THE ACCOUNTING REVIEW
Vol. 98, No. 4
July 2023
pp. 1–32

American Accounting Association
DOI: 10.2308/TAR-2020-0787

Can Shareholders Benefit from Consumer Protection Disclosure Mandates? Evidence from Data Breach Disclosure Laws

Musaib Ashraf
Michigan State University

Jayanthi Sunder
The University of Arizona

ABSTRACT: Data breach disclosure laws are state-level disclosure mandates intended to protect individuals from the consequences of identity theft. However, we argue that the laws help reduce shareholder risk by encouraging managers to take real actions to reduce firms' exposure to cyber risk. Consistent with this argument, we find an on-average decrease in shareholder risk, proxied by cost of equity, after the staggered passage of these laws. We also find the effect is attenuated for firms that already took real actions to manage cyber risk before the laws. Further, after these laws, firms are more likely to increase cybersecurity investments and have a cybersecurity officer. Finally, we observe positive abnormal returns on key dates related to the passage of these laws. Our collective evidence suggests that consumer protection disclosure mandates can benefit shareholders and, specifically, that regulators can use disclosure mandates to incentivize managers to reduce firms' exposure to cyber risk.

Data Availability: All data used in this study are publicly available.

JEL Classifications: G120; G340.

Keywords: cybersecurity; cyber risk; disclosure; cost of capital; information technology; real effects; capital markets; disclosure mandates; consumer protection; corporate governance.

I. INTRODUCTION

Separation of ownership and control, and the existence of externalities, gives rise to opportunistic behavior by managers (Jensen and Meckling 1976). An important dilemma faced by regulators is whether to outright prohibit such behavior or to mandate the disclosure of any occurrences of the behavior. Theory suggests that disclosure mandates can be used in lieu of prohibitory regulation because shining a light on opportunistic behavior through disclosure can discourage managers from engaging in the behavior in the first place (Leuz and Wysocki 2016). Extant literature has extensively studied the effects of shareholder-centric disclosure mandates (e.g., Christensen, Hail, and Leuz 2016). However, evidence is limited on whether shareholders benefit from disclosure mandates that are specifically designed to protect other stakeholders, like consumers (Leuz and Wysocki 2016). To that end, in this study, we examine the effect of data breach disclosure laws on shareholder risk.

We thank Elizabeth Blankespoor (editor), two anonymous reviewers, and workshop or conference participants at the 2019 Financial Accounting and Reporting Section (FARS) Midyear, Southern Methodist University, University at Buffalo, SUNY, The University of Arizona, University of Oregon, and University of Washington for their insightful comments. We thank Broad College of Business and Department of Accounting & Information Systems at Michigan State University and Eller College of Management and Dhaliwal-Reidy School of Accountancy at The University of Arizona for funding that enabled this study. Any errors are our own.

Musaib Ashraf, Michigan State University, Broad College of Business, Department of Accounting & Information Systems, East Lansing, MI, USA; Jayanthi Sunder, The University of Arizona, Eller College of Management, Dhaliwal-Reidy School of Accountancy, Tucson, AZ, USA.

Editor's note: Accepted by Elizabeth Blankespoor, under the Senior Editorship of W. Robert Knechel.

Submitted: December 2020
Accepted: October 2022
Early Access: February 2023

Data breach disclosure laws are state-level disclosure mandates that aim to protect individuals whose personal information is leaked by firms in data breaches. We study these laws because, in addition to allowing us to speak to an important economic question, cybersecurity itself is a growing economy-wide risk that concerns a diverse set of stakeholders, including investors, regulators, practitioners, and the government (Ernst & Young 2011). For example, investors consider cyber risk to be a top threat to firm growth (PricewaterhouseCoopers (PwC) 2018), and the Securities and Exchange Commission (SEC) (2022) has proposed a new rule that requires firms to disclose in 8-K filings the occurrences of material cyber incidents. Consequently, it is of first-order importance to document whether cybersecurity-related disclosure mandates incentivize managers to reduce shareholder risk by prioritizing cybersecurity.

The data breach disclosure laws require breached firms to inform every individual whose information is leaked in a breach (e.g., customers or employees). These private disclosures are intended to provide timely warning to affected individuals so that they can manage the consequences of potential identity theft (Romanosky, Telang, and Acquisti 2011). However, once disclosed, firms cannot prevent the negative breach news (which has been conveyed to potentially millions of individuals) from disseminating more widely in capital markets. Thus, although the laws require private disclosure of breaches, they result in widespread public knowledge of the occurrence of breaches and can be viewed as *de facto* public disclosures of breaches.[1]

We argue that the laws benefit shareholders due to managers' desires to avoid having to disclose bad news (i.e., the occurrence of a breach). Consistent with Leuz and Wysocki (2016, 527) contention that consumer protection disclosure mandates can "incentivize desirable behavior [by firms]," the laws increase the salience of cyber risk and thus likely improve firms' oversight of cybersecurity: firms will arguably take real actions to enhance cybersecurity and reduce the likelihood of incurring a data breach—which they would now need to *de facto* publicly disclose, should one occur. For example, PricewaterhouseCoopers (PwC) (2016, 1) notes that data breach disclosure laws have "spurred a decade of unprecedented corporate spending on information security."[2] Since investors respond negatively to data breaches and cyber risk (Kamiya, Kang, Kim, Milidonis, and Stulz 2021; Ashraf 2021a; Florackis, Louca, Michaely, and Weber 2022), steps taken to mitigate cyber risk are likely to be viewed favorably by shareholders. We refer to this as the "real effects mechanism."

We examine the impact of data breach disclosure laws on shareholder risk proxied by firms' cost of equity capital. Cyber risk is an economy-wide risk that all corporations, governments, and individuals face. Whereas steps can be taken to mitigate cyber risk, it is widely acknowledged that there is no panacea and, given the increasing digitization of firm operations and data, cyber incidents cannot be completely prevented (Deloitte 2015; Online Trust Alliance 2017). Therefore, cybersecurity risk is a systematic risk factor distinct from other risk factors (Florackis et al. 2022), and firms with greater cyber risk exhibit higher cost of equity (Jiang, Khanna, Yang, and Zhou 2022). Thus, we expect the cost of equity to capture changes in shareholder perception of a firm's cyber risk after the passage of data breach disclosure laws.

At different points in time between 2002 and 2014, 47 states in the United States passed a data breach disclosure law (see Figure 1). Using this staggered variation, we first examine the difference-in-differences impact of these laws on the cost of equity. We find that, on average, there is a statistically significant 19-basis-point decrease in the cost of equity after a firm's home state passes a data breach disclosure law (or a 3.8 percent reduction relative to the sample mean).[3]

