) because they always take the same value as *Severity*, *NegDeltaCyberDisclose* × *Severity, and PosDeltaCyberDisclose* × *Severity*, respectively.

[30] Untabulated results indicate that cybersecurity risk factor disclosures measured using our primary keyword list decreased for only 7.2% of the sample and 9.0% of breached firms, underscoring an overall secular increase in risk factor disclosures.

Table 2 Descriptive statistics

Panel A: Characteristics of sample breached firm-years compared with Compustat–CRSP population

	Sample		Compustat–CRSP population		Difference in mean	*t*-stats
	N	Mean	*N*	Mean		
Total asset (in $million)	279	81,207.43	63,898	7,179.40	74,028.03***	6.50
Market value (in $million)	279	34,588.54	71,153	3,936.11	30,652.43***	8.56
MTB	279	3.52	63,762	2.74	0.78***	3.07
Leverage	279	0.24	71,215	0.20	0.04***	3.29

Panel B. Industry composition of sample breached firm-years and Compustat–CRSP population

SIC code	Industry	Sample		Compustat–CRSP population		Difference	Chi-square stats
		N	Percent	*N*	Percent		
73	Business Services	48	17.2	6,488	9.1	8.1%***	21.92
60	Depository Institutions	28	10.0	6,643	9.3	0.7%	0.17
63	Insurance Carriers	18	6.5	1,727	2.4	4.0%***	18.92
48	Communications	17	6.1	1,833	2.6	3.5%***	13.66
58	Eating & Drinking Places	16	5.7	706	1.0	4.7%***	62.55
62	Security & Commodity Brokers	14	5.0	1,149	1.6	3.4%***	20.13
36	Electronic & Other Electric Equipment	13	4.7	4,223	5.9	− 1.3%	0.81
59	Miscellaneous Retail	12	4.3	887	1.3	3.1%***	20.90
35	Industrial Machinery & Equipment	10	3.6	2,555	3.6	0.0%	0.00
53	General Merchandise Stores	10	3.6	242	0.3	3.2%***	83.29
	Other	93	33.3	44,762	62.9	− 29.5%***	103.61
	Total	279	100.0	71,215	100.0		

Panel C. Sample breached firm, by frequency of data breach

Number of data breaches per firm	*N*	Percent
1	154	75.12
2	40	19.51
3 or more	11	5.37
Total	205	100.00

Panel D. Summary statistics for variables in regressions

Variable	*N*	Mean	1st quartile	Median	3rd quartile	Std dev
CyberDisclose	1,116	9.504	1.000	7.000	15.000	9.746
CyberDisclose_HSZ	1,116	0.621	0.000	0.000	0.000	1.687
CyberDisclose_Ghadge	1,116	19.755	6.000	16.000	28.000	17.558
Breach	1,116	0.500	0.000	0.500	1.000	0.500
Severity	1,116	0.486	0.000	0.000	1.099	0.566
Size	1,116	9.160	7.629	8.958	10.691	2.106
MTB	1,116	2.710	1.304	2.203	3.688	10.618
Leverage	1,116	0.243	0.068	0.207	0.355	0.219
Litigation	1,116	0.389	0.000	0.000	1.000	0.488
Length	1,116	8.007	7.589	8.206	8.641	1.068
Post-2011	1,116	0.465	0.000	0.000	1.000	0.499
CAR	558	− 0.000	− 0.015	− 0.001	0.016	0.044
DeltaCyberDisclose	558	1.812	0.000	0.000	2.000	3.660
NegDeltaCyberDisclose	558	0.129	0.000	0.000	0.000	0.520
PosDeltaCyberDisclose	558	1.941	0.000	0.000	2.000	3.553
DeltaLength	558	263.109	− 2.000	140.500	495.000	615.809
MediaAttention	558	0.030	0.000	0.000	0.000	0.112

This table reports sample descriptive statistics. Panel A and Panel B compare firm characteristics and industry composition of breached firms to Compustat/CRSP universe. Panel C presents frequency of data breach incidents for breached firms. Panel D presents summary statistics for the variables used in regressions. ***, **, and * indicate two-sided significance at the 1%, 5%, and 10% levels, respectively. Detailed variable definitions are provided in Appendix 4

Table 3 Changes in cybersecurity risk factor disclosures following data breaches

Panel A. Amount of cybersecurity risk factor disclosure measured using our primary keyword list				
CyberDisclose	*N*	Pre-breach	Post-breach	Difference
Breached firms	279	9.319	11.559	2.240***
				(7.52)
Non-breached firms	279	7.599	9.183	1.584***
				(7.71)
Difference	279	1.720***	2.376***	0.656**
		(3.39)	(4.20)	(2.08)
Panel B. Amount of cybersecurity risk factor disclosure measured using Hilary et al. (2016)'s keyword list				
CyberDisclose_HSZ	N	Pre-breach	Post-breach	Difference
Breached firms	279	0.441	0.731	0.290***
				(4.13)
Non-breached firms	279	0.491	0.681	0.190***
				(3.77)
Difference	279	− 0.050	0.050	0.100
		(− 0.57)	(0.40)	(1.23)
Panel C. Amount of cybersecurity risk factor disclosure measured using Ghadge et al. (2019) keyword list				
CyberDisclose_Ghadge	N	Pre-breach	Post-breach	Difference
Breached firms	279	19.444	22.656	3.212***
				(7.29)
Non-breached firms	279	16.989	19.222	2.233***
				(6.58)
Difference	279	2.455**	3.434***	0.979*
		(2.52)	(3.17)	(1.89)

This table reports the mean amount of cybersecurity risk factor disclosures, separately for breached firms and control firms, in the pre- and the post-breach year, along with tests of difference-in-difference means of *CyberDisclose* measured by the three keyword lists. *t*-statistics are in parentheses. ***, **, and * indicate two-sided significance at the 1%, 5%, and 10% levels, respectively. Detailed variable definitions are provided in Appendix 4

As previously noted, Hilary et al. (2016) find no significant difference in changes in breached firms' combined cybersecurity risk disclosures in Item 1A and Item 7 after a data breach compared to non-breached firms. To test our conjecture that the results (or rather, non-results) in that paper are driven by an incomplete keyword list to measure the amount of cybersecurity risk disclosures, we replicate the test using Hilary et al. (2016)'s keyword list on our sample focusing on Item 1A disclosures only. Results presented in Panel B show an increase in cybersecurity risk factor disclosures for both breached firms and control firms from the pre-breach to post-breach period, similar to results based on our primary keyword list. However, when using Hilary et al. (2016)'s keyword list to quantify the amount of cybersecurity risk factor disclosures, there is no significant difference in the change in cybersecurity risk factor disclosures between breached firms and control firms in the years around a data breach, consistent with Hilary et al. (2016)'s findings.

