Journal of the Association for Information Systems

Volume 23 | Issue 3 Article 2

2022

The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures

John D'Arcy
University of Delaware, jdarcy@udel.edu

Asli Basoglu
University of Delaware, asli@udel.edu

Recommended Citation
D'Arcy, John and Basoglu, Asli (2022) "The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures," *Journal of the Association for Information Systems*, 23(3), 779-805.
DOI: 10.17705/1jais.00740
Available at: https://aisel.aisnet.org/jais/vol23/iss3/2

Journal of the Association for Information Systems (2022) **23**(3), 779-805
doi: 10.17705/1jais.00740

RESEARCH ARTICLE

ISSN 1536-9323

The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures

John D'Arcy,[1] K. Asli Basoglu[2]

[1]University of Delaware, USA, jdarcy@udel.edu
[2]University of Delaware, USA, asli@udel.edu

Abstract

Cybersecurity disclosures in reports filed with the US Securities and Exchange Commission (SEC) inform investors about firms' cybersecurity incidents, risks, and related risk management efforts. Firms have traditionally chosen to communicate such information on a quarterly or annual basis, if at all, and prior research on the topic has largely focused on regulatory factors as driving forces. In this paper, we focus on timely disclosures (via 8-K filings) and derive hypotheses regarding the influences of two alternate forms of pressure as drivers of cybersecurity disclosures—(1) public pressure following a firm's data breach and (2) pressure arising from the breaches of industry peers, which we cast as "institutional pressure." We also theorize on how the source of the breach (internal or external) influences these forms of pressure. Our results suggest that firms' cybersecurity disclosure practices are influenced by public pressure following a data breach and that this pressure is more acute for external breaches than for internal breaches. By contrast, breaches by industry peers, as a form of institutional pressure, appear to prompt fewer cybersecurity disclosures, except when the focal firm suffers its own external breach. From a theoretical perspective, our study supports a nuanced application of legitimacy theory in the cybersecurity disclosure context, especially in the midst of public and institutional pressure, such that the source of a data breach determines whether firms attempt to address the resultant legitimacy gap. From a practical perspective, our results may be viewed as alarming in that firms are not reacting to internal breaches with the same degree of communicative effort about cybersecurity as for external breaches, at least in terms of the timely disclosures we consider in this study. Our findings also point to certain levers that can promote timely cybersecurity disclosures, and thus have important policy implications.

Keywords: Data Breach, Information Security, Cybersecurity, Disclosure, Legitimacy Theory, Institutional Pressure, Public Attention, Longitudinal, Panel Data

Jason Bennett Thatcher was the accepting senior editor. This research article was submitted on September 20, 2020 and underwent three revisions.

1 Introduction

Cybersecurity has risen to the forefront of corporate priorities (Collins, 2018; Kappelman et al., 2020) because of the substantial financial and reputational costs that can accompany data breaches and other cybersecurity incidents (e.g., denial-of-service attacks, ransomware). It's no wonder, therefore, that stakeholders are seeking increased information from firms regarding their cybersecurity. For example, according to one survey, more than 70% of US investors are interested in reviewing firms' cybersecurity practices to assist in their investment decisions (HBGary, 2013). Likewise, regulators are pushing firms to disclose more cybersecurity information that would be useful to investors and other market participants (e.g., credit rating agencies, securities analysts) who have an interest in valuing the firm and its long-term viability. In

2011 the US Securities and Exchange Commission (SEC) issued guidance to assist public companies in preparing disclosures about their cybersecurity risks, incidents, and mitigation efforts in SEC filings (SEC, 2011). While not a formal regulation, the guidance essentially obligated publicly traded companies to disclose such information if it could affect investors' decisions about the firm (i.e., if "material" information in an accounting sense) (Li et al., 2012). Although cybersecurity disclosures had begun to increase before the 2011 SEC guidance (Gordon et al., 2010), they increased substantially afterward, particularly in terms of cybersecurity risk factors disclosed in annual 10-K reports (Hilary et al., 2016; Li et al., 2018). An important point, however, is that because the firm determines whether its potential cybersecurity disclosure is material information to investors, it has much discretion in deciding whether, what, or how much information to disclose (Gordon et al., 2010; Romanek, 2016).

Also at issue is whether the prevailing practice of providing cybersecurity disclosures in quarterly (10-Q) or annual (10-K) reports provides the type of timely information that investors need. The lack of timely information on a firm's cybersecurity risks and risk management efforts can be harmful to investors seeking to determine whether the firm is likely to be victimized by a breach. Likewise, delays regarding the details of a breach [1] and the financial costs and litigation efforts surrounding a breach can be harmful to investors who need timely access to such information to make informed investing decisions. As a result, in 2018, the SEC recommended timelier (i.e., on a regular and ongoing basis) disclosures of cybersecurity information (SEC, 2018).

Timely cybersecurity disclosures are the subject of the current study. Specifically, we focus on firms' cybersecurity disclosures in 8-K reports filed with the SEC. Publicly traded companies use 8-K reports to notify investors of significant/material events (e.g., bankruptcy, senior officer appointments and departures) and these firms typically must file the report within four business days after the event (Lerman & Livnat, 2010). Hence, 8-Ks are known as "current reports" in that they provide timely information to investors on matters they should know about, rather than having them wait for quarterly or annual reports. Empirical studies have shown significant market reactions to 8-Ks, thus supporting their content as being uniquely informative to investors (He & Plumlee, 2020; Lerman & Livnat, 2010). Cybersecurity disclosures in 8-Ks are therefore distinct from cybersecurity disclosures in other, less timely reports filed with the SEC and, as we later elaborate, this "timeliness" aspect makes the disclosure decision particularly amenable to forms of external pressure. Importantly, cybersecurity disclosures in 8-Ks are also distinct from public data breach announcements (see Table 1), as the former can include content on a wide span of cybersecurity issues to assist investors in valuing the firm.

Regarding such content, firms may file an 8-K to disclose a data breach if they deem it a material event, but evidence suggests that 8-Ks filed solely for this reason (i.e., a breach as the triggering event) are relatively rare (Hilary et al., 2016; Richardson et al., 2019).[2] More common are 8-Ks filed for other, non-cybersecurity events but include cybersecurity information at various places in the report. Such information is discretionary and may include details on cybersecurity risk management efforts; discussions of firm-specific cybersecurity risks; and updates on financial costs, legal proceedings, and other issues related to previously announced data breaches (see Appendix A for examples of the range of cybersecurity content in 8-Ks).

Firms have an incentive to strategically manage their cybersecurity disclosures, just as they do with other voluntary disclosures such as those involving business risks, certain financial information, and environmental and social performance (Miller & Skinner, 2015). On the one hand, regulatory forces are pushing firms to disclose more cybersecurity information and to do so on a timely basis. On the other hand, disclosing cybersecurity information could assist hackers in successfully attacking the firm (Li et al., 2018; SEC, 2018), which would weaken disclosure incentives. Likewise, firms may not want to disclose certain cybersecurity information (e.g., firm-specific defense mechanisms and risk management efforts) for fear that it could weaken their competitive standing. Since prior research indicates that even with the recent regulatory pressure, cybersecurity disclosures vary greatly in terms of who discloses, how much is disclosed, and how frequently (e.g., Hilary et al., 2016; Li et al. 2018), an important research question is: *What factors drive timely cybersecurity disclosures (in 8-Ks)?*

We explore this question by drawing on legitimacy theory, perspectives from institutional theory research, and the literature on corporate impression management to derive hypotheses regarding the

[1] State laws and other regulations require firms to publicly report data breaches, but these regulations vary in terms of the threshold for and contents of notification (Coleman et al., 2019). Hence, investors may need to rely on firms' voluntary disclosures about data breaches in their SEC filings, particularly for expanded details about the breach (e.g., source of the attack, type of information breached, what vulnerabilities were exploited) and post-breach updates on financial damages and/or ongoing litigation.

[2] For example, in Hilary et al. (2016), there were five 8-Ks that were filed solely for a previously unannounced data breach during the period 2005-2014.

influence of two forms of pressure—from the public and from industry peers (the latter we cast as "institutional pressure")—as drivers of cybersecurity disclosures. We position these forms of pressure in the context of cybersecurity disclosures following a data breach, as past research shows that firms alter their disclosure practices in response to adverse organizational events, and legitimacy theory supports them doing so in a timely manner. Our theorizing also considers how the source of the breach (internal or external) influences the relationships between public and institutional pressure and cybersecurity disclosures. By focusing on cybersecurity disclosures in 8-Ks, we provide a strong test of the influences of public and institutional pressure, as 8-Ks are investors' first exposure to cybersecurity information, in terms of SEC filings, and thus can be considered firms' most proactive communicative efforts about cybersecurity in this context.

Our analysis is based on a panel dataset that was derived from public sources, including: (1) announcements of data breaches that affected publicly traded firms between 2005 and 2018, (2) cybersecurity disclosures in 8-Ks for these firms, and (3) the volume of Google searches on these firms, as an indicator of public pressure. The results suggest that firms' cybersecurity disclosure practices are influenced by public pressure following a data breach and that this pressure is more acute for external breaches than for internal breaches. By contrast, breaches by industry peers, as a source of institutional pressure, prompt *fewer* cybersecurity disclosures, except when the focal firm suffers its own external breach. These results hold in the post-2011 SEC disclosure guidance period, thereby supporting public and institutional pressure as determinants of cybersecurity disclosures beyond the influence of regulatory pressure. From a theoretical perspective, our study supports a nuanced application of legitimacy theory in the cybersecurity disclosure context, especially in the midst of public and institutional pressure, such that the source of a data breach determines whether firms attempt to address the resultant legitimacy gap. From a practical perspective, our results may be viewed as alarming in that firms are not reacting to internal breaches with the same degree of communicative effort about cybersecurity as for external breaches, at least in terms of the timely disclosures we consider.

2 Relevant Literature

The literature on the antecedents and outcomes of firms' communications about cybersecurity provides a foundation for our research and the specific hypotheses we explore. Our study is also informed by the literature on voluntary disclosures from accounting and other disciplines and perspectives from institutional theory research, as we elaborate in the following section.

2.1 Impact of Firms' Cybersecurity Communications

There is a sizeable body of work on the economic impact of public announcements of cybersecurity incidents such as data breaches and other forms of cyberattack against the firm (e.g., denial-of-service attacks, website defacements, phishing attacks). Spanos and Angelis (2016) reviewed 28 studies that assessed the stock market response to cybersecurity incident announcements and the results showed a significant negative impact to the firm in 20 studies (71.4%). Richardson et al. (2019) provide a comprehensive review (41 studies) of research that explored firms' stock market response to data breach announcements. Their results vary based on the time period being studied, type of information affected, and the means of disclosure, but, in an overall sense, they provide evidence that data breach announcements produce a modest negative stock market response for breached firms that is typically short-lived. Additional research suggests that firms' stock price reaction to data breach announcements may be more significant and longer-term depending on the severity of the incident (Amir et al., 2018).

Gordon et al. (2010) explored more expansive cybersecurity disclosures in SEC filings.[3] Specifically, they studied voluntary disclosures of both positive (e.g., cybersecurity risk management activities) and negative (e.g., cybersecurity risks and vulnerabilities) information in 10-K reports and found them to both be positively associated with the market value of the firm. Wang et al. (2013) focused specifically on disclosures of cybersecurity risk factors in 10-Ks and found the market reaction to be negative, albeit less negative when the disclosures included cybersecurity risk mitigation activities.

There is also evidence that firms' cybersecurity communications have influences besides their stock prices. For example, Janakiraman et al. (2018) found that a data breach announcement from a large retailer resulted in decreased customer spending and migration to its unbreached channels (i.e., from physical stores to internet and catalogue shopping). Benaroch and Chernobai (2017) found that disclosed IT failures related to cybersecurity resulted in changes to the IT competency levels of firms' executive leadership.

[3] Hereafter, "cybersecurity disclosure" refers to cybersecurity communications in reports filed with the SEC. This is not to be confused with other firm communications about cybersecurity, such as data breach announcements.

Lawrence et al. (2018) found a positive relationship between data breach announcements and subsequent year financial reporting deficiencies (e.g., financial reporting control weaknesses, earnings restatements). Other studies focused on disclosures of cybersecurity risk factors, including weak IT controls related to financial reporting, in 10-Ks and their impact on the firm. For example, Li et al. (2012) found that disclosed IT control weaknesses were positively associated with management earnings forecast errors, whereas Masli et al. (2016) found that IT control weakness disclosures predicted subsequent year chief executive officer or chief financial officer turnover. Cybersecurity risks disclosed in 10-Ks have also been linked to an increased likelihood of a data breach in the following year (Li et al, 2018; Wang et al., 2013).

Collectively, the results indicate that communications about cybersecurity are impactful to the firm in a variety of ways—they influence stock prices, financial reporting quality, consumer behavior, likelihood of future data breaches, changes in executive leadership, etc. It follows that gaining an understanding of what drives such communications is important for both cybersecurity research and practice. Yet there is scant research on the drivers of firms' cybersecurity communications, particularly in terms of cybersecurity disclosures in reports filed with the SEC. The limited work in this specific realm has mostly considered regulations to be a driving factor (see the following paragraph). This makes sense considering that certain cybersecurity disclosures are mandatory, such as identifying material IT control weaknesses related to financial reporting per the provisions of the Sarbanes-Oxley (SOX) Act of 2002. SOX requires firms to include a statement about such weaknesses in their quarterly and annual reports, although the decision to report and describe specific weaknesses is discretionary (Gordon et al., 2006; Rice et al., 2015). Even for the types of disclosures that are not mandatory, such as cybersecurity risk factors, cybersecurity risk management activities, and expanded details related to data breaches, there is increasing regulatory pressure to disclose, as described earlier. Hence, regulatory pressure is a major influence on firms' cybersecurity disclosure decisions.