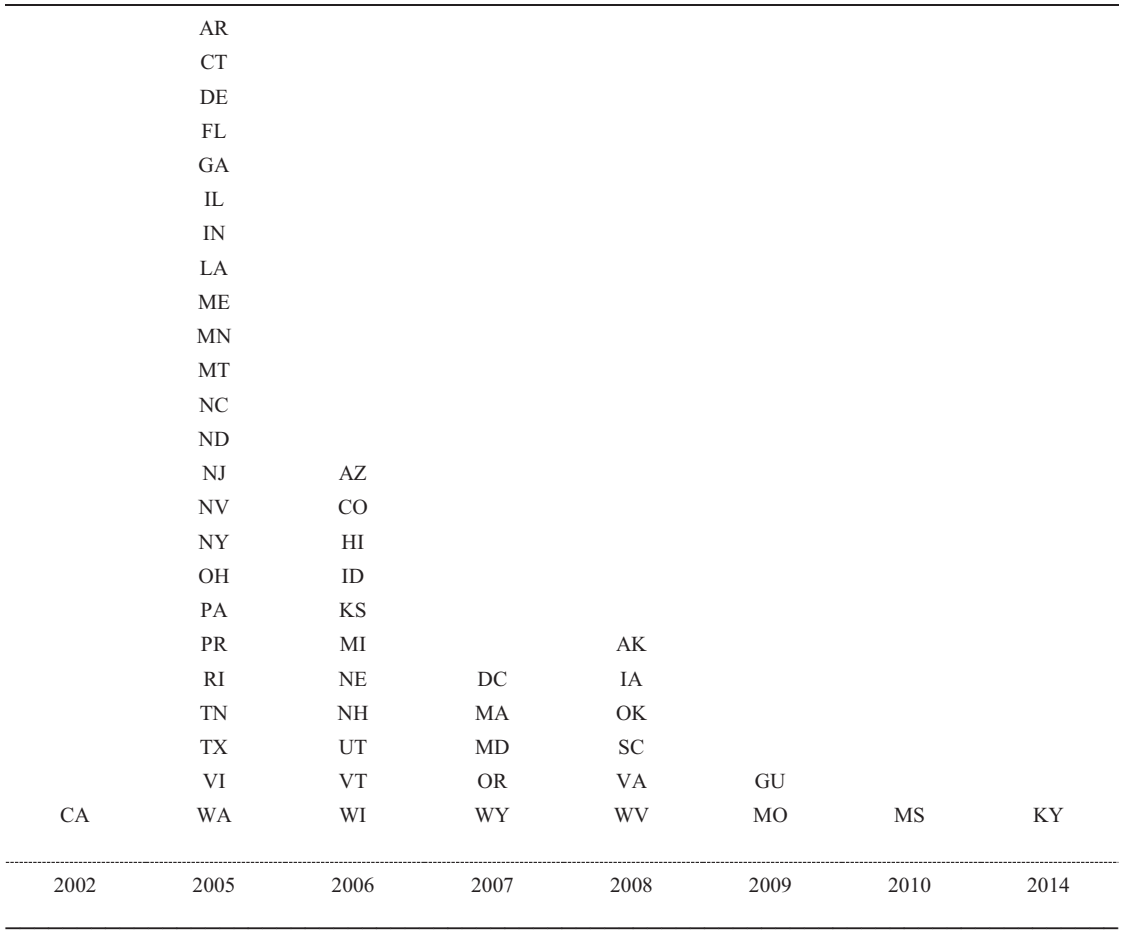
We subject our finding to several sensitivity tests. Data breach disclosure laws of a given state are written to protect breach victims residing in that state; thus, a firm's exposure to these laws is dependent on where the firm's customers and employees are located. Due to data limitations, we cannot observe firms' state-by-state distribution of customers and employees. Consequently, given that a firm arguably has a significant number of customers and employees in their home state, we follow prior literature and assign exposure to the laws based on a firm's home state (Kamiya et al. 2021; Huang and Wang 2021). We conduct eight sensitivity analyses (such as proxying for firms' geographic dispersion using 10-K filings and measuring exposure to the laws based on major customer locations) to provide assurance that our inferences are robust to this research design choice. Further, we use higher-order fixed effects to control for time-varying industry characteristics (which help mitigate concerns that specific industries drive our findings) and double-cluster standard errors by state and by year to mitigate concerns about within-year correlations, mitigate the Goodman-Bacon (2021) concern regarding biased coefficients in generalized difference-in-differences research designs, use placebo dates

[1] Supporting this premise, we find a sharp increase in the number of publicly disclosed data breaches in event time after the state-level data breach disclosure laws become effective (see Appendix B).

[2] Likewise, in unstructured interviews, two practitioners (both with over 20 years of experience, one as a cybersecurity professional in top management teams and the other as a cybersecurity lawyer) expressed to us that the data breach disclosure laws encouraged firms to invest in cybersecurity because firms dislike disclosing negative news about a breach.

[3] For reference, Dhaliwal et al. (2016) find having at least one major customer (10 percent or more of total sales) is associated with a 21.2-basis-point increase in cost of equity, and Goh et al. (2016) find one standard deviation increase in tax avoidance is associated with a 13- to 26-basis-point decrease in cost of equity.

FIGURE 1
Temporal Distribution of When States Sign into Law a Data Breach Disclosure Law



for the laws to rule out other confounding events, and provide evidence that the parallel-trends assumption appears to hold in our setting. We also use alternative methodologies for computing cost of equity (which helps assuage the concern that our chosen method of calculating cost of equity is driving our results). Our inferences remain unchanged.

We next conduct two cross-sectional analyses. Our theory suggests that we observe an on-average reduction in cost of equity because the laws encourage managers to reduce cyber risk exposure through real actions. Arguably, the laws are relatively less able to induce real actions that mitigate cyber risk for firms that already took real actions to mitigate cyber risk prior to the passage of the laws. Accordingly, we find the reduction in cost of equity is attenuated for firms that were already investing in cybersecurity prior to the passage of data breach disclosure laws. Similarly, firms that have an information-technology or cybersecurity officer on the top management team prior to the laws arguably already prioritized cybersecurity more than other firms. We find an attenuated effect of the laws on the cost of equity for firms that possess such executive officers prior to the passage of the laws.

We conduct two more analyses to provide further evidence to support our assertion that the laws induce real actions to reduce cyber risk. Specifically, we study whether firms increase cybersecurity investments and cybersecurity expertise in the top management team after the data breach disclosure laws are passed. We find evidence suggestive of an increase in both.

Finally, we examine the stock-price reaction around key dates related to the passage of the laws. We find positive and statistically significant abnormal returns around these dates. This result supports our main finding that shareholders expect to benefit from these laws.

Notwithstanding the caveats we discuss in the conclusion, we contribute to the literature by providing evidence that suggests that there is a beneficial impact of consumer protection disclosure mandates for shareholders.[4] Our evidence is important for two reasons. First, as digitization of industry has increased over time, there has been a dramatic increase in data breaches specifically and cybersecurity incidents in general (Identity Theft Resource Center 2017). The SEC has voiced growing concern regarding firms' exposure to cyber risk (Clayton 2018); so too have accountants (American Institute of Certified Public Accountants (AICPA) 2015), industry organizations (Depository Trust and Clearing Corporation 2018), governments (U.S. Treasury Department 2013), and shareholders (PwC 2018). Consequently, our evidence is timely, as various stakeholders grapple with firms' cyber risks and how best to mitigate them, and our evidence informs regulators about an important consequence of cybersecurity-related disclosure mandates. Our results are particularly relevant, given the ongoing debate regarding whether there should be a federal law governing disclosure of breaches (Mitnick 2018; Ronaldson 2019; Beckage 2021). For example, the SEC (2022) recently issued a proposal that, if passed, would require public firms to disclose (in 8-K filings) the occurrence of material cyber incidents. Although we are not the first to study data breach disclosure laws (Romanosky et al. 2011; Kamiya et al. 2021; Huang and Wang 2021), we are the first to provide evidence that suggests that the laws induce managers to take real actions to enhance oversight over cyber risk, leading to reduced shareholder risk.