Panel C reports results of the same tests but measuring cybersecurity risk factor disclosure using a different cybersecurity risk-related keyword list. Ghadge et al. (2019) develop a list of search strings to identify relevant academic research papers in the context of a literature review on the topic of cybersecurity risk management in inter-firm supply chains. Given the focus of that study, the Ghadge et al. (2019) list includes keywords from both the fields of supply chain risk management and information technology. Despite having been developed for a research purpose other than measuring the amount of cybersecurity risk factor disclosures, results of our test using Ghadge et al.'s (2019) list indicate a significantly larger increase in breached firms' cybersecurity risk factor disclosures after a breach incident compared to matched control firms. Overall, the evidence in Table 3 supports our conjecture that the absence of results in Hilary et al. (2016) can be explained by an inadequate keyword list. In all our subsequent tests, we use our primary

keyword list to measure the amount of cybersecurity risk factor disclosures.[31]

Empirical Results

Cybersecurity Risk Factor Disclosures After Data Breaches (Test of H1)

Table 4 reports the results from the estimation of Eq. (1). We test whether a firm's cybersecurity risk factor disclosures increase following a data breach. The dependent variable is the amount of cybersecurity risk factor disclosure using our primary keyword and the variable of interest is the interaction term *Breach* × *Post*. The coefficient on *Breach* × *Post* is positive at the significance level of 0.05. Thus, breached firms increase cybersecurity risk factors disclosures more than matched control firms after experiencing a data breach. The economic magnitude of the increase in disclosure is substantial. The results reported in Table 4 translate to the following:

(1) Before a breach, in comparison to non-breached firms, breached firms' risk factor disclosures on average include 1.229 more occurrences of the cybersecurity risk expressions, which is 12.9% (1.229/9.504) higher than the sample mean level;

Table 4 Cybersecurity risk-related disclosure and data breaches

	CyberDisclose (1)
Breach	1.229**
	(2.36)
Post	0.053
	(0.23)
Breach × *Post*	0.733**
	(1.97)
Size	0.206
	(1.19)
MTB	0.026
	(1.57)
Leverage	− 0.809
	(− 0.56)
Litigation	1.977
	(1.15)
Post-2011	− 0.907
	(− 0.72)
Length	2.341***
	(6.86)
Constant	− 22.916***
	(− 6.16)
Industry, year FE	Yes
Clustered by firms	Yes
N	1,116
R-squared	0.593

This table presents coefficients and *t*-statistics in parentheses from pooled regression of the dependent variable *CyberDisclose,* on the independent variables listed. *CyberDisclose* denotes the frequency of cybersecurity risk expressions in Item 1A of 10-K filings identified by our primary keyword list in column (1). *Breach* equals 1 for breached firms, and 0 for matched non-breached firms. *Post* equals 1 for the post period, i.e., the year with data breach incidents for breached firms and the year of the match for non-breached firms, and 0 otherwise. Industry fixed effects correspond to 2-digit SIC codes. Detailed variable definitions are provided in Appendix 4. Standard errors are clustered by firm. ***, **, and * indicate two-sided significance at the 1%, 5%, and 10% levels, respectively

(2) In comparison to the pre-breach year, non-breached firms' risk factor disclosures on average are not significantly different in the post-breach year; and
(3) In comparison to the increase in cybersecurity risk expressions by non-breached firms from the pre- to the post-breach year, the increase in the occurrences of the cybersecurity risk expressions by breached firms on average is 0.733 greater, 7.7% (0.733/9.504) higher than the sample mean level.

The regression results are consistent with the univariate test results in Table 3. After a data breach incident, breached

[31] Ghadge et al.'s (2019) keyword list was developed for a different research purpose than measuring the amount of cybersecurity risk disclosures. We conjecture it is a noisier measure of cybersecurity risk factor disclosures than our primary keyword list. To evaluate our conjecture, we perform an analysis on the subsamples that decreased cybersecurity risk factor disclosures following data breaches, where the decrease was based on either our primary keyword list or Ghadge et al. (2019)'s keyword list, but not both. There are 10 observations identified using our primary keyword lists but not Ghadge et al. (2019)'s list, and 32 observations identified using Ghadge et al. (2019)'s list but not our primary keyword list. We then examine the uses of cybersecurity risk-related expressions in these two subsamples. The frequency counts of the ten expressions with the largest drop in uses are reported in Appendix 5. In the 10 filings identified exclusively using our primary keyword list, the expressions with the largest decreases in frequency are "confidential," "(information|network) security," and "information (technology|attack)." In contrast, in the 32 filings identified exclusively by Ghadge et al. (2019)'s list, the phrases with the largest decreases in uses are "disruption," "infrastructure," and "security," which capture security or threat in a more generic way and less tailored to describe cybersecurity risk. These observations support our conjecture that Ghadge et al. (2019)'s keyword list produces a noisier measure of cybersecurity risk factor disclosures.

Table 5 Change in cybersecurity risk factor disclosures and data breach severity

	CyberDisclose (1)
Breach	1.080
	(1.05)
Post	0.049
	(0.21)
Breach × *Post*	− 0.714
	(− 0.96)
Severity	0.156
	(0.15)
Post × *Severity*	1.486*
	(1.75)
Size	0.186
	(1.07)
MTB	0.026
	(1.59)
Leverage	− 0.691
	(− 0.47)
Litigation	1.951
	(1.13)
Post-2011	− 0.963
	(− 0.76)
Length	2.342***
	(6.87)
Constant	− 22.938***
	(− 6.10)
Industry, year FE	Yes
Clustered by firms	Yes
N	1,116
R-squared	0.594

This table presents coefficients and *t*-statistics in parentheses from pooled regression of the dependent variable *CyberDisclose,* on the independent variables listed. *CyberDisclose* denotes the frequency of cybersecurity risk expressions in Item 1A of 10-K filings identified by our primary keyword list in column (1). *Breach* equals 1 for breached firms, and 0 for matched non-breached firms. *Post* equals 1 for the post period, i.e., the year with data breach incidents for breached firms and the year of the match for non-breached firms, and 0 otherwise. *Severity* is the natural logarithm of one plus an index value that ranges from 0 to 4 based on the severity of the data breach incident (0 = lowest severity and 4 = highest severity). Industry fixed effects correspond to 2-digit SIC codes. Detailed variable definitions are provided in Appendix 4. Standard errors are clustered by firm. ***, **, and * indicate two-sided significance at the 1%, 5%, and 10% levels, respectively

firms increase cybersecurity risk factor disclosures more than non-breached firms.