On this point, the literature provides evidence that firms have responded to regulatory pressure with increased disclosures. For example, Gordon et al. (2006) found increased cybersecurity disclosures in 10-Ks following the passage of SOX, and others have documented increased disclosures of cybersecurity risk factors in 10-Ks following the 2011 SEC disclosure guidance (Hilary et al., 2016; Li et al., 2018) and the passage of state data breach notification laws (Ashraf & Sunder, 2020). Yet there is still much variance in terms of who discloses and to what extent. Similar variance is evident in the studies of cybersecurity disclosures when assessing time periods before the recent regulatory pressure, as well as in our own analysis of cybersecurity disclosures in 8-Ks. These results point to additional, unexplored drivers of firms' cybersecurity disclosures, which is the subject of the current study.

Within the current policy landscape, cybersecurity disclosures are essentially a strategic choice by the firm, which aligns with the notion of discretionary disclosure from the accounting literature—i.e., "a situation in which managers or firms exercise discretion with respect to the disclosure of information about which they may have knowledge" (Verrecchia, 2001, p. 146). The timely and proactive cybersecurity disclosures we consider in this study (via 8-Ks) fit this description, and so we turn to the literature on voluntary disclosures in accounting and other disciplines for direction in terms of potential unexplored determinants of cybersecurity disclosures.

2.2 Determinants of Firms' Voluntary Disclosures

A key finding from the voluntary disclosure literature is that forms of external pressure influence firms' disclosure decisions. The rationale is that firms respond to external pressure through disclosures (in their SEC filings) as a way to manage their reputations and conform to investors' expectations (Bansal & Clelland, 2004; Patten, 2002). Consistent with this logic, research has shown increased disclosures of, for example, environmental and community initiatives, disaster readiness activities, and risk mitigation efforts following highly publicized adverse organizational events or firms' reported poor social or environmental performance (Bansal & Clelland, 2004; Cho et al., 2012; Clarkson et al., 2008; Heflin & Wallace, 2017; Marquis et al., 2016; Patten, 2002; Patten & Trompeter, 2003). Likewise, research has found that firms are more forthcoming with negative information, such as financial and operational risk disclosures, after reporting internal control weaknesses and other material risk-related concerns (Ashbaugh-Skaife et al., 2007; Lawrence et al., 2018; Oliveira et al., 2011a, 2011b).

While research generally points to external pressure as a driver of voluntary disclosures, the influence of public pressure appears particularly salient. Multiple studies have shown that public pressure, measured in different ways (e.g., media attention, firm visibility, industry classification), influences firms' disclosures of financial, social, and environmental information following adverse events or poor performance (Brown & Deegan, 1998; Neu et al., 1998; Oliveira et al., 2011a, 2011b). Drawing on this literature, we consider public pressure, conceptualized as public attention following a data breach, as a driver of cybersecurity disclosures in the current study. Our focus on public pressure is warranted because of the societal impact of data breaches and the

resultant growth in public awareness and concern regarding cybersecurity issues (Albon et al., 2014; Ponemon Institute, 2014), which has helped fuel investor concerns in this area (SEC, 2018).

Noteworthy in the studies showing disclosure practices being influenced by adverse organizational events is that the influences of the events can spill over into the disclosure practices of other firms in the same industry (e.g., Heflin & Wallace, 2017; Patten, 1992; Patten & Trompeter, 2003). This finding suggests that firms' voluntary disclosure decisions are influenced by the actions of their industry peers. Disclosure decisions being influenced by industry peers makes sense in our cybersecurity context, given the evidence that investor reactions to cybersecurity events can be industry-wide (Hinz et al., 2015; Jeong et al., 2019). As well, research has shown that firms closely monitor the practices of industry peers in making strategic IT decisions (Cavusoglu et al., 2015; Ogbanufe et al., 2021). In a broad sense, the evidence of such peer effects aligns with perspectives from institutional theory, which suggests that firms' actions and decisions are often influenced by the behavior of other firms in their industry (DiMaggio & Powell, 1983; Oliver, 1991). Within institutional theory research, external influences or demands at the industry level have been characterized as a form of institutional pressure (Depoers & Jerome, 2020; Hoejmose et al., 2014; Martinez-Ferrero & Garcia-Sanchez, 2017). We draw on this work and consider the breaches of industry peers as a form of institutional pressure that helps drive (focal) firms' cybersecurity disclosure decisions. Importantly, we are not arguing that firms imitate the behavior of their industry peers, as with the idea of institutional isomorphism, but more broadly that the actions of industry peers (in this case, their data breaches) are institutional influences on the decisions of focal firms. We elaborate on these specific influences later in the hypotheses development.

The preceding literature review sets the stage for our theoretical framing and hypotheses, in which we describe a data breach as a baseline form of pressure that influences cybersecurity disclosures, and how public and institutional pressure linked to certain data breaches act as additional forms of pressure in this context.

3 Theoretical Framing and Hypotheses

The idea that firms respond to external forms of pressure by altering their disclosure practices, as a means of managing their reputations and conforming to investor expectations, has a theoretical basis in legitimacy theory. Legitimacy theory proposes that organizations exist in society under an expressed or implied social contract, which stipulates that organizations must act to maintain legitimacy in the eyes of stakeholders (Deephouse & Suchman, 2008; Suchman, 1995). In this context, legitimacy refers to the degree to which an organization's actions are endorsed and accepted by its stakeholders (Scott, 2008). Central to legitimacy theory is thus that stakeholders deliberate on activities that are acceptable by the firm and that firms are expected to carry out their activities within the boundaries of these acceptability standards (Deephouse & Suchman, 2008; Suchman, 1995). Failure to do so represents a breach of the implied social contract (i.e., a violation of stakeholder expectations), which can be damaging to the firm's legitimacy and thus negatively affect its ongoing survival. Stakeholders can vary based on context but, in general, they refer to relevant publics (e.g., customers, investors, community members, business partners, regulators, etc.) that are affected by the organization's activities (Neu et al., 1998). In our study context, when considering the information conveyed in cybersecurity disclosures, the primary stakeholders of interest are the investors and other market participants who use this information to assist in valuing the firm.

In terms of voluntary disclosures in SEC filings, based on the notion that legitimacy is gained through specific firm actions that are endorsed by its stakeholders, firms attempt to legitimize themselves by disclosing information that is in line with investor expectations (e.g., a new environmental program, disaster readiness actions, community initiatives) (Bansal & Clelland, 2004; Marquis et al., 2016). Similarly, when firms face negative circumstances and/or engage in activities that are deemed counter to investor expectations (e.g., an environmental disaster, customer information compromised by a data breach), a legitimacy gap will emerge, and firms will attempt to address the incongruence through disclosure of relevant information (Chalmers & Godfrey, 2004; Cho & Patten, 2007; Patten, 2002).[4] Hence, the link between legitimacy theory and disclosure is that organizational legitimacy is gained, maintained, or restored through a specified level of public disclosure (Bansal & Clelland, 2004; Deephouse & Suchman, 2008).

We consider cybersecurity disclosures as one such type of public disclosure, consistent with the sizeable body of disclosure literature that is rooted in legitimacy theory and thus views corporate disclosures in regulatory filings as tools for legitimization. A key point about legitimacy is that it requires continuous attention because stakeholder expectations can change over time (Suchman, 1995).

[4] Even disclosures of negative information can be legitimacy enhancing, as they can signal to stakeholders the firm's accountability and willingness to address future legitimacy concerns (Skinner, 1994; Suchman, 1995).

Table 1. Summary of Constructs

Construct	Definition	Operationalization
Cybersecurity disclosure	Cybersecurity information included in 8-Ks. Content can include details about a specific data breach incident but may also include details on cybersecurity risk management efforts; discussions of firm-specific cybersecurity risks; and updates on financial costs, legal proceedings, and other issues related to previously announced data breaches. The intended audience is investors and other market participants who seek to value the firm. The content comes directly from the firm.	Number of cybersecurity-related words in 8-Ks
Data breach announcement	Public announcement of a firm's data breach incident. Content is specific to the breach, given what is known at the time of the breach or shortly thereafter, and does not include the more expansive cybersecurity content (e.g., cybersecurity risk factors and risk management efforts) found in cybersecurity disclosures. The intended audience is the general public and so the content is often succinct and purposefully vague. The content may be filtered by the media and/or regulatory bodies.	Public announcement of a data breach
Public pressure	Pressure on the firm, arising from the public, that alters the firm's disclosures of cybersecurity information (in 8-Ks).	Public attention surrounding a firm's data breach
Institutional pressure	Pressure on the firm, arising from the data breaches of industry peers, that alters the firm's disclosures of cybersecurity information (in 8-Ks).	Data breaches by other firms in the same industry

For adverse organizational events in particular, firms have an incentive to address the associated legitimacy gaps in a timely manner to avoid signaling unresponsiveness to investors, since investors can swiftly change their legitimacy perceptions following negative information about a firm (Flammer, 2013). The theoretical reasoning that legitimacy threats compel firms' timely responses aligns with our focus on 8-K reports (i.e., "current reports") as the disclosure medium in this study. As we describe in our hypotheses, we augment the legitimacy theory perspective with the literature on corporate impression management to develop context-specific predictions about whether firms will use cybersecurity disclosures in response to data breaches, and also consider the influences of public and institutional pressure and the source of the breach in the disclosure decision. Table 1 summarizes the main constructs in this study, which we next further elaborate in developing the hypotheses.

In developing our hypotheses, we first position a data breach as a negative organizational event that violates investors' expectancy, and thus raises their legitimacy concerns. As Gwebu et al. (2018) state, "one set of norms that governs data security practices is the expectation concerning organizations' ability and responsibility to properly and safely collect, use, and protect the stakeholder data" (p. 690). Hence, it can be expected that when a data breach occurs, investors will view this organizational activity as incongruent with their expectations for acceptable (or, value-generating) firm behavior, and a legitimacy gap will emerge. Based on legitimacy theory, we conjecture that firms will seek to address the legitimacy gap that is caused by a data breach by proactively disclosing cybersecurity information. Here again, it is important to recognize the distinction between data breach announcements and cybersecurity disclosures. Our contention is that a data breach will prompt increased disclosures of cybersecurity information, in a general sense, rather than just information about the breach. This is similar to, for example, how firms increase their voluntary disclosures of environmental risk strategies and initiatives to improve the environment after reporting poor environmental performance (Clarkson et al., 2008; Heflin & Wallace, 2017).

In keeping with the legitimacy perspective, firms will employ the broader cybersecurity disclosures in an effort to restore investor confidence and trust by taking accountability for the breach (Bansal & Zahedi, 2015; Dean, 2004), provide an honest and transparent view of the firm's cybersecurity operations to address investor concerns, show good faith in efforts to address cybersecurity weaknesses that may contribute to future breaches (Culnan & Williams, 2009; Wang et al., 2013), inform investors about the firm's skills in managing and uncovering cybersecurity weaknesses (Suchman, 1995), and generally project an image of concern about cybersecurity issues and the acceptance of responsibility for the protection of the public's data.

Because of the public nature of data breaches, investors are often aware of these incidents, which puts pressure on breached firms to address the associated legitimacy gaps. In support of this idea, Swift et al. (2020) found that breached firms produced lengthier cybersecurity disclosures in their 10-Ks following a breach. The evidence is not conclusive, however, as Hilary et al. (2016) found no significant difference in length of cybersecurity disclosures in 10-Ks for breached firms as compared to those of a matched

sample of nonbreached firms. Importantly, our conjecture of increased disclosure following a breach is different than in these prior works, which considered annual 10-K reports. We predict *timely* responses to data breaches via cybersecurity disclosures in 8-Ks, as per the legitimacy theory argument that firms have an incentive to quickly respond to adverse organizational events. That is, because a data breach can introduce investor uncertainty regarding the firm's ability to ward off another cyberattack and more generally address its cybersecurity risks, the firm will feel a sense of urgency to address the uncertainty, which poses an immediate threat to its legitimacy. We therefore predict a different result, as compared to Hilary et al.'s (2016) finding, which focused on the more long-term responses of increased cybersecurity disclosures in 10-Ks.

The question of whether firms respond to data breaches via the more proactive communication efforts that we consider in this study has yet to be tested. Although we later argue that the source of the breach influences firms' disclosure decisions, here, as a baseline to support our legitimacy arguments that firms will generally respond to data breaches in a timely fashion (in the context of 8-Ks) with increased cybersecurity disclosures, we predict:

H1: Data breach announcements are positively associated with cybersecurity disclosures.

3.1 Public Pressure and Cybersecurity Disclosures

Prior authors have espoused that there are likely other factors besides data breaches that affect firms' cybersecurity disclosures (Wang et al, 2013). Likewise, we earlier presented evidence from the voluntary disclosure literature suggesting that forms of external pressure play a role. In H1, we consider a data breach announcement as a form of pressure that drives cybersecurity disclosures, given that these adverse events are likely to produce a legitimacy gap in the minds of investors. We now consider pressure in a more substantive manner, in terms of public attention following a data breach. The context of our study provides a basis for couching public attention as a form of public pressure. That is, because news of a data breach evokes negative reactions (e.g., fear, anger, frustration) from the public (Chatterjee et al., 2019; Gwebu et al., 2018), the public attention surrounding the breach should be primarily negative and thus indicative of the level of public scrutiny surrounding the adverse event.