Second, our results support the conjectures of Leuz and Wysocki (2016, 527), who argue that consumer protection disclosure mandates may play a governance role by "incentivizing desirable behaviors and discouraging undesirable ones" and note that "this governance role of disclosure regulation deserves greater attention [in the literature]". Although there is an expansive literature that focuses on shareholder-centric disclosure mandates (e.g., Cho 2015), our manuscript is most related to the more-nascent literature that studies other types of disclosure mandates. We differentiate from this literature by documenting the effects of a pervasive disclosure mandate rather than focusing on a specific industry (e.g., Christensen, Floyd, and Maffett 2020). Further, these studies typically do not explore the impact of disclosure mandates on residual claimants, such as shareholders (e.g., Jin and Leslie 2003), nor do they empirically identify the channel through which the observed effects take place (e.g., Bennear and Olmstead 2008). We document evidence that suggests a beneficial effect for shareholders and are able to attribute it to firms' real actions.

II. INSTITUTIONAL KNOWLEDGE, RELATED LITERATURE, AND CONCEPTUAL DEVELOPMENT

Institutional Knowledge about Data Breach Disclosure Laws

Disclosure of data breaches is governed by state law in the U.S. In 2002, California became the first U.S. state to pass a law that requires firms to notify (California) residents when an unauthorized entity obtains access to a person's private information (Skinner 2003). After California, between 2003 and 2014, 46 other U.S. states phased in their own laws that require firms to disclose data breaches (Perkins Coie 2018) (see Figure 1).

Although there are some specific federal laws that govern personal-data collection by firms in certain industries, such as healthcare (Health Insurance Portability and Accountability Act, or HIPAA) and the financial services industry (Gramm–Leach–Bliley Act, or GLBA), there is no comprehensive federal law regarding data breaches.[5,6] Moreover, currently, attempts to introduce a federal law have thus far been unsuccessful, such as the Cybersecurity and Infrastructure Security Agency Act and the Data Security and Breach Notification Act. Therefore, state-level data breach disclosure laws are the primary statutes designed to strengthen consumer rights and protect individuals from identity theft (Jones Day 2003; Schwartz and Janger 2006).

[4] Some shareholders may not view a decrease in cost of equity as beneficial. For these shareholders, the effects we document in our manuscript may be viewed as harmful.

[5] Although HIPAA and GLBA were both passed in the 1990s, public disclosure of data breaches under HIPAA and GLBA was not required until September 2009 and March 2005, respectively (Department of Health and Human Services 2018; American Bankers Association 2018).

[6] The SEC issued guidance in 2011 that notes that all firms have obligations under existing securities law to disclose material events and risks in 10-K filings, and this requirement applies to material cyber incidents and cyber risks as well (Securities and Exchange Commission (SEC) 2011). Empirically, the SEC's guidance is unlikely to confound our findings because (1) of our difference-in-differences design and the fact that such guidance impacts all firms simultaneously and (2) the majority of data breach–disclosure laws were passed prior to 2011.

The laws mandate that breached firms must notify each person whose nonpublic, personally identifiable information has been obtained by an unauthorized entity (Perkins Coie 2018), and the laws cover all persons whose information is retained by a firm—including customers and employees.[7,8] Nonpublic, personally identifiable information is generally defined as private information about a person that is not normally publicly available (e.g., social security number) (Baker & Hostetler LLP 2017). An unauthorized entity is typically persons who would not have access to the information during the normal course of business, and the laws do not differentiate between intent (i.e., it does not matter if a data breach is accidental or malicious).

The laws do *not* mandate that breached firms compensate affected individuals. Nonetheless, the laws are intended to protect breach victims because notification about a breach enables affected individuals to take appropriate action to protect their identity. The central purpose of the laws is for firms to notify affected individuals (Shaw 2010; Romanosky et al. 2011); this is the common "primary" element in all the laws and is the focus of our study. However, not all the laws are identical, and there are some "secondary" implementation differences across states. In particular, the laws may vary across three characteristics: (1) imposing an explicit deadline by which firms must issue the disclosures after a breach has been discovered; (2) requiring a "harm" assessment prior to making disclosures, which requires firms to make the disclosures only if the firm has determined that the breach is reasonably likely to cause harm to the victims; and (3) mandating the firm to also notify the attorney general or other state or credit agency of a data breach (Perkins Coie 2018). Further, the penalty for nondisclosure varies across the laws, and states' attorneys general are tasked with enforcing the laws—they are empowered to bring penalties and actions against breached firms, which may include seeking restitution for affected individuals (Perkins Coie 2018).[9] Yet, despite differences between the laws, Shaw (2010, 522) notes that the laws "are, on balance, rather harmonious." Refer to Baker & Hostetler LLP (2017), Perkins Coie (2018), and Foley & Lardner LLP (2019) for detailed discussions on the secondary implementation differences of the laws.

It is important to note that the laws do not require market-wide public disclosure of a data breach *per se*; the laws require private disclosure to affected individuals.[10] However, the laws are a *de facto* requirement to make market-wide public disclosure of a data breach because private notification about a data breach to potentially millions of affected individuals is unlikely to stay private. Thus, an important underlying assumption in our study is that the laws increase public awareness of data breaches. In other words, without the disclosure laws, there would be fewer publicly known data breaches. We examine this assumption in Appendix B and find that, when we plot data-breach disclosures in event time (centered on the date when a data breach disclosure law goes into effect in each state), we find a sharp increase in public breach disclosures in the post period. This is consistent with our premise that these laws encourage public awareness of breaches.

Related Literature

Extant literature that studies disclosure mandates can generally be categorized into two groups: work that studies shareholder-centric disclosure mandates, such as securities law or financial-reporting regulation, and work that studies disclosure mandates that are targeted at other stakeholders.[11,12] Focusing on the latter, Jin and Leslie (2003) study the effect of Los Angeles County mandating customers be informed of restaurants' hygiene grades and find that food-borne

[7] Data breach disclosure laws are written from the perspective of the state residency of the person whose information is breached rather than the state residency of the firm that experienced the breach. For example, California law requires a New York firm to disclose to California residents if their personally identifiable information has been compromised even if it is a New York firm rather than a California firm. At the same time, it is unclear whether California law applies to a New York firm with no California presence. In our manuscript, we assign exposure to data breach disclosure laws based on a firm's home state. We discuss this research design in more detail in Section III.

[8] Coca-Cola's 2013 breach is an example of employee-related data breach and was reported on by *The Wall Street Journal* on the same day that Coca-Cola made the disclosure (Esterl 2014). Sony's 2011 breach is an example of a customer-related data breach and was reported on by *Reuters* on the same day that Sony made the disclosure (Baker and Finkle 2011)

[9] It is important to differentiate between litigation for the breach itself and litigation for failure to disclose the breach. The laws are regarding the latter, not the former.

[10] When a firm does not have contact information for affected individuals or when individually notifying affected individuals is impractical or the cost is prohibitive, firms are allowed to opt for alternate disclosure methods, such as posting a notice of the breach on the firm's website and conveying the news through major print and broadcast media.

[11] Gao, Wu, and Zimmerman (2009); Faulkender and Yang (2013); Cho (2015); Christensen, Floyd, Liu, and Maffett (2017); and Granja (2018) are all examples of manuscripts that study shareholder-centric disclosure mandates. Given the vastness of this literature and the fact that our manuscript is more closely related to literature that studies other types of disclosure mandates, we do not delve into a discussion of existing evidence on the effects of shareholder-centric disclosure mandates. Refer to Leuz and Wysocki (2016) for a comprehensive review of such manuscripts.