Cybersecurity Risk Factor Disclosures and Data Breach Severity (Test of H2)

Table 5 shows the regression results of estimating Eq. (2) testing H2 that the increase in the amount of cybersecurity risk factor disclosures after a breach is associated with the severity of the breach. The dependent variable is the amount of cybersecurity risk factor disclosure using our primary keyword list and the variable of interest is the two-way interaction term *Post* × *Severity*. We observe a positive and significant coefficient on the variable of interest. As shown in Table 5, the increase in cybersecurity risk-related expressions in our primary keyword list following a severe data breach is 1.486 more than that after a low severity data breach. The regression results support Hypothesis 2 that firms increase cybersecurity risk factor disclosures more after experiencing a severe data breach. After including the interaction term *Post* × *Severity*, the coefficients on *Breach* and the interaction term *Breach* × *Post* become insignificant, implying that the impact is mainly driven by the interaction term *Post* × *Severity.* In other words, cybersecurity risk factor disclosures of firms that experienced a low severity data breach neither differ significantly from non-breached firms' disclosures in the pre-period, nor do they increase significantly more than non-breached firms after the data breach; firms increase cybersecurity risk factor disclosures only after severe data breaches.[32]

Market Reaction to Changes in Cybersecurity Risk Factor Disclosures (Tests of H3a, H3b, and H4)

Table 6 column (1) shows the regression results of estimating Eq. (3) testing H3a and H3b.[33] In both columns (1) and (2), the coefficient on the interaction term *Breach* × *NegDeltaCyberDisclose* is significantly negative, indicating that that the abnormal returns around the 10-K filing are negatively related to the extent of the decreases in breached firms' cybersecurity risk factor disclosures, supporting our H3b. The coefficient on the interaction term *Breach* × *PosDeltaCyberDisclose* is not significant, providing no evidence of a

[32] The sum of the coefficients on *Breach* and *Severity* are significantly different from zero (*p*-value = 0.019), implying that cybersecurity risk factor disclosures of firms that experienced a severe data breach differ significantly from non-breached firms' disclosures in the pre-period.

[33] Following prior event study literature (e.g., Amir et al., 2018; Baudot et al., 2021; Racine et al., 2020), we examine the short-window market reaction to changes in disclosures. Because the explanatory disclosure variables in Eqs. (3) and (4) measure the changes in cybersecurity risk factor disclosures from the pre- to the post-data breach period, the sample size in Table 6 is reduced by half compared to Tables 4 and 5.

Table 6 Market reaction to reduced cybersecurity risk factor disclosure

	CAR	
	(1)	(2)
Breach	0.001	0.005
	(0.24)	(0.61)
NegDeltaCyberDisclose	0.007	0.006
	(1.59)	(1.30)
Breach × *NegDeltaCyberDisclose*	− 0.041***	− 0.043***
	(− 3.30)	(− 3.31)
PosDeltaCyberDisclose	0.000	0.000
	(0.34)	(0.41)
Breach × *PosDeltaCyberDisclose*	− 0.002	− 0.001
	(− 1.41)	(− 0.62)
Severity		− 0.005
		(− 0.61)
NegDeltaCyberdisclose × *Severity*		0.001
		(1.16)
PosDeltaCyberdisclose × *Severity*		− 0.000
		(− 0.53)
Size	− 0.001	− 0.001
	(− 0.58)	(− 0.50)
Constant	− 0.035*	− 0.036*
	(− 1.70)	(− 1.77)
Industry, year FE	Yes	Yes
Clustered by firms	Yes	Yes
N	558	558
R-squared	0.143	0.146

This table presents coefficients and *t*-statistics in parentheses from pooled regression of the dependent variable *CAR,* on the independent variables listed. *CAR* is the cumulative abnormal returns in the three days around the 10-K filing date. *Breach* equals 1 for breached firms, and 0 for matched non-breached firms. *NegDeltaCyberDisclose* equals the absolute value of the change in the frequency count of cybersecurity risk-related keywords in Item 1A of the 10-K filing using our primary keyword list from the pre- to the post-breach period, conditional on the change is negative (i.e., decrease in the frequency count of keywords). *PosDeltaCyberDisclose* equals the absolute value of the change in the frequency count of cybersecurity risk-related keywords in Item 1A of the 10-K filing using our primary keyword list from the pre- to the post-breach period, conditional on the change is positive (i.e., increase in the frequency count of keywords). *Severity* is the natural logarithm of one plus an index value ranging from 0 to 4 based on the severity of the data breach incident (0 = lowest severity and 4 = highest severity). Industry fixed effects correspond to 2-digit SIC codes. Detailed variable definitions are provided in Appendix 4. Standard errors are clustered by firm. ***, **, and * indicate two-sided significance at the 1%, 5%, and 10% levels, respectively

market reaction to breached firms' increases cybersecurity risk factor disclosures and therefore failing to support H3a.

Table 6 column (2) shows the regression results of estimating Eq. (4) testing H4. The coefficients on the interaction terms *NegCyberDisclose* × *Severity* and *PosCyberDisclose* × *Severity* that address whether the severity of a breach moderates the association between the market reaction and the change in risk factor disclosures following a breach are not statistically significant at the traditional level. The results imply that although investors consider the severity of a data breach at the announcement of the breach, investors penalize the breached firm when observing the firm subsequently decreases cybersecurity risk factor disclosures, regardless of the severity of the breach.

Alternative Explanations

Our findings show that breached firms, especially firms with severe incidents, increase cybersecurity risk factor disclosures. We interpret the results as indications of management's intent to provide information about updated assessment of their firms' risks. Here, we consider two alternative explanations: disclosure increases pertaining to the specific prior data breach, and disclosure increases driven by regulatory requirements.

Disclosures Pertaining to the Specific Prior Data Breach

If the observed increase in the amount of cybersecurity risk factor disclosures pertains exclusively to discussion of the very data breach itself instead of broader modifications to disclosed risk factors, it is less clear that the documented change in disclosures can be interpreted as evidence of managers' intention to inform investors and others of their updated assessments of their firms' cybersecurity risks. The finding in Gao et al. (2020) that disclosures of cyber incidents are most often disclosed in MD&A (Item 7) instead of the risk factor section alleviates this concern. To formally rule out this alternative explanation, we randomly select 50 breached firms from our sample and manually examined the Item 1A of their 10-K filings following the breach for the presence of mentions of the data breach incident. Of these 50 firms' filings, 21 (42%) had an increased frequency count of cybersecurity risk-related keywords in Item 1A compared to the prior year, but only 7 (14%) of these firms mentioned the very data breach. This suggests that the mentions of the data breach incident in Item 1A are not prevalent. Further, when firms mentioned the data breach in Item 1A, they were not just discussing the incident, rather they were citing the incident as a reason why cybersecurity was a material risk in their business or using the breach to illustrate how – despite all efforts – security failures happened and would likely

reoccur.[34] Therefore, the documented increase in the amount of cybersecurity risk factor disclosures after data breaches cannot be attributed to firms merely mentioning the specific data breach, rather it is evidence of firms' modification to risk factor disclosures to incorporate managers' updated risk assessment as we posit.

Disclosure Increases in Response to Regulatory Mandate

We examine cybersecurity risk factor disclosures change following the 2011 SEC guidance on cybersecurity risk disclosures. This analysis is motivated by prior research showing the impact of regulatory changes on the amount of cybersecurity disclosure (e.g., Gao et al., 2020; Gordon et al., 2006; Morse et al., 2017).[35] These prior studies find a sharp increase in cybersecurity risk disclosures following SOX and the 2011 SEC guidance. Given our focus on the differential cybersecurity risk factor disclosures by firms that experience a data breach, we examine whether disclosures following a data breach are affected by the 2011 SEC guidance. We divide our sample into the pre- and the post-2011 subperiods and undertake the DiD regression for both subperiods. As in Fang et al. (2016), we drop firm-years ended in 2011 from the subperiod analysis because the October issuance date of the 2011 makes it unclear whether 2011 should appropriately be classified in the pre- or post-Guidance subperiod. Further, we ensure that both the pre-breach and post-breach periods are under the same regulatory regime by eliminating observations that span 2011. Results in Table 7 show the coefficient on *Breach* × *Post* is significantly positive in both the pre-2011 Guidance period (column 1) and the post-2011 Guidance period (column 2) indicating that breached firms increase cybersecurity risk factor disclosures following a breach in both subperiods.[36] A Chi-squared test of a difference in the estimated coefficients on *Breach* × *Post* between the two subperiods fails to reject the null (p-value = 0.1937), implying that the magnitude of the relative increases in breached firms' cybersecurity risk factor disclosures compared to non-breached firms does not change significantly from the pre- to the post- 2011 SEC guidance period.