According to legitimacy theory, firms react to community expectations, and research indicates that public attention following a negative event may prompt an "accept responsibility" response by the affected firms that causes increased disclosures (Bradford & Garrett, 1995; Dean, 2004). The rationale for this is that investors seek information from external sources such as the public in assessing firms' legitimacy (Bansal & Clelland, 2004; Pollock, Rindova, & Maggitti, 2008). It follows that public attention following a data breach, which is indicative of public scrutiny of the event, would help shape investors' (il)legitimacy perceptions of the firm. In this regard, we submit that the level of public attention following a data breach acts as a form of (public) pressure that influences a firm's inclination to disclose cybersecurity information.

The argument that increased public attention regarding an issue of concern will prompt increased organizational disclosures of the issue, which are propelled by legitimacy motives, was made by Wilmhurst and Frost (2000) regarding disclosures of environmental performance in regulatory filings: "if members of the community are becoming more interested in the environmental impact of companies, it is likely that the senior management will be called on to explain the company's activities affecting the environment" (p. 12). Considering these conceptual arguments, along with the previously described literature which indicates that public pressure influences firms' voluntary disclosure practices, we predict:

H2: Public attention following data breach announcements is positively associated with cybersecurity disclosures.

In linking public attention surrounding a data breach to cybersecurity disclosures, it is important to also consider certain characteristics of the breach because we expect these to alter firms' disclosure decisions in the midst of such public pressure. Our contention is that just as investors look to public attention surrounding a data breach in forming their legitimacy perceptions, so too will they consider the public's attribution of blame for the breach.

The proposed saliency of public blame in our study context is rooted in prior research, which indicates that in situations of corporate crisis or an otherwise negative organizational event, the public seeks to identify the cause and assign blame (Folger & Cropanzano, 1998; Weiner, 1985), which influences corporate responses (Ulmer, et al., 2007). Likewise, in the cybersecurity context, the public makes attributions regarding responsibility for a data breach, which influences firms' post-breach communication strategies (Bansal & Zahedi, 2015; Gwebu et al., 2018). When public attention surrounds a data breach, it represents a more pressure-filled situation for the firm, as compared to just the announcement of the breach itself. Public attention means that more eyes are on the firm and thus the legitimacy gap resulting from a data breach is likely to be more salient to investors and may even become wider with increasing public attention. Consequently, the public's assignment of blame for the breach should be

an important factor in firms' cybersecurity disclosure decisions in this context.

In the public's assignment of blame for a data breach, a key distinction is whether the breach originated from within or outside the organization (i.e., "who" is behind the breach). Breaches that originate from within (internal breaches) are likely to be viewed as more avoidable, given the appropriate controls and management oversight, as these breaches often stem from internal process failures (Kwon & Johnson, 2014). Firms should therefore receive substantive blame for these events (Bansal & Zahedi, 2015). An example of an internal breach is when an employee with legitimate access credentials downloads proprietary information and sells it to a competitor. In contrast, breaches from external sources (external breaches) are likely to be viewed as somewhat beyond the firm's control because these incidents are often not firm-specific (e.g., malware that exploits a popular software program) and do not originate within the organization (e.g., system penetrations that are triggered by external hackers), which often makes it difficult to identify their sources (Tan & Yu, 2018). Hence, the public should allow firms some reprieve in terms of blaming them for external breaches (Bansal & Zahedi, 2015).

The literature on corporate impression management provides guidance in terms of how the public's assignment of blame for a data breach influences firms' cybersecurity disclosures. Within this literature are tactics that firms use to address legitimacy concerns in the wake of adverse organizational events (Bolino et al., 2008; Mohamed et al., 1999; Roberts, 2005). One tactic is an assertive communicative strategy, which is used when the firm feels it can rectify the adverse situation and thereby counter the threat to its legitimacy with increased disclosures of relevant information (Roberts, 2005). External breaches fit this context because, as noted, the public is likely to give some reprieve to firms when the breach is external. Hence, firms may feel that because the breach is not considered entirely their fault, a more proactive communicative strategy about cybersecurity is likely to be well received by investors and help address the legitimacy gap. This view aligns with research that shows that a responsibility acceptance strategy is more effective in garnering investors' trust and willingness to invest in a firm after it suffers an external breach, as compared to an internal breach (Tan & Yu, 2018).

For internal breaches, because the public is more likely to attribute blame to the firm for these negative events, the firm may take a more reserved approach in response to public pressure and not be so proactive in disclosing cybersecurity information. The rationale here is that because the firm must overcome a stronger attribution of blame for the event, it has less capacity to restore legitimacy in the minds of investors via a proactive communicative strategy. Further, the public attention surrounding the internal breach already puts the firm in the spotlight, and so there is an incentive to minimize any further investor attention on cybersecurity, given that internal breaches may signify an inability to "keep one's house in order" from a cybersecurity perspective. It is also possible that regardless of the level of public attention the breach receives, the legitimacy gap resulting from an external breach is larger than that for an internal breach because the former is more common and has historically been more publicized (Verizon, 2020). Taking this angle, firms may choose to respond to public pressure by devoting their legitimacy restoration efforts to external breaches because investors are more familiar with these types of breaches. Based on the preceding discussion, we predict:

H3: The relationship between public attention following data breach announcements and cybersecurity disclosures is moderated by breach type, such that the relationship will be stronger (more positive) for external breaches than for internal breaches.

3.2 Institutional Pressure and Cybersecurity Disclosures

Turning to the influence of institutional pressure as it relates to data breaches and cybersecurity disclosures, we earlier presented evidence from the disclosure literature that firms increase their disclosures in response to highly publicized adverse events in their industry. The reasoning for this is that when assessing firms' legitimacy, investors look to the actions of industry peers as an information source (Bansal & Clelland, 2004), which puts (institutional) pressure on focal firms to respond. Accordingly, a plausible legitimacy theory-based argument is that firms increase their cybersecurity disclosures if other firms in their industry suffer a data breach. We submit, however, that this argument is an oversimplification in our study context.

The prior research on disclosure spillovers following adverse events is mainly in contexts where the event threatened the legitimacy of the entire industry (e.g., the BP oil spill in the Gulf of Mexico). In such cases, investors were concerned about the industry's long-term viability following the "crisis" event, which produced an industry-wide legitimacy gap. Such wide-ranging legitimacy concerns are not likely for data breaches, as these events are rarely catastrophic and occur with relative frequency in the modern business environment. While investors recognize the negative consequences of data breaches, an argument can be made that only the breached firm suffers a legitimacy gap, or, if other firms in the industry do suffer a legitimacy gap, it is not as substantial as that due to a true, industry-wide crisis. This aspect of the data breach context lends itself to an

alternative interpretation of how firms' cybersecurity disclosure practices are influenced by the institutional pressure of industry peers' breaches.

Adverse organizational events by other firms in an industry put negative investor attention on the entire industry (Zavyalova et al., 2012). Consequently, and consistent with prior research on corporate wrongdoing (Lange et al., 2011), investors may assume that if one firm in the industry has a data breach, other firms will be experiencing similar cybersecurity problems. Again, we are not proposing that this investor sentiment creates legitimacy gaps for all firms in the industry but that it raises industry-wide cybersecurity risk concerns (i.e., the potential for future breaches for nonbreached firms). However, any such "guilty by association" stigma is likely amplified when firms increase their cybersecurity disclosures following the breaches of industry peers, as this disclosure action may cross the threshold for investor concerns about legitimacy. To counter the negative investor attention and perceptions, firms may feel the need to differentiate themselves from the breached firms in their industry by disclosing *less* cybersecurity information.

To the extent that investors view increased, proactive cybersecurity disclosures following data breaches as firms' attempts to legitimize themselves, and thus admit fault for such incidents, disclosing *less* when industry peers have a breach is a way for firms to signal their innocence and refute investor perceptions that cybersecurity weakness is an industry-wide problem. This strategy aligns with perspectives from the institutional theory literature that argue that firms may choose to distinguish themselves from industry peers by not conforming to institutional environments, as a means of advancing their legitimacy (Deephouse & Suchman, 2008, Oliver, 1991). The strategy also aligns with the burying tactic described in the corporate impression management literature, in which firms use information management strategies that deliberately reduce their positive ties to a negative/unfavorable other in their industry (Bolino et al., 2008; Mohamed et al., 1999). Drawing on these conceptual views, we predict:

H4: Data breaches by industry peers are negatively associated with cybersecurity disclosures.

3.3 Institutional Pressure, Firm Breaches, and Cybersecurity Disclosures

We posit a different set of cybersecurity disclosure practices, which vary by breach type, for firms when they suffer their *own* breaches alongside those of other firms in their industry. As noted, when other firms in an industry suffer data breaches, it is expected that negative investor attention will be drawn to the entire industry. In addition, if a firm suffers its own breach, it must contend with the legitimacy concerns that arise from being a breach victim. We submit that the increased negative investor attention on the industry acts as a catalyst for breached firms to address their legitimacy concerns via proactive cybersecurity disclosures, as opposed to disclosing less when only industry peers suffer breaches, because, in such cases, there is little or no legitimacy gap to address. However, as with our arguments regarding public pressure, we contend that breached firms will only address their legitimacy concerns when experiencing an external breach. That is, because firms are less at fault for external breaches (as compared to internal breaches) and responsibility acceptance can help with legitimacy concerns, firms may feel more compelled to respond to external breaches with increased cybersecurity disclosures, particularly in the wake of increased industry-wide investor attention. In sum, firms will likely disclose less cybersecurity information to differentiate themselves in response to the institutional pressure of peer breaches in general, but if they also experience their own external breaches, disclosing more will be in their favor from a legitimacy perspective.

When experiencing an internal breach, the increased investor attention (from peer breaches) and the firm's own legitimacy concerns arising from the internal breach provide some impetus for proactive cybersecurity disclosures. Yet it also makes sense that firms will be reluctant to draw any additional investor attention given their own inability to "keep their house in order" based on their internal breach. Further, and as argued previously, firms should be less likely to address legitimacy concerns pursuant to internal breaches because of the stronger attribution of blame for these events, which makes legitimacy restoration more difficult. The specific context where other firms in the industry also suffer a breach facilitates a strategy of refraining from cybersecurity disclosure following an internal breach. Prior research on corporate wrongdoing indicates that in some instances where other organizations engage in similar negative events, investor attention can wane from one particular organization and the focal organization can experience a safety-in-numbers effect (Zavyalova et al., 2012). In a similar vein, firms who experience an internal breach can use the breaches of industry peers as a shield and thereby justify a decision to refrain from proactively disclosing cybersecurity information. This strategy is particularly suited for internal breaches, where the firm has less capacity to achieve legitimacy restoration via proactive communicative efforts about cybersecurity. Moreover, as internal breaches are often less publicized and lesser known among many investors, the safety-in-numbers strategy, where firms retreat from proactive cybersecurity disclosures, fits this context. Accordingly, we predict:

H5: The relationship between data breaches by industry peers and cybersecurity disclosures is moderated by the breach type of the focal firm, such that the relationship will be stronger (more positive) when the focal firm has an external breach as compared to an internal breach.

4 Methodology

4.1 Sample and Data Construction

To test our hypotheses, we constructed a panel dataset from publicly available sources. First, we searched for data breaches during the period 2005-2018 using the Privacy Rights Clearinghouse (PRC) website (privacyrights.org). The PRC website provides a listing of public data breach announcements, with its information sourced from government agencies (e.g., notification documents from state governments) and various media outlets (e.g., news feeds, blogs, websites). We found nearly 9000 breach announcements for the time frame of our study, which encompassed a variety of breach types (e.g., hacks, unintended disclosure, insider). We included all breach types but only the breaches of publicly traded firms because of the nature of our study (i.e., cybersecurity disclosures in 8-K reports filed with the SEC). Our final breach sample consisted of 678 breach announcements across 381 different firms. Of note is that if a firm had more than one breach in a single year, we used only the first breach in our sample.[5]

Regarding the panel structure of our dataset, for each firm year, we created a *Breach* dummy variable, which was coded as "1" if the firm experienced a breach in that year and "0" otherwise. We also created a *PeerBreach* variable for purposes of testing H4 and H5. Following prior operationalizations of corporate wrongdoing by industry peers (Zavyalova et al., 2012), and cybersecurity disclosure literature that segments industries based on two-digit SIC codes (Gordon et al., 2010; Hilary et al., 2016), we measured *PeerBreach* as the sum of data breaches by other firms in the same two-digit SIC code in a given year, excluding the focal firm's breaches. To test H2 and H5, we had to distinguish between internal and external breaches. To do so, we manually coded each of the 678 breaches based on the breach descriptions provided on the PRC website. We followed the criteria of Kwon and Johnson (2014, 2018) in categorizing the breaches as internal or external based on certain keywords in the breach descriptions. For example, if a breach description included "hacker" it was typically coded as *External*, whereas for the *Internal* coding, the description typically included words such as "accidental exposure" or "disgruntled employee." Following Kwon and Johnson (2014), our coding of internal breaches includes a breach maliciously or accidentally occurring within the organization, as we deem both instances as drawing public attributions of blame on the firm due to internal process failures. Any debatable cases were further reviewed by the authors until a consensus coding was achieved. The resultant breakdown was 372 internal and 306 external breaches.