[12] There is a rich literature that studies disclosure and finds greater disclosure has an array of benefits, including, but not limited to, greater liquidity (e.g., Welker 1995; Healy, Hutton, and Palepu 1999; Leuz and Verrecchia 2000; Ng 2011; Balakrishnan, Billings, Kelly, and Ljungqvist 2014), enhanced investment efficiencies (e.g., Biddle and Hilary 2006; Biddle, Hilary, and Verdi 2009; Goodman, Neamtiu, Shroff, and White 2014; and Jung, Lee, and Weber 2014), and reduction in litigation risk (e.g., Skinner 1994, 1997; Field, Lowry, and Shu 2005; and Donelson, McInnis, Mergenthaler, and Yu 2012). However, this literature studies cross-sectional and time-series differences in (usually voluntary) disclosures themselves rather than disclosure mandates *per se*.

illnesses in the county subsequently decrease; Dranove, Kessler, McClellan, and Satterthwaite (2003) and Cutler, Huckman, and Landrum (2004) document that mandatory disclosure of healthcare reports affects matching of patients and providers in New York; Bennear and Olmstead (2008) find a reduction in drinking-water health violations in Massachusetts after drinking-water suppliers are required to inform customers about water quality; Lu (2012) suggests nursing homes reallocate effort toward service quality after the introduction of mandatory quality disclosures; Kolstad (2013) reports a decrease in patient mortality after the introduction of mandatory surgeon performance reports; and Christensen et al. (2020) find price-transparency regulation reduces hospital charges.

In aggregate, the literature is clear that disclosure mandates do have the ability to induce behavior by stakeholders. However, there remain open questions regarding the impact of disclosure mandates (Leuz and Wysocki 2016), because extant literature tends to focus on narrow disclosure mandates that impact particular industries rather than market-wide mandates; for example, Christensen et al. (2020) study hospitals. Further, these manuscripts generally do not analyze the effect of disclosure mandates on residual claimants. For example, Jin and Leslie (2003) are unable to observe whether the hygiene grade card disclosure mandate benefited or harmed the restaurant owners. Relatedly, as Leuz and Wysocki (2016) note, extant literature is often unable to disentangle between the firm taking actions in response to the disclosure mandate or the results being observed because other stakeholders change behavior. For example, Bennear and Olmstead (2008) do not provide evidence on the mechanisms through which the health-violations reduction takes place.

Further, there is a nascent literature that studies data breachdisclosure laws specifically. In particular, the primary intention of the laws is that knowledge about a breach helps breach victims protect themselves from identity theft. Romanosky et al. (2011) directly test this assertion and find evidence that identity theft decreases after the passage of the laws. Kamiya et al. (2021) and Huang and Wang (2021) do not study the disclosure laws *per se*; rather, these manuscripts focus on the effect of actual data breaches on firm value and debt contracting, respectively. Nonetheless, both manuscripts conduct an analysis involving the laws within the larger context of their research questions. Kamiya et al. (2021) find no evidence that the negative impact of breaches on firm value is different based on whether the firm is exposed to a data breach disclosure law. Huang and Wang (2021) find evidence that the negative effect of a breach on loan terms is more salient when a breached firm is exposed to a data breach disclosure law. Both studies highlight the adverse consequences of data breaches, conditional on being known publicly, and thereby underscore the importance of taking real actions to avoid experiencing a breach, because disclosure is more inevitable after the laws are passed.

Conceptual Development

Does Cyber Risk Increase the Cost of Equity?

As noted in a survey of cybersecurity experts by AIG (2016) and supported by Deloitte (2015), World Economic Forum (2016), and Disparte and Williams (2017), cyber risk impacts the market as a whole and thus should be nondiversifiable by investors. For example, cyber risk has been shown to have a contagion effect across multiple firms in the economy, such as supply chains (Crosignani, Macchiavelli, and Silva 2021), peer firms (Kamiya et al. 2021; Ashraf 2021b), and throughout the financial sector (Duffie and Younger 2019). Supporting this notion, the Depository Trust and Clearing Corporation (2018) notes that cyber risks "have grown to a point where they may have become the most important near-term threat to financial stability [of the economy]."

If cyber risk is nondiversifiable, then it should be a priced risk factor. Accordingly, Florackis et al. (2022) provide empirical evidence on commonality in cyber risk across all stocks and show that cyber risk is priced in the cross-section of returns. Therefore, cyber risk is a distinct systematic risk factor that cannot be diversified away by shareholders (Florackis et al. 2022), and firms with greater exposure to cyber risk have a higher *ex ante* cost of capital (Jiang et al. 2022).[13] We illustrate this argument using an expanded version of the standard capital asset–pricing model:

$$E(R_{it}) = \alpha + \beta_i E(R_{mt} - R_{ft}) + \gamma_i E(Cyber\ \ Risk\ \ Premium_t) + \varepsilon_{it},$$

[13] Even if there is an idiosyncratic or diversifiable component of cyber risk, studies show that investors are unable to fully diversify due to market frictions or investor biases, and therefore, some idiosyncratic risk is priced (Malkiel and Xu 2004; Spiegel and Wang 2005; Fu 2009; Dhaliwal et al. 2016). For example, one reason for why cyber risk may not be diversified is the limited development of the cyber insurance market; there is uncertainty amongst firms about the ability of a nascent cyber insurance market to actually pay out in the event of a catastrophic cyber event (Reeve 2015; Jones 2016). Further, although firms that sell cybersecurity systems are a potential hedge against cyber risk, these firms are too few to serve as a hedge for the whole economy and are themselves susceptible to data breaches. In a somewhat related context, Tomunen (2021) argues that natural-disaster risk is undiversifiable and priced because of inadequate risk sharing by market participants. Since frictions to diversification leads to idiosyncratic risk being priced, we expect cyber risk to affect cost of equity, even if cyber risk was theoretically diversifiable.

where γ_i is positive (Florackis et al. 2022; Jiang et al. 2022). Consequently, firms that take real actions to improve cybersecurity will reduce their exposure to the cyber-risk premium, which should manifest as a decrease in the cost of equity. It is important to note that, because of the above-discussed contagion effects, one firm reducing its exposure to cyber risk can also benefit other firms in the economy. In other words, improving cybersecurity has a *direct* effect by reducing the focal firm's γ_i and an *indirect* effect by reducing the cyber-risk premium for all firms. However, as long as the cyber-risk premium is not completely eliminated, firms that take real actions to improve cybersecurity should exhibit lower cost of equity through a reduced γ_i.

Hypothesis

Against the backdrop that cyber risk is a distinct risk factor that increases the cost of equity, we argue that data breach disclosure laws reduce a firm's cost of equity by encouraging managers to take real actions to prioritize cybersecurity, mitigate exposure to cyber risk, and reduce the likelihood of incurring a data breach. This is because the laws result in *de facto* public disclosure of bad news (i.e., data breaches) that, once disclosed, may have material negative consequences for firms (e.g., Gatzlaff and McCullough 2010; Gay 2017; Cisco 2017; Ponemon Institute 2017a, 2017b; Sheneman 2017; Amir, Levi, and Livne 2018; Smith, Higgs, and Pinsker 2019; Lawrence, Minutti-Meza, and Vyas 2018; Janakiraman, Lim, and Rishika 2018; Kamiya et al. 2021; Huang and Wang 2021; Ashraf 2021a, 2021b). Consequently, the desire to avoid disclosing costly bad news provides strong incentives for managers to decrease the likelihood of experiencing a breach in the first place (Laube and Böhme 2016).[14] Indeed, PwC (2016) suggests data breach disclosure laws encourage firms to improve their information technology (IT) and cybersecurity.