Table 7 Change in cybersecurity risk factor disclosures pre- and post-2011 guidance

	CyberDisclose	
	(1)	(2)
	Pre-2011 guidance period	Post-2011 guidance period
Breach	1.233***	1.484*
	(2.47)	(1.44)
Post	− 0.387	0.461
	(− 1.27)	(0.83)
Breach × *Post*	0.303*	1.454*
	(1.31)	(1.63)
Size	− 0.347*	0.776**
	(− 1.59)	(2.10)
MTB	0.107**	− 0.012**
	(2.11)	(− 1.71)
Leverage	− 1.146	0.826
	(− 2.00)	(0.26)
Litigation	3.826***	− 2.817
	(3.14)	(− 0.79)
Length	1.075***	5.015***
	(5.11)	(6.05)
Constant	− 3.484	− 26.943***
	(− 1.14)	(− 3.18)
Industry, year FE	Yes	Yes
Clustered by firms	Yes	Yes
N	432	452
R-squared	0.431	0.410
Sig. difference	Prob > chi^2 = 0.1937	

This table presents coefficients and *t*-statistics in parentheses from regression of the dependent variable *CyberDisclose,* on the independent variables listed, for firm-years ended before 2011 in column (1), and for firm-years ended in/after 2012 in column (2). We ensure the pre-breach and post-breach years (i.e., *Post* equal to 0 and 1 in the DiD regression) are under the same regulatory regime for data used in the regression in both columns of this table. *CyberDisclose* denotes the frequency of cybersecurity risk expressions in Item 1A of 10-K filings identified by our primary keyword list. *Breach* equals 1 for breached firms, and 0 for matched non-breached firms. *Post* equals 1 for the post-breach period, i.e., the year with data breach incidents for breached firms and the year of the match for non-breached firms, and 0 otherwise. Industry fixed effects correspond to 2-digit SIC codes. We use seemingly unrelated estimation (SUEST) to test across models for significant differences between the coefficients on *Breach* × *Post* (reported p-value labeled ''Sig. difference''). Detailed variable definitions are provided in Appendix 4. Standard errors are clustered by firm. ***, **, and * indicate one-sided significance at the 1%, 5%, and 10% levels, respectively

Motivations to Increase Cybersecurity Risk Factors Disclosures

As discussed earlier, potential motivations for managers to increase cybersecurity risks disclosures include mitigating

[34] See Equifax Form 10-K filed after its data breach announced on September 7, 2017 for an example (Link at https://www.sec.gov/Archives/edgar/data/33185/000003318518000011/efx10k20171231.htm).

[35] Morse et al. (2017) identify cybersecurity risk factor disclosures by searching for the following expressions in 10-K filings: (1) the exact phrase "cybersecurity risks," and (2) the Boolean search "cybersecurity /5 risk or incident or threat."

[36] We use one-sided tests to test the significance of coefficients in Table 7 because of our directional hypotheses. The one-sided tests provide more power to detect an effect in one direction, which helps in this analysis with small subperiod samples.

litigation concerns, deterring future cyberattacks and responding to scrutiny over the firm's cybersecurity risks among investors and other stakeholders. In this section, we describe our exploratory investigation of these motivations.

To investigate the impact of litigation risks on managers' disclosure decisions, we adopt two alternative proxies of litigation risks: an indicator of high litigation risk industry membership and a proxy based on industry membership and firm characteristics developed by Kim and Skinner (2012). We re-estimate Eq. (1) incorporating each of these alternative proxies as additional independent variables. Untabulated test results show no statistically significant relation between cybersecurity risk factor disclosures and high litigation risks and thus provides no evidence suggesting that prevention of litigation threats is a dominant factor for increasing cybersecurity risk factor disclosures. We draw a similar inference based on the infrequency of shareholder lawsuits against our sample of breached firms. Records about shareholder lawsuits against our sample breached firms in the period of 2005–2018 in the Securities Class Action Clearinghouse (SCAC) website (http://securities.stanford.edu/) show only four of the breach incidents (1.4%) resulted in subsequent shareholder lawsuits against the breached firms.[37]

A second potential motivation for managers to increase cybersecurity risks disclosures following a data breach is to deter future cyberattacks. Although potential cyberattacks from which hackers have been deterred are unobservable, differences between the recurrence of attacks on breached firms that increase versus decrease cybersecurity risk factor disclosures can shed some light on this. To explore the deterrence effect of increased increase cybersecurity risks disclosures, in an untabulated test we model the relationship between the recurrence of a data breach and changes in cybersecurity risk factor disclosures and find results consistent with increased disclosures having some deterrent effect. Considering the findings in prior studies (Wang et al. 2013; Li et al., 2018) that firms are more likely to experience future data breaches when they have lengthier cybersecurity risk factor disclosures but less likely to incur future breaches when the disclosed information security risk factors include risk-mitigating action terms, our findings provide some corroborating evidence that the increased cybersecurity risk factors disclosures of a breached firm signal its active cybersecurity management strategy and commensurate increased cost of attacks, and thus successfully deter future attackers.

Finally, firms may disclose more cybersecurity risks in reaction to the scrutiny among investors and other stakeholders. In an untabulated test, we use media coverage of breached firms' cybersecurity issues as a proxy for investors' and other stakeholders' scrutiny of related risks. We measure media coverage of breached firms' cybersecurity issues based on news articles in the Nexis Uni database that include both the name of the breached firm and any cybersecurity risk-related expressions (identified using our primary keyword list) in the title of the article. We find preliminary evidence that increases in cybersecurity risk factor disclosures after a severe data breach are present only when there is high media coverage of breached firms' cybersecurity issues. This finding is consistent with the reaction to the public scrutiny being an important factor in managers' decisions to revise cybersecurity risk factor disclosures.

Overall, our exploratory analyses suggest that—in general—reaction to the public scrutiny over the firm's cybersecurity risks and deterring future attacks are important motivations for increasing cybersecurity risk factor disclosure following a data breach. These findings can be understood in the context of stakeholder theory.

Conclusion

Our study addresses the changes in cybersecurity risk disclosures following a data breach and the market reaction to such changes. We acknowledge our study is subject to certain inherent limitations of the "bag-of-words" approach to capturing disclosure content, including synonymy and polysemy. Our use of the difference-in-difference structure and our change analysis mitigate another potential limitation that keyword-based measures may capture generic boilerplate disclosures repeated from period to period. Despite limitations, we believe our work contributes to the streams of research on risk factor disclosures and cyber business ethics.