The second source of data consisted of cybersecurity disclosures in 8-Ks obtained from the Edgar database (sec.gov/edgar.shtml) between 2005 and 2018 for the firms in our breach sample. We first had to manually obtain the Central Index Key (CIK) for each breached firm, so it could be matched to the Edgar database (and later to our other data sources). We then used a Ruby script to scrape any 8-K during 2005-2018 for our selected firms that contained one or more of the cybersecurity keywords listed in Table 2. The keywords are similar to those used in prior cybersecurity disclosure studies (Gordon et al., 2010; Li et al., 2018; Wang et al., 2013). This process resulted in 5518 unique 8-K reports. Next, one of the authors manually examined each 8-K to ensure that it was accurately identified as a cybersecurity disclosure. For example, in some cases, the word "virus" pertained to a non-computer virus. There were also instances where an identified keyword was not in relation to a true cybersecurity disclosure (e.g., a company description mentions being an identity theft service provider, but there was otherwise no cybersecurity-related information disclosed). After removing the cases where a keyword or the associated content was not part of a cybersecurity disclosure, we had 5227 unique 8-K reports.

Using these 8-Ks reports, we constructed a measure of cybersecurity disclosure for use as our dependent variable: *DiscWord*, which is the total number of cybersecurity-related words (i.e., our keywords) aggregated across a firm's 8-Ks in a given year. Utilizing the number of cybersecurity-related words as a disclosure measure is consistent with prior cybersecurity disclosure studies that focus on the length of disclosure (Hilary et al., 2016; Li et al., 2018). Likewise, disclosure studies in accounting and other disciplines have used the number of related words as proxies for the extent of disclosure (e.g., He & Plumlee, 2020; Islam & Deegan, 2010). The coding of the 8-Ks resulted in *DiscWord* values in 1560 firm years. The third source of data was internet search activity, using data collected from Google Trends, for our measure of public attention. Google Trends provides access to historical Google search activity with the data being normalized (scale of 0 to 100 for a particular search term) to account for total search activity based on when and where a search took place. The results provide an indicator of how popular a particular search term was at a specified point in time.

[5] There were 75 firm years out of the total 4785 in our dataset, or 1.56% that had more than one breach. We reran our models with a control variable to indicate whether the firm had multiple breaches in a year and the results were qualitatively similar to our main results.

Table 2. Cybersecurity Keywords Searched (# of Instances in Parentheses)

Security breach (2301)	Network security (230)	Data theft (26)
Virus (1180)	Denial of service (220)	Computer security (21)
Cybersecurity* (1134)	Data breach (219)	Information risk (20)
Information security (763)	Malware (194)	Phishing (20)
Cyberattack* (678)	Encryption (145)	InfoSec (5)
Intrusion (377)	Hacker (140)	Cyberfraud* (1)
Security measure (305)	Worm (132)	Information systems security (1)
Security incident (286)	Access control (75)	Security expenditure
Identity theft (272)	Security monitoring (40)	Computer system security
Computer virus (237)	Security management (29)	Computer breach
*Represent wild card searches (e.g., both "cyber security" and cybersecurity" were used).		

According to previous empirical research, internet searches provide valid indicators of public attention (e.g., Da et al., 2011; Ripberger, 2011). In particular, Ripberger (2011) found strong convergent validity between Google search volume and traditional media-based measures of public attention (e.g., articles in major newspapers) based on the logic that internet searches encompass individuals' thought, willingness, and effort to search particular topics. Prior research has also used Google search volume as a gauge for public interest in cybersecurity and data breaches (Hilary et al., 2016).

For each of the 678 breaches in our sample, we collected daily search volume on the breached firm for a period preceding and following the breach announcement. To construct our measure of public attention (*PubAtt*), we developed a baseline level of Google search volume activity for each firm by using its daily search volume for the 90 days prior to the breach announcement. This approach resembles that used in stock market-based event studies that first develop an estimation period prior to the event as a means to ascertain abnormal returns (Brown & Warner, 1985). We then took the average Google search volume for the period from the day of the breach announcement to three days after (i.e., [0,3] "event window") and subtracted that value from the baseline value. Hence, our measure of public attention is the deviation from the norm for Google search activity around the breach announcement. We selected the four-day event window to avoid the confounding influences of extraneous events, which become more likely as the event window increases (Brown & Warner, 1985). At the same time, we wanted to allow sufficient time for the breach announcements to be received, understood, and acted upon by the public. Stock market-based event studies of IT phenomena have similarly used four-day event windows based on the reasoning that stock prices need time to adjust to the event (Goldstein et al., 2011; Konchitchki & O'Leary, 2011).

We collected data on several other variables to use as controls in our analyses in line with prior voluntary disclosure studies in cybersecurity and other contexts (Amir et al., 2018; Gordon et al., 2010; He & Plumlee, 2020; Hilary et al., 2016; Lang & Lundholm, 1993; Li et al., 2018; Wang et al., 2013). Specifically, for each firm year we controlled for firm size via its total assets (natural log-transformed to control for skew) (*Assets*), number of employees (*Employees*), and capital expenditures (*CapEx*). We also controlled for firm financial condition using return on assets (*ROA*), an indicator of whether the firm suffers negative earnings for the year (*Loss*), and its financial leverage ratio (*Leverage*). Additionally, we included a control variable for the number of analysts following the firm per year (*Analysts*).

The combination of variables for firm size and analysts following the firm controlled for the visibility of the firm (Li et al., 2018). In this way, we address a potential endogeneity concern regarding the omission of public visibility in our study. The issue is that a firm's level of public visibility may simultaneously affect the level of public attention that it receives from a data breach and its likelihood of cybersecurity disclosure, which could bias our results. Our control variables therefore address this concern.

Additionally, to control for prior cybersecurity disclosures in our analyses, we constructed a lagged-year measure of our *DiscWord* dependent variable. This measure (*PrDiscWord)* is the total number of cybersecurity-related words across a firm's 8-Ks in year *t*-1. Including this lagged variable as a control helped isolate our hypothesized influences of public and institutional pressure on cybersecurity disclosures, beyond that of prior disclosure tendencies.

Finally, we controlled for unobserved time-invariant industry effects by including industry sector dummies based on two-digit SIC codes (Gordon et al., 2010; Hilary et al., 2016) and controlled for temporal effects by including year dummy variables. Regarding industry influences, certain industries are more cybersecurity sensitive and, therefore, firms in these industries could be more likely to detect a breach and/or disclose cybersecurity information. Additionally, research indicates that certain industries are differentially prone to data breaches and that breach severity varies by industry (Ayyagari, 2012; Sen & Borle, 2015). Our industry dummies controlled for these factors, which presumably did not change from year to year. The year dummies controlled for

time trends in our data and any shocks that could affect a firm in a given year, such as the influence of a prominent data breach, trends in the progression of breaches, or advances in IT infrastructures that could assist in detecting cybersecurity incidents and weaknesses.

Upon the removal of firm years in which firms were not publicly traded or data was otherwise missing from at least one of our data sources, we ended up with an unbalanced panel dataset consisting of 4785 observations with complete data for our models. Appendix B provides a summary of our study variables, including their operational definitions and data sources. Table 3 provides the correlations among the study variables and their descriptive statistics.

4.2 Main Results

We estimated the relationships specified by our hypotheses using ordinary least squares (OLS) regression models with robust standard errors clustered by firm. The results of the OLS regressions are presented in Table 4, with *DiscWord* serving as the dependent variable in each model. We first assessed the variance inflation factor (VIF) of our covariates to ensure that multicollinearity was not an issue for our models. We found an average VIF of 1.30 across all models and the highest VIF score for any variable was 2.01. Both VIF results are below the recommended threshold of 10 and the more restrictive threshold of 3.3.

Regarding the hypotheses testing, H1 states that data breach announcements are positively associated with cybersecurity disclosures. As shown by the significant coefficient on *Breach* in the Model 1 results ($\beta = 0.638$, $p < 0.001$), this hypothesis is supported. H2 states that public attention following data breach announcements is positively associated with cybersecurity disclosures. Recall that our measure of public attention is abnormal search volume on the name of the company/firm following the announcement of its data breach. Hence, in order to test H2, we considered only firm years in which there was a breach. Using this subset of the data, as shown in the results for Model 2, *PubAtt* is positively and significantly associated with *DiscWord* ($\beta = 0.058$, $p < 0.05$); thus, H2 is supported.

H3 states that the relationship between public attention and cybersecurity disclosures is stronger (more positive) for external breaches than for internal breaches. To test H3, we created subsets of the data consisting of firm years with external breaches ($N = 306$) and firm years with internal breaches ($N = 372$). As shown in the Model 3 and 4 results, *PubAtt* is positive and significant in the external subset ($\beta = 0.095$, $p < 0.01$) but nonsignificant in the internal subset. The statistical result for the equality of the *PubAtt* coefficients in Models 3 and 4 is significant ($z = 1.71$, $p < 0.05$, one-sided test) (see Paternoster et al., 1998 for the formula). Hence, beyond eyeballing the coefficient values, there is evidence that the relationship between *PubAtt* and *DiscWords* is significantly stronger in the external breach subset, thus supporting H3.[6]

Table 3. Variable Correlations and Descriptive Statistics

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. DiscWord	1.00													
2. PrDiscWord	**0.61**	1.00												
3. Breach	**0.04**	-0.00	1.00											
4. Internal	0.02	-0.01	**0.76**	1.00										
5. External	**0.04**	0.01	**0.58**	**-0.07**	1.00									
6. PeerBreach	**0.03**	**0.04**	**0.07**	**0.05**	**0.05**	1.00								
7. PubAtt	**0.06**	0.01	**0.16**	**0.09**	**0.14**	**0.04**	1.00							
8. Assets	**0.09**	**0.09**	**0.11**	**0.09**	**0.06**	-0.00	0.02	1.00						
9. Employees	0.02	0.02	0.02	0.00	0.02	**-0.04**	-0.00	**0.09**	1.00					
10. CapEx	-0.00	0.01	**0.07**	**0.06**	**0.03**	**-0.10**	-0.00	**0.34**	**0.08**	1.00				
11. ROA	-0.01	-0.01	**0.03**	0.02	0.02	0.01	-0.00	-0.02	0.02	0.01	1.00			
12. Loss	-0.01	-0.00	-0.02	-0.02	-0.00	**-0.04**	-0.01	**-0.18**	**-0.04**	**-0.09**	**-0.25**	1.00		
13. Leverage	-0.01	-0.02	0.01	0.01	-0.00	-0.10	-0.01	0.02	0.00	0.00	-0.01	0.02	1.00	
14. Analysts	**0.10**	**0.09**	**0.10**	**0.07**	**0.07**	-0.01	**0.03**	**0.40**	**0.06**	**0.20**	**0.10**	**-0.16**	0.00	1.00
Mean	1.99	1.66	0.14	0.09	0.05	3.01	0.26	3.99	84.11	1032	0.05	0.16	0.82	14.31
Std. deviation	5.44	4.83	0.35	0.28	0.22	3.68	3.93	0.93	611.6	2955	0.27	0.37	19.61	8.71
Min	0	0	0	0	0	0	-22.27	0.23	0.05	-582	-4.70	0	-776.6	1
Max	105	89	1	1	1	19	61.57	7.01	28500	36108	7.70	1	324.9	54.67

Note: Bold represents statistically significant correlation coefficients at the $p < 0.05$ level.

[6] We also found support for H3 using a dummy variable approach. Specifically, we ran Model 2 with the interaction term *PubAtt*External* included, and its coefficient was positive and significant ($\beta = 0.082$, $p < 0.001$), whereas a separate Model 2 run with *PubAtt*Internal* included showed its coefficient to be nonsignificant ($\beta = 0.034$, n.s.).