Data breach disclosure laws should help reduce a firm's cost of equity for three reasons. First, managers often underinvest in cybersecurity, even though such investments reduce firms' exposure to cyber risk. Arguably, managers and investors both do not desire a breach. However, cybersecurity investments usually enable firms to avoid costs instead of generate revenue, and managers prefer revenue-generating investments over cost-saving investments (Gordon 2007). This problem is amplified specifically for cybersecurity because the costs avoided through better cybersecurity, such as preventing a breach, are usually unobservable (Gordon, Loeb, Lucyshyn, and Zhou 2018). Further, managers may not always shoulder the costs of poor cybersecurity due to the unpredictable timing of cyber incidents: the current managers may leave the firm before a breach happens. Therefore, self-interested managers—who determine how to allocate limited resources—often deploy insufficient resources to cybersecurity. For example, Accenture (2014) reports that 45 percent of executives admit to underinvesting in cybersecurity. Likewise, the U.S. Treasury Department (2013, 5) notes that firms underinvest in cybersecurity "for reasons of cost or perception that existing threats do not warrant investment." We argue that data breach disclosure laws incentivize investments in cybersecurity by making cyber risk more salient. The resulting investments in cybersecurity should reduce a firm's γ_i and, thereby, the cost of equity.

Second, firms can benefit from reduced cyber risk through a network effect. A firm's cyber risk is a function of both its own cybersecurity and the cybersecurity of the trade partners that the firm may share interorganizational information systems with (e.g., Premkumar and Ramamurthy 1995). For example, Target's 2013 breach occurred because criminals gained access to Target's network through one of Target's vendors (Krebs 2014). Thus, the laws may reduce a firm's cyber risk by encouraging its trade partners (who are also subject to the laws) to invest in cybersecurity. Reduction in γ_i through a network effect should manifest as a reduction in the cost of equity.[15]

Third, investments in cybersecurity can involve upgrades to overall control environment (Ashraf 2022), and this can have a within-firm spillover effect of decreasing shareholder risk that is not directly related to cybersecurity. For example, the National Institute of Standards and Technology Cybersecurity Framework mandates that firms first develop a deep understanding of their control environment before they develop cybersecurity strategies. A potential consequence of this process is the strengthening of a firm's control environment. Any within-firm spillover that helps improve controls should decrease cost of equity (e.g., Ashbaugh-Skaife, Collins, Kinney, and Lafond 2009).

Taken together, the previous arguments suggest that shareholders should experience a reduction in shareholder risk after the passage of data breach disclosure laws. It is important to note that reduction in shareholder risk may occur based on *either* or *both* the market's expectation that firms will take real actions to reduce exposure to cyber risk and/or the market actually observing these real actions (which firms may disclose to investors through a variety of channels,

[14] Although there is some debate over whether the negative impact of the average data breach is economically meaningful (e.g., Ponemon Institute 2017b; Amir et al. 2018; Richardson et al. 2019; Kamiya et al. 2021), in the context of our study, we argue that it isn't necessarily the average impact on firm value that incentivizes firms to mitigate cyber risk but rather the desire to avoid tail risk—i.e., rare events that have a catastrophic impact on firm value, such as an immediate 19 percent stock price decline after Equifax disclosed its 2017 data breach (Fortune 2017).

[15] Reduction in γ_i through a network effect is related to but different from a reduction in the cyber-risk premium. The former is possessing stronger cybersecurity because trade partners enhanced their cybersecurity. The latter is the cyber-risk premium being a less-significant risk factor overall.

such as 10-K filings). We state our hypothesis in its alternative form: data breach disclosure laws are associated with a decrease in the cost of equity capital.

III. RESEARCH DESIGN

Model

To test the effect of data breach disclosure laws on a firm's cost of equity capital, we estimate the following ordinary least squares (OLS) regression model:

$$COE_{it} = \beta_i + \beta_t + \beta_1 LAW_{it} + \sum \beta_n Controls_{it} + e_{it}, \quad (1)$$

where i indexes firm, t indexes years, and COE is our measure of implied cost of equity. Following Hail and Leuz (2006) and Dhaliwal, Judd, Serfling, and Shaikh (2016), COE is the average of the implied cost of equity methodologies of Claus and Thomas (2001); Gebhardt, Lee, and Swaminathan (2001); modified Easton (2004); and Ohlson and Juettner-Nauroth (2005).[16] COE is calculated for firm i's year t using stock prices and analyst estimates in the first June after year end, and we subtract the risk-free rate (10-year Treasury bond rate) from each measure (Dhaliwal et al. 2016).[17]

The test variable in our study is LAW. LAW equals 1 for all years with a fiscal year end after a data breach disclosure law has been signed into law in firm i's home state (i.e., business headquarters state) and 0 otherwise (Kamiya et al. 2021; Huang and Wang 2021).[18] We cluster robust standard errors at the state level, since our test variable is a state-level treatment (Abadie, Athey, Imbens, and Wooldridge 2022).[19] Because we include firm and year fixed effects (β_i and β_t, respectively), β_1 captures the difference-in-differences effect of the laws on cost of equity (Bertrand and Mullainathan 2003; Armstrong, Balakrishnan, and Cohen 2012).

Finally, following Dhaliwal et al. (2016), Campbell, Dhaliwal, and Schwartz (2012), and K. Chen, Z. Chen, and Wei (2011), we include a vector of firm-year control variables that prior literature has shown to impact cost of equity. These variables are *SIZE*, *LEVERAGE*, *ROA*, *MTB*, *MOMENTUM*, *VW_BETA*, *DISPERSION*, *LT_GROWTH*, and *RISK*. All variables are defined in Appendix A.

Sample Selection

Table 1 summarizes our sample selection. We begin with 91,478 firm years for U.S.-based firms on Compustat between 2001 and 2015, with data available on historical business headquarters states.[20,21] We next match observations to Institutional Brokers' Estimate System (I/B/E/S) to calculate cost of equity measures and eliminate 24,591 firm years that have no I/B/E/S coverage. Finally, we eliminate 37,705 observations that have data missing to calculate necessary variables and 2,718 observations that change business headquarters state during our sample period (to ensure our firm

[16] We calculate these measures as implemented by Dhaliwal et al. (2016). Refer to Appendix A in Dhaliwal et al. (2016) for more details.

[17] In other words, the convention established in the cost of equity literature is to calculate cost of equity for each firm in June of every year and assign that cost of equity calculation to the most recently ended firm-year observation (e.g., Gebhardt et al. 2001; Gode and Mohanram 2003; Dhaliwal et al. 2016). So, instead of calculating cost of equity on the day that a firm-year ends, the literature has calculated it in the month of June that immediately follows firm-year end to allow for financial information pertaining to the fiscal year to become publicly available. For example, the cost of equity is calculated in June 2011 for firm years with a December 2010 year end.

[18] As we note in Section II, data breach–disclosure laws are written from the perspective of the state residency of the breach victim. Thus, firms are exposed to the laws based on the states where they have operations, not just their home state. Given data limitations such that we cannot observe firms' state-by-state operations, we assign the laws to firms based on home state, because the average firm will tend to have a significant, if not largest, customer and employee base in their home state (e.g., Pirinsky and Wang 2006); thus, firms should conceptually respond to the laws passed in their home state. However, to the extent that firms may have begun responding to the laws prior to their home state passing such a law, our measured response is a lower bound of the total effect of these laws, as the impact on cost of equity should be weaker if a firm started responding to the laws when exposed to one of the laws prior to the firm's home state passing its own law. We conduct several sensitivity analyses in Section IV to ensure that our inferences are robust to this concern.

[19] We do not double cluster by state and by year in our main specification, because we have relatively few years in our sample and standard errors are not consistent when the number of clusters is too few (e.g., Petersen 2009; Cameron and Miller 2015). However, we double cluster by state and by year in sensitivity analyses in Section IV to provide evidence that our results are not driven by within-year correlation of standard errors. Conley, Goncalves, and Hansen (2018) propose a novel methodology to deal with this issue by running regressions in "groups" rather than in a pooled analysis. We do not implement the Conley et al. (2018) methodology for our analyses, because the methodology is not feasible for our generalized difference-in-differences research design.