We present evidence that firms experiencing a data breach increase the amount of cybersecurity risk factor disclosures, consistent with managers intending to inform investors about their assessment of risks through disclosures. The increase in cybersecurity risk factor disclosures is even larger when the data breach was more severe. We focus on the setting of cybersecurity risk factor disclosures after a data breach because data breaches, especially severe breaches, serve as a natural experiment where an exogenous shock to managers' assessment of their firm's cybersecurity risks occurs.

Consistent with the market anticipating and valuing increased disclosures, we find the abnormal returns around the 10-K filing are negatively related to the extent of the

[37] Our observation is similar to Romanosky et al. (2014) who find only 65 (3.7%) of the 1,772 US data breaches in 2005–2010 recorded by Datalossdb Clearinghouse are litigated in federal court. Comments by the SEC chairman highlighting recent actions against firms failing to accurately disclose cybersecurity incidents and risks may signal an overall shift in the enforcement environment which could potentially also affect the overall litigation environment (Gensler, 2022). We leave this question for future research.

decreases in breached firms' cybersecurity risk factor disclosures, while there is no evidence of a non-zero market reaction to breached firms that increase cybersecurity risk factor disclosures. Finally, our exploratory analyses imply that—in general—reaction to public scrutiny over the firm's cybersecurity risks and deterrence of future cyberattacks are likely motivations for increasing cybersecurity risk factor disclosure following a data breach.

Appendix 1

In this appendix, we list the cybersecurity keywords by Li et al. (2018) and our primary keyword list, which is an augmentation of Li et al. (2018). For comparison, we list similar phrases on the same row. We have also merged some similar phrases for more concise presentation (Table 8).

Table 8 Comparison of alternative cybersecurity keyword lists

Li et al. (2018)	Our primary keyword list
Cyber(-|)(attack|fraud|threat|risk|terrorist|incident|security)	Cyber(\s|-)(attack|fraud|threat|risk|terrorist|incident|security)
Cybersecurity	
Cyber-based attack	Cyber-based attack
Data breach	Data breach
Security (breach|incident)	Security (breach|incident)
Network break-in	Network break-in
Computer (virus|breach|break-in|attack|security)	Computer (virus|breach|break-in|attack|security)
(information|network) security	(information|network) security
Encryption	Encryption
Intrusion	Intrusion
Hacking|hacker	Hacking|hacker
Denial of service	Denial of service
Infosec	Infosec
System security	System security
Data theft	Data theft
Phishing	Phishing
Malware	Malware
Social engineering	Social engineering
Unauthorized access	Unauthorized access
Data corruption	Data corruption
Corruption of data	Corruption of data
Espionage	Espionage
Cyber(-|)insurance	Cyber(-)insurance
Crimeware	Crimeware
Ransomware	Ransomware
Keylogger	Keylogger
Keystroke logging	Keystroke logging
Information technology (security|attack)	Information (technology|attack)
Data confidentiality	Confidential(ity)
Confidentiality of data	
Confidential data	

Appendix 2: Example of the Pre- and the Post-cyberattack Disclosures

Gymboree Corp.

(A specialty retail company, listed on NASDAQ).

Form 10-K for the fiscal year ended January 28, 2006 (Pre-cyberattack).

Item 1A. Risk Factors.

…

Our ability to successfully implement significant information technology systems is critical to our business.

In the coming year, we plan to undertake a series of initiatives to upgrade our information technology infrastructure. These initiatives include a program to upgrade our point-of-sale, sales audit and financial systems. Such technology

systems changes are complex and could cause disruptions that would adversely affect our business. We cannot assure you that we will be able to successfully execute these changes without significant disruption to our business. If we are not successful, we may not achieve the expected benefits from these initiatives, despite having expended significant capital. We may also determine that additional investment is required to bring our systems to their desired state; this could result in a significant additional investment of time and money and increased implementation risk. Furthermore, the Company will rely on third parties to fulfill contractual obligations related to the upgrade of these systems. Failure of these third parties to fulfill their contractual obligations could lead to significant expenses or losses due to a disruption in business operations.

Our business may be harmed if our computer network security is compromised.

Despite the Company s considerable efforts and technology to secure our computer network, security could be compromised, confidential information, such as customer credit card numbers, could be misappropriated, or system disruptions could occur. This could lead to adverse publicity, loss of sales and profits or cause the Company to incur significant costs to reimburse third parties for damages.

Damage to our computer systems could severely hamper our ability to manage our business.

Our operations depend on our ability to maintain and protect our computer systems on which we rely to manage our purchase orders, store inventory levels, web applications, accounting functions and other aspects of our business. We have computer systems located in each of our stores, with the main database servers for our systems located in San Francisco, California, which exists on or near known earthquake fault zones. An earthquake or similar disaster could have a material adverse impact on our business and operating results not only by damaging our stores or corporate headquarters, but also by damaging our main servers, which could disrupt our business for an indeterminate length of time. Our systems are vulnerable to damage from fire, floods, earthquakes, power loss, telecommunications failures, and similar events. We do not have back-up sites from which to conduct our business in the event of a natural disaster. There can also be no assurance that the Company can maintain or protect its on-line business application from a significant disruption that could result in a material adverse effect on its on-line revenue.

Our growth will be hampered if we are unable to locate new stores and relocate existing stores in appropriate retail venues and shopping area.

…

Form 10-K for the fiscal year ended February 3, 2007 (Post-cyberattack).

Item 1A. Risk Factors.

…

Our ability to successfully implement significant information technology systems is critical to our business.

In the coming year, we plan to undertake a series of initiatives to upgrade our information technology infrastructure. These initiatives include a program to upgrade our point-of-sale and sales audit systems, implement a new customer relationship management system, and continue to support and enhance functionality for the Company s websites. Such technology systems changes are complex and could cause disruptions that would adversely affect our business. While management will make every effort to ensure the orderly implementation of various information technology systems, we cannot ensure that we will be able to successfully execute these changes without potentially incurring a significant disruption to our business. If we are not successful, we may not achieve the expected benefits from these initiatives, despite having expended significant capital. We may also determine that additional investment is required to bring our systems to their desired state; this could result in a significant additional investment of time and money and increased implementation risk. Furthermore, the Company intends to rely on third parties to fulfill contractual obligations related to the upgrade of these systems. Failure of these third parties to fulfill their contractual obligations could lead to significant expenses or losses due to a disruption in business operations.

Our business may be harmed if our computer network security is compromised.

Despite the Company s considerable efforts and technology to secure our computer network, security could be compromised, confidential information, such as customer credit card numbers, could be misappropriated, or system disruptions could occur. This could lead to adverse publicity, loss of sales and profits, or cause the Company to incur significant costs to reimburse third parties for damages which could impact profits. The Company is currently in the process of upgrading its systems and procedures to meet the Payment Card Industry (PCI) data security standards. The Company s compliance with these standards is required to undergo audits by independent third parties. Failure to comply with the security requirements or rectify a security issue may result in fines and the imposition of restrictions on the Company s ability to accept payment cards. There can be no assurance that the Company will satisfy audit requirements.