Table 4. OLS Regressions of Cybersecurity Disclosures (DiscWord)

	(1) Model 1	(2) Model 2	(3) Model 3 (external)	(4) Model 4 (internal)	(5) Model 5	(6) Model 6
PrDiscWord	0.648*** (0.030)	0.805*** (0.055)	0.770*** (0.088)	0.775*** (0.071)	0.629*** (0.031)	0.647*** (0.006)
Breach	0.638** (0.204)					
PubAtt		0.058* (0.023)	0.095** (0.030)	0.035 (0.028)		
PeerBreach					-0.080* (0.035)	-0.076* (0.034)
PeerBreach*External						0.134* (0.058)
Assets	0.183† (0.096)	0.393 (0.273)	0.508 (0.396)	0.587 (0.418)	0.128 (0.095)	0.193* (0.098)
Employees	0.000 (0.000)	0.000 (0.000)	0.000 (0.000)	0.001 (0.001)	0.000 (0.000)	0.000 (0.000)
CapEx	-0.000* (0.000)	-0.000 (0.000)	-0.000 (0.000)	-0.000 (0.000)	-0.000 (0.000)	-0.000* (0.000)
ROA	-0.110 (0.101)	-0.077 (0.157)	0.370* (0.161)	-0.282 (0.290)	-0.063 (0.126)	-0.094 (0.099)
Loss	0.070 (0.162)	0.287 (0.560)	-1.181 (1.023)	0.595 (0.743)	0.028 (0.182)	0.077 (0.162)
Leverage	0.003 (0.002)	-0.007 (0.024)	-0.000 (0.038)	-0.011 (0.023)	0.003 (0.002)	0.003 (0.002)
Analysts	0.014 (0.0011)	0.006 (0.018)	-0.030 (0.031)	0.014 (0.030)	0.015 (0.014)	0.014 (0.012)
Constant	-0.348 (0.338)	-1.589 (1.457)	-4.834* (2.149)	-2.108 (1.887)	-0.238 (0.377)	-1.004** (0.293)
Industry dummies	Yes	Yes	Yes	Yes	Yes	Yes
Year dummies	Yes	Yes	Yes	Yes	Yes	Yes
Observations	4785	678	306	372	4107	4785
R-squared	0.415	0.475	0.577	0.504	0.412	0.420

Note: Standard errors (in parentheses) are clustered at the firm level; † $p < 0.10$, *$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

H4 states that data breaches by industry peers are negatively associated with cybersecurity disclosures. This hypothesis considers industry peers having breaches when the focal firm does not. Hence, to test the hypothesis, we included only firm years in which focal firms did not have breaches to avoid the potential confounding influences of a firm's own breach on the relationship between peer breaches and cybersecurity disclosures. As shown by the significant negative coefficient on *PeerBreach* in the Model 5 results (β = -0.080, $p < 0.05$), H4 is supported.[7]

H5 states that the relationship between data breaches by industry peers and cybersecurity disclosures is stronger (more positive) when the focal firm has an external breach, as compared to when it has an internal breach. Because this hypothesis considers when the focal firm has a breach alongside those of its industry peers, we included the full sample for its testing. Also, unlike for H3 where we split the data into external and internal breach subsamples for focal firms, we could not use this approach to test H5 because it would have excluded many firm years in which industry peers had breaches but focal firms did not. Hence, we created a variable for the interaction of peer breaches and external breaches (by the focal firm) and included that in the regression. As shown in the positive and significant coefficient on *PeerBreach*External* in the Model 6 results (β = 0.134, $p < 0.05$), H5 is supported. The interpretation of this coefficient is that there is a positive effect of *PeerBreach* when the focal firm has an external breach. Alternatively, we tested the same model (not shown) with the interaction of *PeerBreach* and *Internal*, and the interaction coefficient was not significant, which also supports H5.

4.3 Robustness Checks and Additional Analyses

Since our dependent variable is a count variable, we ran negative binominal regressions as an alternative empirical estimation to ensure the robustness of our

[7] We also ran a model with the full dataset (N = 4785) and included *Breach* as a control variable, to control for focal firm breaches. The results for *PeerBreach* were unchanged in terms of sign and significance level.

results. The rationale is that OLS regression may produce biased results when the dependent variable is a count measure and when the count measure has a substantially larger variance than its mean (Blevins et al., 2015; Long & Freese, 2001). This latter issue is called overdispersion. We statistically confirmed the overdispersion in our data by conducting likelihood ratio tests (G^2 values for our models each significant at $p < 0.001$). Negative binomial regression is an appropriate alternative to OLS under these conditions (Blevins et al., 2015). As seen in the Model 1 through 6 results in Table 5, the negative binominal regression results are largely consistent with those of the OLS regressions in Table 4, and thus continue to support our hypotheses.

We conducted additional analyses to address alternative explanations for our findings. One concern was that our measure of public attention could be a proxy for severity of breach or that severity of breach was an omitted variable that could have had an endogenous effect on our results. To address this issue, as described in Appendix C, we applied three different measures of breach severity as control variables in a series of OLS regressions that tested H1 and H2. As shown in Columns 1 through 6 of Table C1, the hypothesized influences of *Breach* and *PubAtt*, respectively, remain significant after controlling for each of the severity measures.

Another concern was the potentiality of unobserved factors that simultaneously affect both the likelihood of a firm suffering a breach and its cybersecurity disclosures, which could have biased our baseline results for H1 (and perhaps indirectly those of H2 and H3). In other words, *Breach* may be an endogenous variable in our study. One way to address this issue is to run a two-stage least squares (2SLS) regression with instrumental variables (IVs). As described in Appendix C, we conducted two IV analyses to address the endogeneity associated with *Breach*—one with *CapEx* as the IV and the other with Lewbel's (2012) technique for constructing IVs based on existing variables. The second stage 2SLS results for both analyses (see Columns 7 and 8 of Table C1) show that the *Breach* coefficient remained positive and significant, thereby helping to alleviate the endogeneity concern surrounding *Breach*.

Table 5. Negative Binomial Regressions of Cybersecurity Disclosures (DiscWord)

	(1) Model 1	(2) Model 2	(3) Model 3 (External)	(4) Model 4 (Internal)	(5) Model 5	(6) Model 6
PrDiscWord	0.054*** (0.006)	0.117*** (0.009)	0.100*** (0.019)	0.117*** (0.011)	0.129*** (0.013)	0.054*** (0.006)
Breach	0.258** (0.083)					
PubAtt		0.016* (0.006)	0.023** (0.007)	0.014 (0.009)		
PeerBreach					-0.040* (0.020)	0.012 (0.015)
PeerBreach*External						0.062*** (0.017)
Assets	0.131† (0.076)	0.266* (0.118)	0.384* (0.156)	0.262 (0.186)	0.126 (0.093)	0.134† (0.077)
Employees	0.000* (0.000)	0.000* (0.000)	0.000 (0.000)	0.000 (0.001)	0.000 (0.000)	0.000* (0.000)
CapEx	-0.000† (0.000)	-0.000 (0.000)	-0.000 (0.000)	-0.000 (0.000)	-0.000 (0.000)	-0.000 (0.000)
ROA	-0.223 (0.177)	-1.698** (0.646)	-0.063 (0.240)	-2.829** (0.959)	-0.464 (0.409)	-0.216 (0.175)
Loss	0.175† (0.090)	0.102 (0.218)	-0.162 (0.301)	0.202 (0.329)	0.112 (0.125)	0.181* (0.091)
Leverage	0.000 (0.000)	0.019** (0.006)	0.026** (0.010)	0.006 (0.009)	0.000 (0.000)	0.000 (0.000)
Analysts	0.010† (0.005)	0.014 (0.009)	-0.014 (0.013)	0.016 (0.014)	0.016* (0.007)	0.011* (0.005)
Constant	-0.999** (0.294)	-1.209** (0.388)	0.488 (0.521)	-0.928* (0.449)	-0.916** (0.301)	-1.004** (0.293)
Industry dummies	Yes	Yes	Yes	Yes	Yes	Yes
Year dummies	Yes	Yes	Yes	Yes	Yes	Yes
Observations	4785	678	306	372	4107	4785
Log pseudolikelihood	-6580.75	-1017.31	-399.99	-558.57	-5537.13	-6578.32

Note: Standard errors (in parentheses) are clustered at the firm level; † $p < 0.10$, *$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

Table 6. OLS Regressions of Cybersecurity Disclosures (DiscWord) Split by Pre- and Post-SEC Disclosure Guidance Period

	Model 1		Model 2		Model 3		Model 4		Model 5		Model 6	
	(1) Pre-	(2) Post-	(3) Pre-	(4) Post-	(5) Pre- (external)	(6) Post- (external)	(7) Pre- (internal)	(8) Post- (internal)	(9) Pre-	(10) Post-	(11) Pre-	(12) Post-
PrDiscWord	0.683***	0.627***	0.859***	0.723***	0.901***	0.632**	0.806***	0.680***	0.591***	0.614***	0.687***	0.625***
	(0.089)	(0.031)	(0.067)	(0.084)	(0.141)	(0.209)	(0.086)	(0.179)	(0.023)	(0.021)	(0.089)	(0.031)
Breach	0.691**	0.667*										
	(0.225)	(0.295)										
PubAtt			0.040	0.080**	0.068	0.095**	0.028	0.062				
			(0.044)	(0.025)	(0.101)	(0.031)	(0.037)	(0.056)				
PeerBreach									-0.003	-0.093	-0.009	-0.114†
									(0.028)	(0.065)	(0.031)	(0.068)
PeerBreach* external											0.091	0.153*
											(0.112)	(0.073)
Assets	0.202*	0.139	0.413	0.203	0.660	0.543	0.553	0.518	0.120	0.126	0.217**	0.144
	(0.084)	(0.159)	(0.353)	(0.439)	(0.684)	(0.656)	(0.458)	(0.825)	(0.074)	(0.193)	(0.087)	(0.160)
Employees	0.000*	-2.660	-0.000	0.000	0.005	0.000*	0.001	0.000	0.000**	-0.000	0.000**	-7.662
	(0.000)	(0.000)	(0.000)	(0.001)	(0.007)	(0.000)	(0.001)	(0.002)	(0.000)	(0.000)	(0.000)	(0.000)
CapEx	-0.000	-0.000*	-0.000	-0.000	-0.001	-0.000	-0.000	-0.000	1.170	-0.000	-0.000	-0.000*
	(0.000)	(0.000)	(0.000)	(0.000)	(0.001)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
ROA	-0.032	-0.353	-0.565	-0.624	0.369	1.137	-0.289	-2.414	0.057	-0.419	-0.027	-0.300
	(0.055)	(0.542)	(0.159)	(1.555)	(0.264)	(2.674)	(0.302)	(2.189)	(0.165)	(0.970)	(0.053)	(0.538)
Loss	0.052	0.051	-0.174	0.087	-2.826†	-1.252	-0.010	1.505	0.111	-0.042	0.057	0.056
	(0.144)	(0.281)	(0.673)	(1.101)	(1.681)	(1.466)	(0.873)	(2.048)	(0.147)	(0.384)	(0.144)	(0.280)
Leverage	0.004	0.002	0.013	-0.062†	0.005	-0.117	0.002	-0.030	0.002	0.004	0.004	0.002
	(0.005)	(0.002)	(0.017)	(0.034)	(0.042)	(0.139)	(0.018)	(0.032)	(0.003)	(0.005)	(0.005)	(0.002)
Analysts	0.002	0.024	0.015	-0.003	0.020	0.038	0.026	0.001	-0.001	0.028†	0.003	0.023
	(0.007)	(0.020)	(0.026)	(0.028)	(0.079)	(0.034)	(0.030)	(0.061)	(0.008)	(0.016)	(0.007)	(0.020)
Constant	-0.723*	-0.651	-1.558	-1.490*	-3.001	-4.801†	-2.223	-0.170	-0.447	-0.390	-0.754**	-0.490
	(0.301)	(0.580)	(1.698)	(1.863)	(2.040)	(2.521)	(2.192)	(3.046)	(0.943)	(2.205)	(0.310)	(0.620)
Industry dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	2374	2411	349	329	132	174	221	151	2025	2082	2374	2411
R-squared	0.369	0.404	0.492	0.502	0.593	0.606	0.535	0.523	0.320	0.406	0.365	0.405

Note: Standard errors (in parentheses) are clustered at the firm level; † $p < 0.10$, *p < 0.05, **p < 0.01, ***p < 0.001

Finally, we conducted additional analyses to explore our hypotheses in light of the 2011 SEC cybersecurity disclosure guidance. Again, while not a formal regulation, this SEC guidance put pressure on firms to increase their cybersecurity disclosures. Evidence shows that firms responded with increased cybersecurity disclosures in 10-Ks after 2011 (Hilary et al., 2016; Li et al., 2018), although there was substantial variation in terms of which firms disclosed and how much. We likewise found a general increase in cybersecurity disclosures in our 8-K data after 2011,[8] as well as variation in the frequency and volume of these disclosures among the firms in our dataset. Focusing on our research question, of interest is whether our public and institutional pressure factors are robust to the 2011 SEC guidance or perhaps become less salient with the increased regulatory pressure to disclose. To explore this, we partitioned the dataset into two periods: a pre-guidance period, which includes firm-year data through 2011; and a post guidance period, which includes firm-year data after 2011 (i.e., 2012-2018). We reran the models from our main analysis for both periods and the results are shown in Table 6.

We acknowledge that several of these results should be interpreted with caution, given the diminished sample sizes due to the partitioning of the data. However, in general, the results in Table 6 support our hypothesized influences of public and institutional pressure in the post-guidance period, thereby suggesting that these forms of pressure exist beyond the influence of regulatory pressure. Interestingly, the results show that public and institutional pressure are even stronger influences on cybersecurity disclosures in the post-guidance period, as compared to the pre-guidance period, and especially when the firm has its own external breach. We also note that while the hypothesized

[8] The number of 8-Ks in our dataset with cybersecurity-related content per year is: 2005—89; 2006—101; 2007—143; 2008—169; 2009—200; 2010—223; 2011—310; 2012—102; 2013—485; 2014—595; 2015—783; 2016—809; 2017—438; 2018—780.

negative influence of *PeerBreach* on cybersecurity disclosures is not supported in the post-guidance period in the model in Column 10 (p = 0.16), it is supported when the interaction of *PeerBreach* and *External* is added to the model (Column 12).

5 Discussion, Implications, and Limitations

Regulatory filings with the SEC provide a means for publicly traded firms to communicate to investors about cybersecurity, on issues such as how the firm is preventing, detecting, and correcting data breaches, the costs of such efforts, current and future cybersecurity risks, and cybersecurity risk management efforts. Firms have traditionally chosen to communicate such information on a quarterly or annual basis, if at all. However, there has been a recent regulatory push for firms to provide timelier cybersecurity disclosures, which prompted our focus on cybersecurity disclosures in 8-Ks. Given the discretion afforded firms in terms of whether, what, and how much information to disclose, even in the wake of regulatory pressure, we focused on public and institutional pressure as two alternate drivers of timely cybersecurity disclosures.