[20] Our sample covers laws that were passed between 2002 and 2014, and therefore, our sample includes observations between 2001 and 2015. As a result, firms in the three states that passed a data breach disclosure law in 2017 or 2018 are in our sample in the control group but never the treatment group.

[21] We identify a firm's historical business headquarters location from 10-K filings. We thank Bill McDonald for sharing these data.

TABLE 1

Cost of Equity Sample Selection

	Observations
Firm-year observations for U.S. firms from 2001 to 2015 with available historical business headquarters location (Compustat, 10-K filings)	91,478
Less: Not followed by analysts (I/B/E/S)	(24,591)
Less: Data missing for required variables	(37,705)
Less: Firms that change business headquarters state during our sample period (Bourveau et al. 2018; Conley et al. 2018)	(2,718)
Final cost of equity sample of firm-year observations	26,464
Total number of unique firms	4,280

fixed effects are nested within our state clusters (Conley et al. 2018; Bourveau, Lou, and Wang 2018). This results in 26,464 firm-year observations in our main sample.[22]

IV. RESULTS

Pearson Correlations and Descriptive Statistics

Tables 2 and 3 present the Pearson correlations and descriptive statistics for our sample, respectively. Consistent with Dhaliwal et al. (2016), the mean of *COE* (after subtracting the risk-free rate) is 5 percent. In general, the correlations and descriptive statistics are consistent with prior literature (e.g., Botosan and Plumlee 2005, Chen et al. 2011, Dhaliwal et al. 2016; Goh, Lee, Lim, and Shevlin 2016).

Main Analysis

The results of our primary analysis are presented in Table 4.[23] The coefficient on *LAW* is negative and significant ($p \leq 0.05$) and represents a 19-basis-point decrease in the cost of equity (or a 3.8 percent reduction relative to the sample mean). Given the coefficient on *LAW* is a difference-in-differences estimate, this provides strong evidence that suggests that firms experience an on-average decrease in the cost of equity after the passage of data breach disclosure laws. The results support our conjecture that the laws benefit shareholders by decreasing their risk.[24,25] We next probe this finding with sensitivity analyses and then provide evidence to support our assertion that the decrease in cost of equity is due to real actions managers take to reduce a firm's cyber-risk exposure.

Sensitivity Analyses

Sensitivity Analyses: Is Pre-Exposure to the Laws a Material Threat to Inferences?

As noted previously, we conduct all our analyses based on when a firm's home state passes a data breach disclosure law. Some firms may conduct business in states other than their home state and thus may be partly exposed to one of

[22] The state-level distribution of the sample is available in Table C1.

[23] Consistent with extant literature (e.g., Badolato et al. 2014; Ashraf et al. 2020), all p-values in our analyses are reported one-tailed when the directional prediction matches the coefficient estimate (if applicable) and two-tailed otherwise. Inferences remain consistent if instead we report all p-values as two-tailed.

[24] Results are consistent if we drop observations where the cost of equity calculation falls into a period between when the law is signed, but not yet effective (untabulated).

[25] As discussed in Section II, we focus on the primary disclosure characteristic of the laws rather than the secondary implementation differences. Anecdotally, two practitioners (both with over 20 years of experience, one as a cybersecurity professional in top management teams and the other as a cybersecurity lawyer) support our research design choice to not focus on the secondary implementation differences by noting that, in their experience, firms are generally aware of the disclosure obligation if the firm were to experience a breach but are generally unaware of the secondary implementation characteristics that vary across states. It is also conceptually unclear whether any of the secondary implementation characteristics should have a differential effect in our setting. Nonetheless, we study whether there is an incrementally stronger reduction in the cost of equity for state laws that possess any of the following secondary implementation characteristics: (1) imposing an explicit deadline by which firms must disclose after a breach has been discovered; (2) mandating disclosure of a breach, regardless of the results of a harm assessment; (3) mandating the firm also notify the attorney general or other state or credit agency of a data breach; and (4) explicitly stipulating a penalty for failure to disclose a breach. We find no statistically significant incremental effect (untabulated).

TABLE 2

Pearson Correlations for Cost of Equity Sample

		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
(1)	*COE*									
(2)	*SIZE*	**−0.17**								
(3)	*LEVERAGE*	**0.12**	**0.13**							
(4)	*ROA*	**−0.19**	**0.21**	**−0.13**						
(5)	*MTB*	**−0.18**	**0.18**	0.01	**0.24**					
(6)	*MOMENTUM*	**−0.05**	**0.02**	**−0.03**	**0.11**	**0.19**				
(7)	*VW_BETA*	**0.13**	−0.01	**−0.04**	**−0.06**	**0.03**	**0.08**			
(8)	*DISPERSION*	**0.25**	**−0.19**	**0.07**	**−0.28**	**−0.06**	**−0.08**	**0.15**		
(9)	*LT_GROWTH*	**0.11**	**−0.18**	**−0.11**	**−0.05**	**0.16**	**0.12**	**0.20**	**0.17**	
(10)	*RISK*	**0.14**	**−0.50**	**−0.11**	**−0.20**	0.00	**0.07**	**0.34**	**0.27**	**0.33**

This table presents Pearson correlations for the cost of equity sample. Bold values indicate significance at the 0.10 level or better.
All variables are defined in Appendix A.

TABLE 3

Descriptive Statistics for Cost of Equity Sample

Variables	Mean	Std. Dev.	25%	Median	75%
Dependent Variable					
COE	0.05	0.03	0.04	0.05	0.07
Control Variables					
SIZE ($millions)	6,199	15,855	488	1,337	4,031
LEVERAGE	0.18	0.18	0.02	0.14	0.30
ROA	0.05	0.07	0.01	0.04	0.08
MTB	3.07	3.40	1.47	2.22	3.61
MOMENTUM	0.18	0.47	−0.09	0.12	0.36
VW_BETA	1.12	0.56	0.73	1.05	1.43
DISPERSION	0.08	0.15	0.02	0.03	0.08
LT_GROWTH	0.15	0.10	0.10	0.14	0.18
RISK	0.34	0.17	0.22	0.30	0.43

This table presents descriptive statistics for the cost of equity sample. All continuous variables are Winsorized at the 1st and 99th percentiles.
All variables are defined in Appendix A.

the laws prior to their home state passing such a law. For firms with pre-exposure to a law, the coefficient on *LAW* is likely an underestimate, rather than an overestimate, of our treatment effect. Nonetheless, an explicit solution to address the pre-exposure concern is to identify each firm's state-by-state customers and employees and calculate our *LAW* variable accordingly. However, since firms do not disclose this information, we conduct eight sensitivity analyses that collectively suggest that pre-exposure to the laws is not a significant threat to inferences, all of which we tabulate in Panel A of Table 5.

First, following an approach similar to extant literature (e.g., García and Norli 2012; Bernile, Kumar, and Sulaeman 2015), we identify a firm's concentration in any particular state based on the number of times the firm mentions the state in its 10-K. For example, if firm *i* mentions New York nine times and New Jersey one time in its 10-K for year *t*, then firm *i* is 90 percent concentrated in New York and 10 percent in New Jersey. We then define a new variable, *LAW_WEIGHTED*, and rerun our *COE* analysis. *LAW_WEIGHTED* equals *LAW* times how concentrated firm *i* is in its home state in year *t*.[26] This variable measures how concentrated a firm is in its home state when that firm is subject

[26] We keep *LAW_WEIGHTED* constant for firms. So, for example, if Firm A is 80 percent concentrated in its home state of New York in 2005 (the year that New York passed its law), then we maintain that 80 percent concentration in all years after 2005 for Firm A, even if, for example, Firm A's 10-K in 2008 shows a 90 percent concentration in New York. Results are consistent if we allow *LAW_WEIGHTED* to vary temporally (untabulated).