Damage to our computer systems could severely hamper our ability to manage our business.

Our operations depend on our ability to maintain and protect our computer systems on which we rely to manage our purchase orders, store inventory levels, web applications, accounting functions and other aspects of our business. We have computer systems located in each of our stores, with the main database servers for our systems located in San Francisco, California, which exists on or near known earthquake fault zones. An earthquake or similar disaster could have a material adverse impact on our business and operating results not only by damaging our stores or corporate headquarters, but also by damaging our main servers, which could disrupt our business for an indeterminate length of time. Our systems are vulnerable to damage from fire, floods, earthquakes, power loss, telecommunications failures, and similar events.

Our failure to successfully manage our on-line businesses could have a negative impact on our business.

The operation of our on-line businesses depends on our ability to maintain the efficient and uninterrupted operation of our order-taking and fulfillment operations and our on-line stores. Disruptions or slowdowns in these areas could result from disruptions in telephone service or power outages, inadequate system capacity, system issues, computer viruses, security breaches, human error, changes in programming, natural disasters or adverse weather conditions. Our on-line businesses are vulnerable to additional risks and uncertainties associated with the Internet, including changes in required technology and other technical failures as well as changes in applicable federal and state regulation, security breaches, and consumer privacy concerns. Problems in any of these areas could result in a reduction in sales, increased selling, general and administrative expenses and damage to our reputation and brands.

In addition, we face the risk that we cannot hire enough qualified employees, or that there will be a disruption in the labor we hire from third party providers, especially during our peak season, to support our on-line operations, due to circumstances that reduce the available workforce. The need to operate with fewer employees could negatively impact our customer service levels and our operations.

Our growth will be hampered if we are unable to locate new stores and relocate existing stores in appropriate retail venues and shopping area.

…

Appendix 3: Frequency Counts of Phrases in Alternative Keyword Lists in 10-K Filings

This appendix compares the frequency counts of phrases in our primary keyword list and Hilary et al.'s (2016) keyword list (referred to in this appendix as "HSZ") using the entire corpus of the 92,277 10-K filings from 2005 to 2018. Document frequency is the frequency of all documents containing any keyword from the specified keyword list. Word frequency is the number of times the particular phrase in the keyword list occurs in all documents in the corpus. The following table presents frequency counts of all the ten most frequently occurring keywords in our primary list that are not in HSZ followed by all expressions in HSZ.

Most frequently occurring expressions in our primary keyword list but not in the HSZ keyword list	Document frequency	Word frequency
Confidential(ity)	35,710	103,183
INFORMATION (technology|attack)	26,232	71,548
Security (breach|incident)	26,084	68,664
Cyber(\s|−|)(attack|fraud|threat|risk|terrorist|incident|security)	19,086	52,074
Computer (virus|breach|break-in|attack|security)	18,334	23,481
Unauthorized access	15,201	24,852
(hacking|hacker)	11,964	16,618
(information|network) security	11,448	21,083
Intrusion	4,334	7,270
Malware	3,841	4,791
Encryption	3,386	5,477
All expressions in HSZ keyword list	**Document frequency**	**Word frequency**
Cyber risk	719	890
Cyber attack	4,786	10,565
Cybersecurity risk	1,849	2,718
Cybersecurity attack	1,299	2,315
Data breach	3,034	4,394
Information breach	137	151
Network breach	133	133

As shown, many cybersecurity risk-related phrases and their derivative forms which occur frequently in Item 1A are omitted from HSZ's list. For example, the phrase with the highest document frequency using HSZ's list ("cyber attack") identifies only 4,786 documents (around 5% of total documents), while its derivative forms ("cyber(\s|-|)attack") identify 13,485 documents (around 15% of total documents). The table above shows 19,086 documents identified using the regular expression "cyber(\s|-|)(attack|fraud|threat|risk|terrorist| incident|security)" in our primary keyword list. The 13,485 documents identified using the regular expression "cyber(\s|-|)attack" are a subset of these 19,086 documents.

Appendix 4

See Table 9.

Table 9 Variable definitions

Variable name	Definition
CyberDisclose	Frequency of cybersecurity risk-related keywords in Item 1A of 10-Ks, based on our primary keyword list, which is an augmentation of the Li et al. (2018)'s keyword list
CyberDisclose_HSZ	Frequency of cybersecurity risk-related keywords in Item 1A of 10-Ks, based on Hilary et al. (2016)'s keyword list
CyberDisclose_Ghadge	Frequency of keywords in Item 1A, based on Ghadge et al. (2019)'s list
Length	The natural logarithm of total nonstop word frequency count in Item 1A
NegDeltaCyberDisclose	A truncated variable taking the absolute value of the change in the frequency count of cybersecurity risk-related keywords in Item 1A of the 10-K filing using our primary keyword list from the pre- to the post-breach year, conditional on the change is negative (i.e., decrease in the frequency count of keywords), and 0 otherwise
PosDeltaCyberDisclose	A truncated variable taking the value of the change in the frequency count of cybersecurity risk-related keywords in Item 1A of the 10-K filing using our primary keyword list from the pre- to the post-breach year, conditional on the change is positive (i.e., increase in the frequency count of keywords), and 0 otherwise
Breach	Indicator variable taking the value of 1 in the fiscal year before and the fiscal year during which the company has any data breach, and 0 otherwise
Post	Indicator variable taking the value of 1 for the post period, i.e., years when a data breach occurs for breached firms and years of the match for non-breached firms, and 0 otherwise
Severity	An index value ranging from 0 to 4 based on the severity of the data breach incident (0 = lowest severity and 4 = highest severity). The value of index is decided by four attributes of each data breach incident including type of data breached, the amount of data breached, the source of the breach, and whether the hackers used the breached data. For each of the four attributes mentioned above, we assign the value of 1 to more severe cases or 0 otherwise. In particular, a data breach is considered as a severe case when there are multiple types of data breached, when the number of records breached is greater than 10,000, when the source of the breach is either hacking or insiders[a], and when there is evidence shows the breached information is used. Summing up the values of the four attributes, we get *Severity*
CAR	Cumulative abnormal return in the three days around the 10-K filing date [-1,1]. We estimate this variable using the Carhart four-factor model
Size	The natural logarithm of total assets at the end of the fiscal year during which a data breach occurred
MTB	Market value (Compustat PRCC_F × CSHO) divided by book value of equity (Compustat CEQ) at the end of the fiscal year during which a data breach occurred
Leverage	Total of long-term debt (Compustat DLTT) and current debt (Compustat DLC) divided by total assets (Compustat AT) at the end of the fiscal year during which a data breach occurred
Litigation	An indicator variable that equals one for firms in SIC codes 2833–2836, 3570–3577, 3600–3674, 5200–5961, 7370–7374, and 8731–8734, zero otherwise
Post-2011	An indicator variable that equals one for firm-years if the fiscal year end date is after Dec 31, 2011, and zero otherwise
MediaAttention	Daily average of the number of news articles in Nexis Uni database that include both the name of breached firm and any cybersecurity risk-related expressions in the title of the article between the announcement date of the breach and the 10-K filing date identified using our primary keyword list
DeltaCyberDisclose	Change in the frequency count of cybersecurity risk-related keywords in Item 1A of 10-Ks from pre to post-data breach period, based on our primary keyword list, which is an augmentation of the Li et al. (2018)'s keyword list
DeltaLength	The change in total nonstop word frequency count in Item 1A of 10-Ks from pre to post-data breach period