We first considered the occurrence of a data breach as a baseline form of pressure that prompts timely cybersecurity disclosures, based on the legitimacy theory view that firms will respond to the breach swiftly as means to address the resultant legitimacy gap. Consistent with our prediction, we found that breaches were associated with increased cybersecurity disclosures in terms of the number of cybersecurity-related words in 8-Ks. This finding aligns with prior work which found that firms significantly increased cybersecurity disclosures after a data breach announcement (Swift et al., 2020). However, in that extant work, the disclosures were captured using annual 10-K reports, which is a longer-term response. Our results show that breached firms also react more quickly, in terms of 8-Ks, and thus engage in timely cybersecurity disclosures as prompted by the breach incident.

Next, we explored public pressure as a driver of firms' timely cybersecurity disclosures. Our results suggest that public attention surrounding a data breach announcement, in terms of internet search activity, prompts firms to react by disclosing more cybersecurity information to investors. This is a key finding because it suggests that public scrutiny surrounding the incident provides a form of pressure that drives firms to respond, presumably in an attempt to address the legitimacy gap created by the breach. Hence, the firm is responding to public pressure, which one might argue is not a completely rational response for the firm (or at least not completely market-driven), in terms of the cybersecurity information it chooses to disclose to investors. Also, because cybersecurity disclosures influence investors' valuation of the firm (Gordon et al., 2010; Wang et al., 2013), an extension of our finding is that public pressure surrounding a data breach ultimately influences the overall market value of the firm. More broadly, the finding speaks to the growing importance of public discourse in shaping firm actions and how firms chose to communicate with their stakeholders. Outside the cybersecurity context, there are numerous examples of how firms have chosen to act or react, not based solely on market forces but based on public sentiment regarding topics of importance (e.g., Walmart's decision to raise wages for its employees[9]). Our results point to a similar phenomenon when it comes to firms' decisions to provide timely cybersecurity disclosures in SEC filings.

Also important is that we found the influence of public pressure to be stronger when it is due to an external breach, as compared to that for an internal breach. This finding aligns with our theoretical position that the public ascribes less blame to the firm for external breaches and therefore the firm feels confident in its ability to address investors' legitimacy concerns through increased cybersecurity disclosures following these breaches. Crucially, we found that this result holds in the post-2011 SEC disclosure guidance period, which suggests that the influence of public pressure from external breaches is beyond that of regulatory pressure to disclose. By contrast, we did not find increased cybersecurity disclosures when the public pressure was due to an internal breach. This result is consistent with our reasoning that the public ascribes more blame to firms for internal breaches and that firms thus feel less confident in their abilities to address investors' legitimacy concerns when subject to this form of public pressure. Collectively, the findings point to the pivotal role of attributions of blame for a breach, as per the breach source, in determining how the firm reacts to the resultant public pressure. The findings thereby shed light on the variance in firms' cybersecurity disclosure practices.

As another source of this variation, we focused on institutional pressure, in the form of breaches incurred by other firms in the same industry, as a driver of firms' cybersecurity disclosures. Counter to the conventional reasoning that firms increase their disclosures following an adverse event in their industry, we found important nuance in our context of timely cybersecurity disclosures. Specifically, our results suggest that firms disclose *less* cybersecurity information when others in

[9] https://www.cnbc.com/2017/04/20/wal-mart-still-front-and-center-of-debate-over-minimum-wages.html

their industry suffer breaches. This finding supports the notion that firms try to distinguish themselves from their breached peers in situations when they do not suffer their own breaches as a way to counter investors' "guilty by association" perception in terms of cybersecurity being an industry-wide problem. However, in situations when a focal firm suffers its own external breach alongside breaches of its industry peers, the institutional pressure appears to serve as a catalyst for increased cybersecurity disclosure by the focal firm. As with our results for the influence of public pressure following an external breach, the results for the influence of institutional pressure when the focal firm suffers an external breach also hold in the post-2011 SEC disclosure guidance period, thereby suggesting that the influence of institutional pressure exists beyond that of regulatory pressure. Alternatively, when a focal firm suffers its own internal breach alongside breaches of its industry peers, the firm appears to adopt a safety-in-numbers mentality and use breaches of industry peers as a shield, resulting in less disclosed cybersecurity information. We attribute this approach to the firm trying to deflect investor attention away from its own internal process failures in the wake of industry-wide attention resulting from breaches of industry peers. Together, these findings provide fresh insight into how a firm's institutional environment manifests itself in terms of influencing cybersecurity disclosure practices.

From a theoretical perspective, our work supports a nuanced and contextualized version of legitimacy theory in the cybersecurity disclosure context. Unlike applications of legitimacy theory in other contexts, which assume that firms will generally seek to address legitimacy concerns following an adverse event, we theorize on and find evidence for the idea that firms are selective in their efforts to address legitimacy concerns amid public and institutional pressure and do so based on their presumed degree of blame for the breach event. We use external and internal breaches to instantiate the blame concept, but our enhanced legitimacy theory can be more generally extended to other contexts where stakeholders are likely to vary in their attributions of blame for adverse organizational events.

We also contribute to the normative discussion regarding firms' responsibilities toward improved cybersecurity because of the costs that data breaches impose on the economy and society as a whole. A central theme within this discussion is that firms should be more aggressive in releasing cybersecurity information than required by law (Culnan & Williams, 2009; Matwyshyn, 2009). Although our context is cybersecurity communications to investors, in a more general sense, our finding that public pressure is a conduit to increased disclosures indicates that the public acts as a "moral authority" that helps guide firms toward proactive cybersecurity disclosures in the wake of a data breach.

Our results also have implications for investors and other stakeholders who are clamoring for increased cybersecurity information from firms. Foremost is the concern that at least some of the cybersecurity information disclosed in 8-Ks may be "lip service," or perhaps not completely objective, and provided in an overzealous manner in response to public and institutional pressure. In such cases, the disclosed information may not reflect the firm's true commitment to cybersecurity or its cybersecurity capabilities. Our study did not ascertain disclosure motives, but the results do point to public and institutional pressure as external forces that act upon firms' cybersecurity disclosure decisions. As investors and other market participants use disclosed cybersecurity information to help value the firm, it is important that these constituents understand that our forms of external pressure may be driving such disclosures and consider them in their valuations. Similarly, these stakeholders should understand that cybersecurity information is less likely to be disclosed after an internal breach, even when the firm experiences public and institutional pressure. The evidence that firms hold back on timely cybersecurity disclosures following an internal breach is problematic in the sense that these incidents are oftentimes more costly than external breaches; hence, insofar as some of the disclosed information following a breach would relate to the breach itself (i.e., updates on financial costs, legal proceedings, and other findings related to the breach), limiting such information could lead to inaccurate estimates of the firm's value and its likelihood of sustaining a similar future breach.

From a policy perspective, regulators have been pushing firms to disclose more cybersecurity information and to do so on a timely basis (SEC, 2011; 2018). Firms have often countered that they are not obligated to report such information because it is not material information to investors. Our results point to levers that can be used to encourage cybersecurity disclosures beyond regulatory pressure. Specifically, policymakers can institute mechanisms that provide greater public recognition of data breaches, as opposed to the current approach of mostly relying on the firm's own announcement or that from a government agency (e.g., state attorney general's office). An example in this regard could be a mainstream website, similar in form to the "wall of shame" website from the US Department of Health and Human Services that is used to publicize data breaches in the healthcare sector. The website could be linked to other related, popular sites (e.g., Department of Homeland Security; dhs.gov) to generate public attention. Additionally, the website could have a function that clearly links to the breaches of industry peers to promote institutional pressure on firms to disclose in cases when they have their own external breaches. Regarding internal breaches, regulators may need to engage in stronger efforts to

follow up on such breaches to encourage more detailed disclosures of related information, given that public and institutional pressure do not seem particularly effective.

This study has certain limitations that should be considered. One is our measurement of public attention, which is based on abnormal internet search activity using the Google search engine. The specific limitation is that this measurement does not indicate whether the attention is positive or negative. We made the reasonable assumption that the attention is negative and therefore indicative of public pressure because data breaches have adverse effects on the public. However, a direct assessment of public attention surrounding data breaches is needed to verify this assumption. A valuable expansion of our study would be to build on our measure of public attention by using interviews with focus groups, social media feeds, and so on to conduct a sentiment analysis to determine the degree of positive or negative valence of public attention and then analyze whether this degree of positive or negative public attention differently influences firms' timely cybersecurity disclosures.

Another limitation is that by operationalizing our breach and disclosure variables using summated measures over the course of a given year, we were unable to ascertain how "timely" a firm's response to public and/or institutional pressure may have been. For example, a breach in January may have influenced disclosures in February, or it could have taken until later in the year. Moreover, it is possible in our data that some cybersecurity disclosures occurred at a point in the year prior to the breaches of focal firms and/or industry peers, which raises issues about reverse causality. Regarding any potential reverse causality, as described in Appendix C, we used subsets of our data to create temporal precedence between the breach and disclosure variables, and the results support our hypothesized causal flow (i.e., breaches predicting disclosures and not the other way around). As also described in Appendix C, we used shorter time frames to test for the influences of focal firm and peer breaches on disclosures, and the results continue to support our hypotheses. That said, future research could assess the robustness of our findings with alternative measures for breach and disclosure variables, so that more precise time horizons for the influences of public and institutional pressure can be ascertained.

Another issue with our operationalizations that could be considered a limitation is the overlap in measurement for our breach and disclosure variables. On this point, we found six 8-Ks in our dataset that were original, pure breach announcements—that is, the 8-K was triggered solely by the public announcement of a data breach and it was the first such public announcement. We cross-checked these six 8-Ks with their corresponding breach announcements from the PRC and the dates were the same, which means that the 8-K filing was the same "event" recorded as a breach announcement by the PRC (even though the specific content may have been different). In terms of our operationalizations, using the same event to derive the breach and disclosure variables is potentially problematic from a statistical standpoint in terms of independent-dependent variable independence. It also conflicts with the conceptual distinction between data breach announcements and cybersecurity disclosures (Table 1). To address this limitation, we removed the six breach instances from our operationalizations of the breach/peer breach variables and also subtracted their associated keywords from the operationalizations of disclosures (*DiscWord* and *PrDiscWord*). A total of 15 keywords were removed. We reran all the analyses described in Tables 4, 5, and 6, and the results were qualitatively the same. Hence, while we acknowledge the very limited degree of measurement overlap in our breach and disclosure variables, it does not appear problematic to the study.

A final limitation worth noting is that we focused on external and internal breaches. However, there are other ways to categorize breaches. For example, some prior studies (e.g., Amir et al., 2018; Gordon et al., 2010) have segmented data breaches in terms of confidentiality, integrity, and availability; malicious versus accidental; hack versus nonhack; digital versus physical; etc. We chose the external-internal categorization based on our theorizing, which considers the source of the breach in determining whether the firm is at fault and thus attempts to address its legitimacy concerns. Future research could explore additional categorizations of data breaches to shed further light on the relationships between public and institutional pressure and cybersecurity disclosures. Future research could also study how public and institutional pressure drive the specific content of timely cybersecurity disclosures. That is, similar to how prior work has delved into the content of cybersecurity disclosures in annual 10-Ks (Gordon et al., 2010; Swift et al., 2020; Wang et al., 2013), considering factors such as the type of language used and whether positive (e.g., risk mitigation strategies) or negative (e.g., risk factors) information is conveyed, future research could explore relationships among forms of public and institutional pressure and varying types of cybersecurity content in the more timely 8-K reports.

References

Albon, L., Heaton, P., & Lavery, D. C. (2014). *Consumer attitudes toward data breach notifications and loss of personal information*. RAND Corporation.

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.

Ashbaugh-Skaife, H., Collins, D. W., & Kinney, W. R. (2007). The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. *Journal of Accounting and Economics, 44*(1-2), 66-192.

Ashraf, M., & Sunder, J. (2020). *Does consumer protection regulation benefit shareholders? Evidence from data breach disclosure laws and the cost of equity.* Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3308551

Ayyagari, R. (2012). An exploratory analysis of trends of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security, 8*(2), 33-56.

Bansal, P., & Clelland, I. (2004). Talking trash: Legitimacy, impression management, and unsystematic risk in the context of the natural environment. *Academy of Management Journal, 47*(1), 93-103.

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems, 71*, 62-77.

Baum, C. F., & Lewbel, A. (2019). Advice on using heteroscedasticity-based identification. *The Stata Journal, 19*(4), 757-767.

Benaroch, M., & Chernobai, (2017). A. Operational IT failures, IT value-destruction, and board-level IT governance changes. *MIS Quarterly, 41*(3), 729-762.

Blevins, D. P., Tsang, E. W. K., & Spain, S.M. (2015). Count-based research in management: Suggestions for improvement. *Organizational Research Methods, 18*(1), 47-69.

Bolino, M. C., Kacmar, K. M., Turnley, W. H., & Gilstrap, J.B. (2008). A multi-level review of impression management motives and behaviors. *Journal of Management, 34*(6), 1080-1109.

Bradford, J. L., & Garrett, D. E. (1995). The effectiveness of corporate communicative responses to accusations of unethical behavior. *Journal of Business Ethics, 14*(11), 875-892.

Brown, N., & Deegan, C. (1998). The public disclosure of environmental performance information: A Dual test of media agenda setting theory and legitimacy theory. *Accounting and Business Research, 29*(1), 21-41.