TABLE 4

Main Analysis: Effect of Data Breach Disclosure Laws on Cost of Equity

		Dependent Variable: *COE*	
Independent Variables	**Pred.**	**(1)**	
Test Variable:			
LAW	−	−0.0019	**
[t-stat] (p-value)		[−2.14]	(0.019)
Control Variables:			
SIZE	−	−0.0044	***
LEVERAGE	+	0.0173	***
ROA	?	0.0009	
MTB	−	−0.0002	**
MOMENTUM	−	−0.0032	***
VW_BETA	+	0.0010	***
DISPERSION	+	0.0261	***
LT_GROWTH	+	0.0534	***
RISK	+	0.0083	***
Firm Fixed Effects		Yes	
Year Fixed Effects		Yes	
n/Adjusted R^2		26,464/65.23%	

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests when the sign of prediction matches the sign of coefficient estimate (if applicable) and two-tailed tests otherwise (Badolato et al. 2014; Ashraf et al. 2020).
This table presents the results of estimating the effect of *LAW* on *COE* (Equation (1)). The results are estimated using an OLS regression with robust standard errors clustered by state.
All variables are defined in Appendix A.

to the state's law. We tabulate this analysis in Column 1, where the coefficient on *LAW_WEIGHTED* is negative and significant ($p \leq 0.05$).[27]

Second, we restrict our sample to observations that mention their home state the most in their 10-K. Results remain consistent ($p \leq 0.01$; see Column 2). Third, we replace our test variable *LAW* with *LAW_HIGHEST*, which is calculated similar to *LAW*, except it loads as a one if firm *i*'s home state has passed a data breach disclosure law by firm *i*'s year *t* or if the state with the most mentions in firm *i*'s year *t*'s 10-K has passed a data breach disclosure law by firm *i*'s year *t*. Results remain consistent ($p \leq 0.05$; see Column 3).[28]

Fourth, some industries tend to have a more-geographically concentrated customer and employee base than others. In particular, Gervais and Jensen (2019) analyze trade inputs and outputs for 969 industries and calculate *SES* for each industry, a measure that captures the extent to which an industry's products are consumed locally relative to production. In effect, industries with low *SES* indicate firms where consumption of goods and services are close to production (e.g., dental offices), and industries with high *SES* indicate firms where consumption is not close to production (e.g., sugarcane mills). *SES* varies between 0 and 1. Relevant to our setting, arguably, firms with lower *SES* are more likely to have customers and employees based in their home state. Consequently, we rerun our main analysis but weight each firm by [one minus its *SES* score] (i.e., we run a weighted least squares regression where firms with lower *SES* scores are weighted more heavily). Results remain consistent ($p \leq 0.01$; see Column 4).

Fifth, smaller firms are arguably less likely to operate outside their home state, and it is more likely that their customer and employee base is concentrated locally. Consequently, we rerun our main analysis in a sample of firms that are smaller than $100 million in assets. Results remain consistent ($p \leq 0.05$; see Column 5). Sixth, if these smaller firms do operate in other states, arguably they are more likely to operate in a state that is physically close to their home state. Thus, in the sample of firms with $100 million in assets or less, we replace our test variable *LAW* with *LAW_BORDER*, which is calculated similar to *LAW*, except it loads as a one if firm *i*'s home state has passed a law by firm *i*'s year *t* or if

[27] The mean of *LAW_WEIGHTED* is 0.2627 (untabulated).
[28] The mean of *LAW_HIGHEST* is 0.7302 (untabulated).

TABLE 5

Sensitivity Analyses

Panel A: Is Pre-Exposure to the Laws a Threat to Inferences?

		Dependent Variable: *COE*							
Independent Variables	**Pred.**	**(1)**		**(2)**		**(3)**		**(4)**	
Test Variables:									
LAW_WEIGHTED	−	−0.0036	**						
[t-stat] (p-value)		[−2.37]	(0.011)						
LAW	−			−0.0024	***			−0.0019	***
[t-stat] (p-value)				[−2.92]	(≤0.01)			[−2.55]	(≤0.01)
LAW_HIGHEST	−					−0.0019	**		
[t-stat] (p-value)						[−2.06]	(0.023)		
Control Variables:									
SIZE	−	−0.0045	***	−0.0042	***	−0.0044	***	−0.0043	***
LEVERAGE	+	0.0177	***	0.0174	***	0.0173	***	0.0198	***
ROA	?	0.0012		−0.0005		0.0008		0.0008	
MTB	−	−0.0002	**	−0.0002	**	−0.0002	**	−0.0002	**
MOMENTUM	−	−0.0031	***	−0.0029	***	−0.0032	***	−0.0034	***
VW_BETA	+	0.0009	***	0.0012	***	0.0010	***	0.0010	***
DISPERSION	+	0.0263	***	0.0279	***	0.0262	***	0.0288	***
LT_GROWTH	+	0.0534	***	0.0586	***	0.0534	***	0.0519	***
RISK	+	0.0087	***	0.0067	***	0.0083	***	0.0112	***
Firm Fixed Effects		Yes		Yes		Yes		Yes	
Year Fixed Effects		Yes		Yes		Yes		Yes	
n/Adjusted R^2		26,464/65.32%		17,257/64.47%		26,464/65.23%		21,259/63.79%	
		(5)		(6)		(7)		(8)	
Test Variables:									
LAW	−	−0.0049	**						
[t-stat] (p-value)		[−1.74]	(0.045)						
LAW_BORDER	−			−0.0062	**				
[t-stat] (p-value)				[−1.80]	(0.039)				
LAW_CUSTOMER	−					−0.0018	**		
[t-stat] (p-value)						[−1.86]	(0.035)		
LAW_HIGHEST& CUSTOMER	−							−0.0020	**
[t-stat] (p-value)								[−2.00]	(0.025)
Control Variables:									
SIZE	−	−0.0052	**	−0.0052	**	−0.0044	***	−0.0044	***
LEVERAGE	+	−0.0058		−0.0074		0.0173	***	0.0173	***
ROA	?	−0.0248	***	−0.0248	***	0.0008		0.0008	
MTB	−	−0.0001		−0.0001		−0.0002	**	−0.0002	**
MOMENTUM	−	0.0003		0.0003		−0.0032	***	−0.0032	***
VW_BETA	+	0.0035	***	0.0036	***	0.0010	***	0.0010	***
DISPERSION	+	0.0036		0.0031		0.0262	***	0.0262	***
LT_GROWTH	+	0.0601	***	0.0603	***	0.0534	***	0.0534	***
RISK	+	−0.0072		−0.0069		0.0084	***	0.0084	***
Firm Fixed Effects		Yes		Yes		Yes		Yes	
Year Fixed Effects		Yes		Yes		Yes		Yes	
n/Adjusted R^2		1,016/60.06%		1,016/60.09%		26,464/65.23%		26,464/65.23%	

(continued on next page)

TABLE 5 (continued)