[a]Other sources not as severe include the following: fraud Involving debit and credit cards not via hacking; paper documents that are lost, discarded, or stolen; portable device lost; stationary computer loss; unintended disclosure of sensitive information; and not enough information about the breach to know how exactly the information was exposed

Table 10 Frequency of cybersecurity risk-related expressions in 10-Ks containing decreased cybersecurity risk factor disclosures

Identified exclusively using our primary keyword list	*N*	Post-breach	Pre-breach	Difference
Confidential(ity)	10	35	39	− 4
(information|network) security	10	16	20	− 4
Information (technology|attack)	10	22	25	− 3
Computer (virus|breach|break-in|attack|security)	10	11	12	− 1
Phishing	10	2	3	− 1
Data breach	10	0	1	− 1
Security (breach|incident)	10	24	24	0
Unauthorized access	10	14	14	0
Encryption	10	5	5	0
(hacking|hacker)	10	3	3	0
Identified exclusively using Ghadge et al. (2019)'s keyword list	*N*	Post-breach	Pre-breach	Difference
Disruption	32	150	173	− 23
Infrastructure	32	65	79	− 14
Security	32	226	235	− 9
Cyberattack	32	1	5	− 4
Terrorism	32	24	28	− 4
Threat	32	24	28	− 4
Cybersecurity	32	4	6	− 2
Cybersecurity	32	11	13	− 2
Information (security|risk)	32	5	6	− 1
Risk assessment	32	1	1	0

Appendix 5: Frequency of Cybersecurity Risk-Related Expressions Whose Uses Drop Most After Data Breaches

This appendix presents the frequency of cybersecurity risk-related keywords whose uses in the 10-K filings drop most after data breaches. Frequency of the expressions for firm-years with decreased cybersecurity risk factor disclosures exclusively identified using our primary keyword list are presented in Panel A and frequency for firm-years exclusively identified using Ghadge et al. (2019)'s keyword list are presented in Panel B. Our entire primary keyword list is reported in Appendix 1. The keywords in Ghadge et al. (2019)'s keyword list include follows: "enterprise risk management," "risk management," "supply chain attacks," "supply chain crime," "supply chain integrity," "supply chain integrity risk," "supply chain resilience," "supply chain risk(s)," "supply chain security," "supply chain threats," "risk identification," "risk assessment," "risk mitigation," "risk control," "cyber security," "cyber attack," "cyber breaches," "cyber crime," "cyber crisis," "cyber disruptions," "cyber/IT failure," "cyber incident," "cyber resilience," "cyber supply chain(s)," "cyber supply chain risk management," "cyber systems," "cyber supply network," "data/information security," "information infrastructure," "information security/risk," "cybersecurity," "disruption," "firewall," "hacker," "infrastructure," "phishing," "sabotage," "security," "spoofing," "surveillance," "terrorism," "threat" (Table 10).

Acknowledgements An earlier version of this paper circulated under the title "Cybersecurity Risk Factor Disclosures Following a Data Breach." We thank Steven Dellaportas (Section Editor), two anonymous reviewers, Naomi Soderstrom and workshop participants at Stevens Institute of Technology, the 2021 Joint Midyear Meeting of the AIS and SET Sections, and the 2021 AAA Annual Meeting for helpful suggestions and comments. Jing Chen gratefully acknowledges the support of Jack Howe Fellowship from the Stevens' School of Business.

Funding Jack Howe Fellowship from the Stevens' School of Business.

Data Availability All data are from publicly available sources.

Material Availability All data are from publicly available sources.

Code Availability SAS and Stata code used will be made available to the editor upon request.

Declarations

Conflicts of interest The authors have no conflicts of interest to declare that are relevant to the content of this article.

Ethical Approval Not applicable.

Informed Consent Not applicable.

References

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*(3), 1177–1206.

Audit Analytics. (2020). Trends in cybersecurity breach disclosures. Retrieved from https://blog.auditanalytics.com/trends-in-cybersec

Armental, M. (2019). Marriott takes $126 million charge related to data breach, *Wall Street Journal*, August 5. Retrieved from https://www.wsj.com/articles/marriott-take-126-million-charge-related-to-data-breach-11565040121

Baudot, L., Huang, Z., & Wallace, D. (2021). Stakeholder perceptions of risk in mandatory corporate responsibility disclosure. *Journal of Business Ethics, 172*(1), 151–174.

Beatty, A., Cheng, L., & Zhang, H. (2019). Are risk factor disclosures still relevant? Evidence from market reactions to risk factor disclosures before and after the financial crisis. *Contemporary Accounting Research, 36*(2), 805–838.

Bennett, C. (2015). SEC weights cybersecurity disclosure rules. *The Hill*. Retrieved from https://thehill.com/policy/cybersecurity/229431-sec-weighs-cybersecurity-disclosure-rules

Berkman, O. (2018). Disclosure effectiveness weakened by complicated ownership. *Financial Executives International Daily.* Retrieved from https://www.financialexecutives.org/FEI-Daily/January-2018/owns-risk-help-disclose-risk.aspx

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2021). Digital insiders and informed trading before earnings announcements. Working Paper. Available at https://ssrn.com/abstract=3180531.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy, 37*(6), 508–526.

Burns, J. (2017). SEC reveals its EDGAR database was hacked, maybe used for illegal trades. Retrieved from https://www.forbes.com/sites/janetwburns/2017/09/21/sec-reveals-that-hackers-may-have-used-edgar-data-for-illegal-trades/.

Bushee, B. J., & Miller, G. S. (2012). Investor relations, firm visibility, and investor following. *The Accounting Review, 87*(3), 867–897.

Campbell, J. L., Cecchini, M., Cianci, A. M., Ehinger, A. C., & Werner, E. M. (2019). Tax-related mandatory risk factor disclosures, future profitability, and stock returns. *Review of Accounting Studies, 24*(1), 264–308.

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. M., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies, 19*(1), 396–455.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70–104.

Chiu, T. T., Guan, Y., & Kim, J. B. (2018). The effect of risk factor disclosures on the pricing of credit default swaps. *Contemporary Accounting Research, 35*(4), 2191–2224.

Clayton, J. (2018). Statement on cybersecurity interpretive guidance. Retrieved from https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21.

Cowley, S. (2019). Equifax to pay at least $650 million in largest-ever data breach settlement. *The New York Times*.

Deloitte (2016). Beneath the surface of a cyberattack. A deeper look at business impact. *Deloitte Development*. Retrieved from https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/beneath-the-surface-of-a-cyberattack.html.

Diamond, D. W., & Verrecchia, R. E. (1991). Disclosure, liquidity, and the cost of capital. *The Journal of Finance, 46*(4), 1325–1359.