Brown, S. J., & Warner, J. B. (1985). Using daily returns: The case of event studies. *Journal of Financial Economics, 14*(1), 3-31.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*(4), 385-400.

Chalmers, K., & Godfrey, J. M. (2004). Reputation costs: The impetus for voluntary derivative financial instrument reporting. *Accounting, Organizations and Society, 20*(2), 95-125.

Chatterjee, S., Gao, X., Sarkar, S., & Uzmanoglu, C. (2019). Reacting to the scope of a data breach: The differential role of fear and anger. *Journal of Business Research, 101*, 183-193.

Cho, C.H., & Patten, D. M. (2007). The role of environmental disclosures as tools of legitimacy: A research note. *Accounting, Organizations and Society, 32*(7-8), 639-647.

Cho, C. H., Freedman, M., & Patten, D. M. (2012). Corporate disclosure of environmental capital expenditures: A test of alternative theories. *Accounting, Auditing & Accountability Journal, 25*(3), 486-507.

Clarkson, P. T., Li, Y., Richardson, G.D., & Vasvari, F. P. (2008). Revisiting the relation between environmental performance and environmental disclosure: An empirical analysis. *Accounting, Organizations and Society, 33*(4-5), 303-327.

Coleman, D., Usvyatsky, O., & Koren, R. (2019). *Trends in cybersecurity breach disclosures*. Audit Analytics. https://www.auditanalytics.com/audit-analytics-reports

Collins, A. (2018). *The global risks report 2018, 13th edition*. World Economic Forum. http://reports.weforum.org/global-risks-2018/

Crown, W. H., Henk, H. J., & Vanness, D. J. (2011). Some cautions on the use of instrumental variables estimators in outcomes research: How bias in instrumental variables estimators is affected by instrument strength, instrument contamination, and sample size. *Value in Health, 14*(8), 1078-1084.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from

the ChoicePoint and TJX data breaches. *MIS Quarterly, 33*(4), 673-689.

Da, Z., Engelberg, J., & Gao, P. (2011). In search of attention. *Journal of Finance, 66*(5), 1461-1499.

Dean, D. H. (2004). Consumer reaction to negative publicity: Effects of corporate reputation, response, and responsibility for a crisis event. *Journal of Business Communication, 41*(2), 192-211.

Deephouse, D. L., & Suchman, M. (2008). Legitimacy in organizational institutionalism. In R. Greenwood, C. Oliver, & R. Suddaby (Eds.), *The SAGE handbook of organizational institutionalism* (pp. 49-77). SAGE

Depoers, F., & Jerome, T. (2020). Coercive, normative, and mimetic isomorphisms as drivers of corporate tax disclosure: The case of tax reconciliation. *Journal of Applied Accounting Research, 21*(1), 90-105.

DiMaggio, P., & Powell, W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147-160.

Flammer, C. (2013). Corporate social responsibility and shareholder reaction: The environmental awareness of investors. *Academy of Management Journal, 56*(3), 758-781.

Folger, R., & Cropanzano, R. (1988). *Organizational justice and human resource management*. SAGE.

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems, 12*(9), 606-631.

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*(3), 567-594.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems, 35*(2), 683-714.

HBGary. (2013). *Cybersecurity directly affects investor attitudes, new HBGary survey finds*. https://www.prnewswire.com/news-releases/cybersecurity-directly-affects-investor-attitudes-new-hbgary-survey-finds-193105951.html

Haislip, J., Lim, J.-H., & Pinsker, R. (2021). The impact of executives' IT expertise on reported data security breaches. *Information Systems Research, 32*(2), 318-334.

He, J., & Plumlee, M. A. (2020). Measuring disclosure using 8-K filings. *Review of Accounting Studies, 25*(3), 903-962.

Heflin, F., & Wallace. D. (2017). The BP oil spill: Shareholder wealth effects and environmental disclosures. *Journal of Business Finance & Accounting, 44*(3-4), 337-374.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: Who cares? Georgetown McDonough School of Business Research Paper No. 28521519. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852519

Hinz, O., Nofer, M., Schiereck, D, & Trillig, J. (2015) The influence of data theft on the share prices and systematic risk consumer electronics companies. *Information & Management, 52*(3), 337-347.

Hoejmose, S. U., Grosvold, J., & Millington, A. (2014). The effect of institutional pressure on cooperative and coercive "green" supply chain practices. *Journal of Purchasing & Supply Management, 20*(40, 215-224.

Islam, M. A., & Deegan, C. (2010). Media pressures and corporate disclosure of social responsibility performance information: A study of two global clothing and sports retail companies. Accounting and Business Research, *40*(2), 131-148.

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.

Jeong, C. Y., Lee, S-Y. T., & Lim, J.-H. (2013). Information security breaches and IT security investments: Impacts on competitors. *Information & Management, 56*(5), 681-695.

Kappelman, L., Johnson, V. L., Maurer, C., Guerra, K., McLean, E., Torres, R., Snyder, M., & Kim, K. (2020). The 2019 SIM IT issues and trends study. *MIS Quarterly Executive, 19*(1), 69-104.

Konchitchki, Y., & O'Leary, D. E. (2011). Event study methodologies in information systems research. *International Journal of Accounting Information Systems, 12*(2), 99-115.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly, 38*(2), 451-471.

Kwon, J., & Johnson, M. E. (2018). Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quarterly, 42*(4), 1043-1067.

Lang, M., & Lundholm, R. (1993). Cross-sectional determinants of analyst ratings of corporate disclosures. *Journal of Accounting Research, 31*(2), 246-271.

Lange, D., Lee, P. M., & Dai, Y. (2011). Organizational reputation: A review. *Journal of Management, 37*(1), 153-184.

Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of undetected financial reporting deficiencies? *Auditing: A Journal of Practice & Theory, 37*(1), 139-165.

Lerman, A., & Livnat, J. (2010). The new form 8-K disclosures. *Review of Accounting Studies 15*(4), 752-778.

Lewbel, A. (2012). Using heteroscedasticity to identity and estimate mismeasured and endogenous regressor models. *Journal of Business and Economic Statistics, 30*(1), 67-80.

Li, C., Peters, G. F., Richardson, V. J., & Watson, M. W. (2012). The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. *MIS Quarterly, 36*(1), 179-203.

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.

Liu, C. W., Huang, P., & Lucas, H. C. (2020). Centralized information technology decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems, 37*(3), 758-787.

Long, J. S., & Freese, J. (2001). *Regression models for categorical dependent variables using Stata*. Stata Press.

Marquis, C., Toffel, M. W., & Zhou, Y. (2016). Scrutiny, norms, and selective disclosure: A global study of greenwashing. *Organization Science, 27*(2), 483-504.

Martinez-Ferrero, J., & Garcia-Sanchez, I.-M. (2017). Coercive, normative and mimetic isomorphism as determinants of the voluntary assurance of sustainability reports. *International Business Review, 26*(1), 102-118.

Masli, A., Richardson, V. J., Watson, M. D., & Zmud, R. W. (2016). Senior executives' IT management responsibilities: Serious IT-related deficiencies and CEO/CFO turnover. *MIS Quarterly 40*(3), 687-708.

Matwyshyn, A. M. (2009). CSR and the corporate cyborg: Ethical corporate information security practices. *Journal of Business Ethics, 88*(4), 579-594.

Miller, G. S., & Skinner, D. J. (2015). The evolving disclosure landscape: How changes in technology, the media, and capital markets are affecting disclosure. *Journal of Accounting Research, 53*(2), 221-239.

Mohamed, A. A., Gardner, W.L., & Paolillo, J.G.P. (1999). A taxonomy of organizational impression management tactics. *Advances in Competitiveness Research, 7*, 108-130.

Neu, D., Warsame, H., & Pedwell, K. Managing public impressions: Environmental disclosures in annual reports. *Accounting, Organizations and Society, 23*(3), 265-282.

Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & Management, 58*(7), Article 103507.

Oliveira, J., Rodrigues, L. L., & Craig, R. (2011a). Risk-related disclosures by non-finance companies: Portuguese practices and discloser characteristics. *Managerial Auditing Journal, 26*(9), 817-839.

Oliveira, J., Rodrigues, L. L., & Craig, R. (2011b). Voluntary risk reporting to enhance institutional and organizational legitimacy: Evidence from Portugal. *Journal of Financial Regulation and Compliance, 19*(3), 271-289.

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of Management Review, 16*(1), 145-179.

Paternoster, R., Brame, R., Mazerolle, P., & Piquero, A. (1998). Using the correct statistical test for the equality of regression coefficients. *Criminology, 36*(4), 859-866.

Patten, D. M. (1992). Intra-industry environmental disclosures in response to the Alaskan oil spill: A note on legitimacy theory. *Accounting, Organizations and Society, 17*(5), 471-475.

Patten, D. M. (2002). The relation between environmental performance and environmental

disclosure: A research note. *Accounting, Organizations and Society, 27*(8), 763-773.

Patten, D., & Trompeter, G. (2003). Corporate responses to political costs: An examination of the relation between environmental disclosure and earnings management. *Journal of Accounting and Public Policy, 22*(1), 83-94.

Pollock, T. G., Rindova, V. P., & Maggitti, P.G. (2008). Market watch: Information and availability cascades among the media and investors in the U.S. IPO market. *Academy of Management Journal, 51*(2), 335-358.

Ponemon Institute. (2014). *The aftermath of a data breach: Consumer sentiment*. Ponemon Institute.

Rice, S. C., Weber, D. P., & Wu, B. (2015). Does Sox 404 have teeth? Consequences of the failure to report existing internal control weaknesses. *The Accounting Review, 90*(3), 1169-1200.

Richardson, V. J., Smith, R. S., & Watson, M. D. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Syste*ms, *33*(3), 227-265.

Ripberger, J. T. (2011). Capturing curiosity: Using Internet search trends to measure public attentiveness. *The Policy Studies Journal, 39*(2), 239-259.

Roberts, L.M. (2005). Changing faces: Professional image construction in diverse organizational settings. *Academy of Management Review, 30*(4), 685-711.

Romanek, B. (2016). *Cybersecurity disclosures: Not happening much in SEC filings*. TheCorporateCounsel. https://www.thecorporatecounsel.net/blog/2016/09/cybersecurity-disclosures-not-happening-much-in-sec-filings.html

Scott, W. R. (2008). *Institutions and organizations: Ideas and interests* (3rd ed.). SAGE.

Securities and Exchange Commission (SEC). (2011). *CF disclosure guidance, Topic: 2*. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Securities and Exchange Commission (SEC). (2018). *Commission statement and guidance on public company cybersecurity disclosures*. https://www.sec.gov/rules/interp/2018/33-10459.pdf

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341.

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.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review, 20*(3), 571-610.

Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cybersecurity disclosures. *Journal of Forensic and Investigative Accounting, 12*(2), 197-212.

Tan, H.-T., & Yu, Y. (2018). Management's responsibility acceptance, locus of breach, and investors' reactions to internal control reports. *The Accounting Review, 93*(6), 331-355.

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2007). *Effective crisis communication: Moving from crisis to opportunity*. SAGE.

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.

Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychological Review, 92*(4), 548-573.

Wilmhurst, T. D. & Frost, G. R. (2000). Corporate environmental reporting: A test of legitimacy theory. *Accounting, Auditing & Accountability Journal, 13*(1), 10-26.

Verizon. (2020). *2020 data breach investigations report*. https://enterprise.verizon.com/resources/reports/dbir/

Verrecchia, R. E. (2001). Essays on disclosure. *Journal of Accounting and Economics, 32*(1-3), 97-180.

Yen, J.-C., Lim, J-H., Wang, T., & Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy, 37*(6), 489-507.

Zavyalova, A., Pfarrer, M. D., Reger, R. K., & Shapiro, D.L. (2012). Managing the message: The effects of firm actions and industry spillovers on media coverage following wrongdoing. *Academy of Management Journal, 55*(5), 1079-1101.

Appendix A

Table A1. Samples of Cybersecurity Content Disclosed in 8-Ks

8-K triggering event(s)	Cybersecurity content in the 8-K
Revised financial statements from prior year annual 10-K report	We have a dedicated Quality and Productivity team to manage and certify the process management and improvement efforts. For selected risks, we use specialized support groups, such as Information Security and Supply Chain Management, to develop corporate-wide risk management practices, such as an information security program to ensure that suppliers adopt appropriate policies and procedures when performing work on behalf of the Corporation. (excerpted from https://www.sec.gov/Archives/edgar/data/70858/000119312507121631/dex991.htm) Full 8-K details: https://www.sec.gov/Archives/edgar/data/70858/0001193125-07-121631-index.html
Nonreliance on previously issued financial statements Updates on litigation and expenses related to previously announced data breach	In connection with the data breach previously disclosed in the Company's Current Report on Form 8-K filed with the SEC on March 4, 2016, the Company received notice that class action complaints have been filed against the Company. The complaints allege, among other things, that the Company failed to take the necessary security precautions to protect patient information and prevent the data breach. The Company has insurance coverage and contingency plans for certain potential liabilities relating to the data breach. Nevertheless, the coverage may be insufficient to satisfy all claims and liabilities related thereto and the Company will be responsible for deductibles and any other expenses that may be incurred in excess of insurance coverage. (excerpted from https://www.sec.gov/Archives/edgar/data/1503518/000110465916107691/a16-7241_18k.htm) Full 8-K details: https://www.sec.gov/Archives/edgar/data/0001503518/000110465916107691/0001104659-16-107691-index.htm
Disclosure of a data breach, deemed by the firm as meeting the materiality threshold	On September 19, 2018, Chegg learned that on or around April 29, 2018, an unauthorized party gained access to a Company database that hosts user data for chegg.com and certain of the Company's family of brands such as EasyBib. The Company understands that the information that may have been obtained could include a Chegg user's name, email address, shipping address, Chegg username, and hashed Chegg password. The investigation into the incident, which is supported by third-party forensics, is ongoing. To date, the Company understands that no social security numbers or financial information such as users' credit card numbers or bank account information were obtained. Chegg takes the security of its users' information seriously and will be initiating a password reset process for all user accounts. (excerpted from https://www.sec.gov/Archives/edgar/data/1364954/000136495418000187/cyrus.htm) Full 8-K details: https://www.sec.gov/Archives/edgar/data/1364954/0001364954-18-000187-index.html
Announcement of incentives for CEO and other top executives	We constantly work to reinforce the safety and security of customer accounts. PNC has added EMV chip technology to business banking credit cards and will expand the technology to consumer credit and debit cards throughout 2015 in order to provide a stronger form of authentication and to help protect against fraudulent access to customers' information and funds. (excerpted from https://www.sec.gov/Archives/edgar/data/713676/000119312515073000/d877680dex991.htm) Full 8-K details: https://www.sec.gov/Archives/edgar/data/713676/0001193125-15-073000-index.html
Public offering of common stock	Our business is highly dependent upon the uninterrupted operation of our computer systems. We rely on these systems throughout our business for a variety of functions, including processing claims and applications, providing information to customers and distributors, performing actuarial analyses, and maintaining financial records. Despite the implementation of security measures, our computer systems may be vulnerable to physical or electronic intrusions, computer viruses or other attacks, and programming errors or similar disruptive problems. The failure of these systems for any reason could cause significant interruptions to our operations, which could result in a material adverse effect on our business, financial condition, or results of operation. We retain confidential information in our computer systems, and we rely on sophisticated commercial technologies to maintain the security of those systems. Anyone who is able to circumvent our security measures and penetrate our computer systems could access, view, misappropriate, alter, or delete any information in the systems, including personally identifiable customer information and proprietary business information. In addition, an increasing number of states and foreign countries require that customers be notified if a security breach results in the disclosure of personally identifiable customer information. Any compromise of the security of our computer systems that results in inappropriate disclosure of personally identifiable customer information could damage our reputation in the marketplace, deter people from purchasing our products, subject us to significant civil and criminal liability and require us to incur significant technical, legal and other expenses. (excerpted from https://www.sec.gov/Archives/edgar/data/1276520/000119312505185152/dex99.htm) Full 8-K details https://www.sec.gov/Archives/edgar/data/1276520/0001193125-05-185152-index.html

Appendix B

Table B1. Summary of Study Variables

Construct	Operational variable	Operational variable definition	Data source
Cybersecurity disclosure	DiscWord	Number of cybersecurity keywords (total word count) in 8-Ks by firm *i* in year *t*.	Edgar
	PrDiscWord	Number of cybersecurity keywords (total word count) in 8-Ks by firm *i* in year *t-1*.	Edgar
Data breach Announcement	Breach	Indicator variable equal to 1 if firm *i* has a breach in year *t*, 0 otherwise.	PRC
	Internal	Indicator variable equal to 1 if firm *i* has an internal breach in year *t*, 0 otherwise.	PRC
	External	Indicator variable equal to 1 if firm *i* has an external breach in year *t*, 0 otherwise.	PRC
Public pressure	PubAtt	Abnormal internet search activity for the name of the breached firm *i* following its breach announcement; calculated as the average search volume from the day of the breach announcement to three days after, minus the average search volume for the prior 90 days. This variable is only included for firm years with a breach.	Google Trends
Institutional pressure	PeerBreach	Number of breaches by other firms in the same two-digit SIC code in year *t*, excluding breaches by the focal firm.	PRC
	Control variables		
	Assets	Natural log of total assets, in millions, for firm *i* in year *j*.	Compustat
	Employees	Number of employees, in thousands, for firm *i* in year *j*.	Compustat
	CapEx	Total capital expenditures for acquisition and upgrading of physical assets, in millions, by firm *i* in year *j*.	Compustat
	ROA	Return on assets (net income divided by total assets) for firm *i* in year *j*.	Compustat
	Loss	Indicator variable equal to 1 if firm *i* reports negative net income in year *t*, 0 otherwise.	Compustat
	Leverage	Ratio of total liabilities divided by total assets for firm *i* in year *j*.	Compustat
	Analysts	Number of analysts that follow the firm *i* in year *j*.	I/B/E/S
	Industry	Indicator variables for each industry based on two-digit SIC code.	Compustat
	Year	Indicator variables for each year between 2005-2018.	PRC

Appendix C

To address the concern that our measure of public attention could be a proxy for severity of breach or that severity of breach is an omitted variable that could have an endogenous effect on our results, we tested for the effects of three different measures of breach severity in our analyses. For the first measure (*Severity1*), we used the number of individual records compromised for each breach, when provided by the PRC website in its breach descriptions. In our dataset, 376 of the 678 breach announcements included the number of individual records that were compromised. We then tested the correlations between *Severity1* and *PubAtt* (r = 0.16) and *Severity1* and *DiscWord* (r = 0.14), which were fairly low, thereby suggesting the distinctness of these variables. We then reran the OLS regression models that tested H1 and H2, but with *Severity1* included as an independent variable. As shown in Columns 1 and 2 of Table C1, the hypothesized influences of *Breach* and *PubAtt*, respectively, remain significant after controlling for the *Severity1* measure.

We then used a second severity measure (*Severity2*) from Liu et al. (2020), in which breach severity is determined by the type of information compromised in a breach. Specifically, for the *Severity2* measure, we used the PRC breach descriptions to code each breach as either 1 = low severity or 2 = high severity. As described by Liu et al. (2020), high severity is if a breach involves the loss of sensitive information such as social security number, financial information, or medical information, whereas low severity is all other types of breaches. As shown in Columns 3 and 4 of Table C1, the influences of *Breach* and *PubAtt,* respectively, remain significant after controlling for the *Severity2* measure.

For our third severity measure (*Severity3*), we used Haislip et al.'s (2021) measure in which breach severity is scaled from 0 (low severity) to 7 (high severity). The details of the coding are provided in Haislip et al.'s (2021) supplemental appendix, but as a general description, the ranking of severity for each breach is based on whether the breach contained financial data, was instigated by an outsider who used the data, and compromised at least 5000 records. As shown in columns 5 and 6 of Table C1, the influences of *Breach* and *PubAtt,* respectively, remain significant after controlling for the *Severity3* measure.

Obviously, the three different severity measures do not provide perfect tests, but they do provide some assurance that breach severity is not an omitted variable that could bias our results. We also indirectly addressed breach severity in all our models. Recall that rates of breach severity, in terms of the number of records compromised, have been shown to vary by industry (Ayyagari, 2012; Sen & Borle, 2015). Accordingly, Sen and Borle (2015) used industry-related dummy variables (e.g., medical and financial) as proxies for breach severity. In the same way, we accounted for breach severity by including industry dummy variables in each of our models.

We also conducted analysis to address the potential endogeneity of *Breach*, using 2SLS with an instrumental variable (IV) approach. An ideal IV should be correlated with *Breach* but not the error term of *DiscWord* (our dependent variable). Firms' yearly capital expenditures (*CapEx)* fits these criteria, as shown in the correlations in Table 3. The logical rationale for *CapEx* being a suitable IV is that it is a proxy for firm size, and the size of the firm should influence its likelihood of suffering a breach, but there is no strong reason to expect that *CapEx* correlates with cybersecurity disclosures, especially after controlling for the other factors that are captured by our control variables. In the first stage of the 2SLS analysis, *CapEx* is shown as a suitable instrument as it is positively and significantly correlated with *Breach* (p < 0.05). In the second stage, as shown in Column 7 of Table C1, the *Breach* coefficient remains positive and (marginally) significant, thereby continuing to support H1.

As an additional IV analysis, we used Lewbel's (2012) technique for constructing IVs based on existing variables. The details of this technique are described elsewhere (Baum & Lewbel, 2019; Yen et al., 2018). To briefly describe, we conducted a first-stage regression of *Breach* on its exogenous variables (*lnAssets*, *Employees*, *CapEx*, *ROA*, *Loss*, *Leverage*, *Analysts*). For each case (firm year) in our dataset, we then multiplied the residual value from this regression by the mean-centered value of each of the exogenous variables, to generate separate IVs for each exogenous variable. We then used these seven generated IVs to run a 2SLS regression based on our Model 1 in the main analyses (i.e., test of H1) with *Breach* as the endogenous variable. The second stage 2SLS results, shown in Column 8 of Table C1, reveal that the *Breach* coefficient remains positive and significant, thereby continuing to support H1. Note that we did not conduct the IV analyses on the subsamples for internal and external breaches, due to concerns about insufficient statistical power, which can lead to inferential errors in IV analyses (Crown et al., 2011). In a general sense, however, the IV analyses help to alleviate endogeneity concerns surrounding our breach variables.

Finally, we conducted additional analysis to better gauge the time horizon for the influences of public and institutional pressure on cybersecurity disclosures. Again, our summated measures of breaches and cybersecurity disclosures (i.e., keywords) over the course of a given year do not allow us to determine the exact time frame for the influences of public and institutional pressure. To help address this issue, we reran Model 1 (from the main analysis in Table 4) but with *Breach* operationalized as whether the focal firm had a breach in April, May, or June of a given year (i.e., during

the second quarter of the year; coded as "1" or "0" otherwise) and with *DiscWord* operationalized as the total number of cybersecurity-related words (i.e., our keywords) aggregated across a firm's 8-Ks for the last six months of the year (i.e., third and fourth quarters of the year). With these operationalizations, in testing Model 1, we created temporal precedence between focal firm breaches and cybersecurity disclosures and also a smaller time horizon for testing the relationship in H1 (and perhaps indirectly for H2 and H3). The results supported H1, now with stronger evidence of causality, in that the new *Breach* variable was positively associated with the new *DiscWord* variable ($\beta = 0.281$, $p = 0.12$), although the coefficient dipped below significance. We attribute this nonsignificance to the loss of statistical power from the much lower number of breaches that comprised the new *Breach* variable ($N = 176$). For this reason, we did not further split the analysis by internal and external breaches.

We conducted a similar analysis for the influence of peer breaches, as a form of institutional pressure, on cybersecurity disclosures (as per H4). Specifically, we reran Model 5 (from the main analysis in Table 4) but with (1) *PeerBreach* operationalized as the sum of data breaches in the same two-digit SIC code in April, May, and June (i.e., second quarter) of a given year, excluding the focal firm's breaches, and (2) with *DiscWord* operationalized as the total number of cybersecurity-related words (i.e., our keywords) aggregated across a firm's 8-Ks for the last six months of the year. The results showed that the new *PeerBreach* variable had a negative and significant relationship with the new *DiscWord* variable ($\beta = -0.132$, $p < 0.05$), thus supporting H4, over the shorter time horizon and with stronger evidence of causality.

Table C1. Breach Severity and Instrumental Variable (IV) Analysis

	(1) Model 1 w/Severity1	(2) Model 2 w/Severity1	(3) Model 1 w/Severity2	(4) Model 2 w/Severity2	(5) Model 1 w/Severity3	(6) Model 2 w/Severity3	(7) Model 1 2SLS (2nd stage) IV: CapEx	(8) Model 1 2SLS (2nd stage) IV: Lewbel's
PrDiscWord	0.786*** (0.110)	0.797*** (0.105)	0.802*** (0.058)	0.805*** (0.055)	0.807*** (0.059)	0.804*** (0.056)	0.646*** (0.032)	0.649*** (0.030)
Breach	4.352** (1.854)		2.330* (1.129)		2.297* (1.130)		4.780† (2.764)	1.699* (0.736)
PubAtt		0.059* (0.025)		0.058* (0.023)		0.057* (0.022)		
Severity	2.160* (9.601)	1.831* (8.930)	0.342 (0.446)	0.375 (0.439)	0.013 (0.117)	-0.013 (0.119)		
Constant	-4.600 (3.103)	-0.957 (2.285)	-3.691 (2.227)	-2.476 (1.830)	-2.959 (1.989)	-1.608 (1.502)	-1.382 (0.694)	-0.148 (0.380)
Control variables	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	375	374	678	678	678	678	4785	4785
R-squared	0.396	0.407	0.464	0.474	0.461	0.472	0.300	0.410

Note: Standard errors (in parentheses) are clustered at the firm level; † $p < 0.10$, *$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

About the Authors

John D'Arcy is a professor of MIS in the Lerner College of Business and Economics, University of Delaware. His research interests include information security and IT risk management. He received his PhD from the Fox School of Business, Temple University. He currently serves as a senior editor at *MIS Quarterly* and an associate editor at the *Journal of the Association for Information Systems*.

K. Asli Basoglu is an associate professor of MIS and accounting in the Lerner College of Business and Economics, University of Delaware. She holds a PhD from Washington State University, an MA from the University of Virginia, and a BA from Bilkent University. Her research focuses mainly on interrupted decision-making and performance in technology-mediated work environments. Her research has appeared in journals such as *MIS Quarterly*, *Group Decision and Negotiations*, *ACM Transactions on MIS*, and *Accounting, Organizations, and Society*.