Engster, D. (2011). Care ethics and stakeholder theory. In M. Hamington & M. S. Staudt (Eds.), *Applying care ethics to business* (pp. 93–110). Dordrecht: Springer.

Ernst & Young LLP. (2005). Comment letter on Securities Offering Reform Commission File No. S7–38–04. Retrieved from https://www.sec.gov/rules/proposed/s73804/ernst013105.pdf

Fang, V. W., Huang, A. H., & Karpoff, J. M. (2016). Short selling and earnings management: A controlled experiment. *The Journal of Finance, 71*(3), 1251–1294.

Fields, T. D., Lys, T. Z., & Vincent, L. (2001). Empirical research on accounting choice. *Journal of Accounting and Economics, 31*(1–3), 255–307.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468.

Gensler, G. (2021). Testimony before the United States Senate Committee on Banking, Housing, and Urban Affairs. Accessed at: https://www.sec.gov/news/testimony/gensler-2021-09-14.

Gensler, G. (2022). Cybersecurity and Securities Laws. Speech at the Northwestern Pritzker School of Law's Annual Securities Regulation Institute. Retrieved from https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124.

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy, 25*(5), 503–530.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly, 34*, 567–594.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33–56.

Haislip, J., Kolev, K., Pinsker, R., & Steffen, T. (2019). The economic cost of cybersecurity breaches: A broad-based analysis. In *Workshop on the Economics of Information Security (WEIS)* (pp. 1–37).

Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics, 31*(1–3), 405–440.

Hermalin, B. E., & Weisbach, M. S. (2012). Information disclosure and corporate governance. *The Journal of Finance, 67*(1), 195–233.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: Who cares?. *Georgetown McDonough School of Business Research Paper* (2852519).

Hope, O. K., Hu, D., & Lu, H. (2016). The benefits of specific risk-factor disclosures. *Review of Accounting Studies, 21*(4), 1005–1045.

Huang, H. H., & Wang, C. (2021). Do Banks Price Firms' Data Breaches? *The Accounting Review, 96*(3), 261–286.

Intel Corporation. (2005). Re: File No. S7–38–04; Securities offering reform. Retrieved from https://www.sec.gov/rules/proposed/s73804/cklafter013005.htm

Investor Responsibility Research Center Institute (IRRC). (2016). *The corporate risk factor disclosure landscape*.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing, 82*(2), 85–105.

Johnson, S. (2010). SEC pushes companies for more risk information. *CFO Magazine*, *2*.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719–749.

Kim, I., & Skinner, D. J. (2012). Measuring securities litigation risk. *Journal of Accounting and Economics, 53*(1–2), 290–310.

Kothari, S. P., Li, X., & Short, J. E. (2009). The effect of disclosures by management, analysts, and business press on cost of capital, return volatility, and analyst forecasts: A study using content analysis. *The Accounting Review, 84*(5), 1639–1670.

Kravet, T., & Muslu, V. (2013). Textual risk disclosures and investors' risk perceptions. *Review of Accounting Studies, 18*(4), 1088–1122.

Lang, M. H., & Lundholm, R. J. (1996). Corporate disclosure policy and analyst behavior. *Accounting Review*, 467–492.

Lewis, P. V. (1985). Defining 'business ethics': Like nailing jello to a wall. *Journal of Business Ethics, 4*(5), 377–383.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems, 30*, 40–55.

Malone, S. (2005). Refco risks boiler-plate disclosure. Reuters, October 21.

Morgan, G., & Gordijn, B. (2020). A care-based stakeholder approach to ethics of cybersecurity in business. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The ethics of cybersecurity* (pp. 119–138). Cham: Springer.

Morse, E. A., Raval, V., & Wingender, J. R., Jr. (2017). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. *The Business Lawyer, 73*(1), 1–34.

Nagar, V., Nanda, D., & Wysocki, P. (2003). Discretionary disclosure and stock-based incentives. *Journal of Accounting and Economics, 34*(1–3), 283–309.

Nelson, K. K., & Pritchard, A. C. (2016). Carrot or stick? The shift from voluntary to mandatory disclosure of risk factors. *Journal of Empirical Legal Studies, 13*(2), 266–297.

Patrignani, N., & Whitehouse, D. (2014, July). Slow Tech: the bridge between computer ethics and business ethics. In *IFIP International Conference on Human Choice and Computers* (pp. 92–106). Springer, Berlin, Heidelberg.

PwC. (2017). Consumer intelligence series: Protect.me. Retrieved from https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html

Racine, M., Wilson, C., & Wynes, M. (2020). The value of apology: How do corporate apologies moderate the stock market reaction to non-financial corporate crises? *Journal of Business Ethics, 163*(3), 485–505.

Radu, C., & Smaili, N. (2021). Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure. *Journal of Business Ethics*, 1–24.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies, 11*(1), 74–104.

Schechter, S. E., & Smith, M. D. (2003, January). How much security is enough to stop a thief?. In *International Conference on Financial Cryptography* (pp. 122–137). Springer, Berlin, Heidelberg.

Securities and Exchange Commission (SEC). (2005). *Securities and exchange commission final rule, release no. 33-8591: 1-468*. Retrieved from https://www.sec.gov/rules/final/33-8591.pdf

Securities and Exchange Commission (SEC). (2010). *17 CFR PARTS 211, 231 and 241. Release Nos. 33-9106; 34–61469; FR-82*. Retrieved from https://www.sec.gov/rules/interp/2010/33-9106.pdf

Securities and Exchange Commission (SEC). (2011). CF disclosure guidance: Topic No. 2, cybersecurity, provided by the division of corporation finance. Retrieved from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Securities and Exchange Commission (SEC). (2016). *Business and financial disclosure required by Regulation S-K, release no. 33–10064; 34-77599*; File No. S7-06-16: 1–341. Retrieved from https://www.sec.gov/rules/concept/2016/33-10064.pdf

Securities and Exchange Commission (SEC). (2017). *SEC Chairman Clayton issues statement on cybersecurity*. Retrieved from https://www.sec.gov/news/press-release/2017-170.

Securities and Exchange Commission (SEC). (2018). *Commission statement and guidance on public company cybersecurity disclosures, release no. 33-10459*. https://www.sec.gov/rules/interp/2018/33-10459.pdf

Securities and Exchange Commission (SEC). (2019). *Modernization of Regulation S-K Items 101, 103, and 105, release no. 33-10668*. Retrieved from https://www.sec.gov/rules/proposed/2019/33-10668.pdf

Skinner, D. J. (1994). Why firms voluntarily disclose bad news. *Journal of Accounting Research, 32*(1), 38–60.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security, 58*, 216–229.

Stein, K. (2018). Statement on commission statement and guidance on public company cybersecurity disclosures. Retrieved from https://www.sec.gov/news/public-statement/statement-stein-2018-02-21

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information systems research, 24*(2), 201–218.

Watts, R. L., & Zimmerman, J. L. (1986). Positive accounting theory.

Wicks, A. C., Gilbert, D. R., Jr., & Freeman, R. E. (1994). A feminist reinterpretation of the stakeholder concept. *Business ethics quarterly, 4*, 475–497.