Panel B: Other Sensitivity Analyses

		Dependent Variable: *COE*							
Independent Variables	**Pred.**	**(1)**		**(2)**		**(3)**		**(4)**	
Test Variables:									
LAW	−	−0.0018	**	−0.0019	**	−0.0017	***		
[t-stat] (p-value)		[−2.21]	(0.016)	[−1.87]	(0.042)	[−2.40]	(≤0.01)		
PLACEBO_LAW	n.s.							0.0001	
[t-stat] (p-value)								[0.13]	(0.898)
Control Variables:									
SIZE	−	−0.0045	***	−0.0044	***	0.0077	***	−0.0044	***
LEVERAGE	+	0.0157	***	0.0173	***	−0.0138		0.0173	***
ROA	?	−0.0016		0.0009		−0.0255	***	0.0008	
MTB	−	−0.0002	**	−0.0002	**	−0.0002		−0.0002	**
MOMENTUM	−	−0.0030	***	−0.0032	***	−0.0014	*	−0.0032	***
VW_BETA	+	0.0007	**	0.0010	**	0.0025	*	0.0010	***
DISPERSION	+	0.0259	***	0.0261	***	0.0328	***	0.0261	***
LT_GROWTH	+	0.0540	***	0.0534	***	0.0543	***	0.0534	***
RISK	+	0.0083	***	0.0083	***	−0.0025		0.0082	***
Firm Fixed Effects		Yes		Yes		Yes		Yes	
Year Fixed Effects		No		Yes		Yes		Yes	
Industry-Year Fixed Effects		Yes		No		No		No	
n/Adjusted R^2		26,464/67.07%		26,464/65.23%		8,772/73.47%		26,464/65.21%	

		Dependent Variable: *COE_PEG*		**Dependent Variable: *COE_RI***		**Dependent Variable: *COE***	
		(5)		**(6)**		**(7)**	
Test Variables:							
LAW	−	−0.0026	***	−0.0014	**		
[t-stat] (p-value)		[−2.43]	(≤0.01)	[−2.33]	(0.012)		
LAW_GLBA&HIPAA	−					−0.0023	***
[t-stat] (p-value)						[−2.66]	(≤0.01)
Control Variables:							
SIZE	−	−0.0050	***	−0.0087	***	−0.0043	***
LEVERAGE	+	0.0119	***	0.0049	*	0.0173	***
ROA	?	−0.0349	***	−0.0598	***	0.0008	
MTB	−	0.0001		−0.0035	***	−0.0002	**
MOMENTUM	−	−0.0029	***	−0.0074	***	−0.0032	***
VW_BETA	+	0.0021	***	0.0010	**	0.0010	***
DISPERSION	+	0.0838	***	0.0106	***	0.0261	***
LT_GROWTH	+	0.0155	***	−0.0246	***	0.0534	***
RISK	+	0.0223	***	0.0142	***	0.0084	***
MISSING_DISPERSION	?			0.0047	***		
MISSING_LT_GROWTH	?			−0.0029	***		
Firm Fixed Effects		Yes		Yes		Yes	
Year Fixed Effects		Yes		Yes		Yes	
n/Adjusted R^2		26,464/56.79%		31,973/68.48%		26,464/65.24%	

(continued on next page)

any of the states that border firm *i*'s home state have passed a law by firm *i*'s year *t*. Results remain consistent ($p \leq 0.05$; see Column 6).[29]

[29] The mean of *LAW_BORDER* is 0.6604 (untabulated).

TABLE 5 (continued)

Panel C: Is the Parallel Trends Assumption Violated?

		Dependent Variable: *COE*			
Independent Variables	**Pred.**	**(1)**		**(2)**	
Test Variables:					
LAW t−1	n.s.	−0.0008		−0.0008	
[t-stat] (p-value)		[−0.93]	(0.357)	[−1.00]	(0.324)
LAW	−	−0.0025	**		
[t-stat] (p-value)		[−1.78]	(0.041)		
LAW t	−			−0.0022	*
[t-stat] (p-value)				[−1.46]	(0.075)
LAW t+1	−			−0.0028	**
[t-stat] (p-value)				[−2.29]	(0.013)
LAW t+2 … n	−			−0.0025	**
[t-stat] (p-value)				[−1.84]	(0.036)
Control Variables:					
SIZE	−	−0.0044	***	−0.0044	***
LEVERAGE	+	0.0173	***	0.0173	***
ROA	?	0.0008		0.0008	
MTB	−	−0.0002	**	−0.0002	**
MOMENTUM	−	−0.0032	***	−0.0032	***
VW_BETA	+	0.0010	***	0.0010	***
DISPERSION	+	0.0261	***	0.0261	***
LT_GROWTH	+	0.0535	***	0.0535	***
RISK	+	0.0084	***	0.0084	***
Firm Fixed Effects		Yes		Yes	
Year Fixed Effects		Yes		Yes	
n/Adjusted R^2		26,464/65.24%		26,464/65.23%	

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests when the sign of prediction matches the sign of coefficient estimate (if applicable) and two-tailed tests otherwise (Badolato et al. 2014; Ashraf et al. 2020).
This table presents sensitivity analyses. In Panel A, we analyze whether our inferences are robust to the concern that firms may be exposed to a data breach disclosure law prior to their home state passing such a law. In Panel B, we conduct several miscellaneous sensitivity analyses: in Column 1, we analyze whether our inferences can be attributed to industry-level time trends or time-varying characteristics; in Column 2, we double-cluster standard errors by state and by year, thereby mitigating concerns that within-year correlation is driving our inferences; in Column 3, we conduct our analysis using the stack regression research design to mitigate concerns raised by Goodman-Bacon (2021) regarding generalized difference-in-differences research designs (the model is fully saturated with indicators for each event-cohort); in Column 4, we run a placebo analysis to mitigate concerns about confounding events; in Column 5, we calculate implied cost of equity using the unmodified Easton methodology; in Column 6, we calculate implied cost of equity using predicted future earnings from cross-sectional residual income model; and in Column 7, we remeasure our main treatment variable to take into account the potential effects of GLBA and HIPPA. In Panel C, we analyze whether the parallel-trends assumption is reasonable in our setting. The results are estimated using an OLS regression with robust standard errors clustered by state in all regressions except by state and by year in Column 2 in Panel B and by state–cohort in Column 3 in Panel B.
All variables are defined in Appendix A.

Finally, we use FactSet to identify firms' known customers and rerun our main analysis with the variable *LAW_CUSTOMER*, which is calculated similar to *LAW*, except it loads as a one if firm *i*'s home state has passed a law by firm *i*'s year *t* or if the state of firm *i*'s customer has passed a law by firm *i*'s year *t*. We also rerun our analysis with *LAW_HIGHEST&CUSTOMER*, which loads as a one when either *LAW_HIGHEST* or *LAW_CUSTOMER* loads as a one. Results remain consistent for both sensitivity analyses ($p \leq 0.05$; see Columns 7 and 8).[30]

Sensitivity Analyses: Industry Concentration in States, Double Clustering, and Other Analyses

We conduct seven more sensitivity analyses, all of which we tabulate in Panel B of Table 5. First, certain industries may be concentrated in certain states and may face similar levels of cyber risk. Thus, if a major breach happens in an

[30] The mean of *LAW_CUSTOMER* is 0.7255 and *LAW_HIGHEST&CUSTOMER* is 0.7428 (untabulated).

industry, all firms in that industry might respond to that breach by taking real actions. If such breaches coincide with the passage of the data breach disclosure laws, it is possible that we incorrectly attribute this industry response to the laws. This is an unlikely explanation for our results, because we use a staggered adoption setting that exploits multiple events across multiple states. Nonetheless, we directly address this concern by replacing year fixed effects in our *COE* model with industry-year fixed effects. We tabulate this analysis in Column 1 and find the coefficient on *LAW* continues to be negative and significant ($p \leq 0.05$). In fact, the economic significance of *LAW* in this analysis is remarkably similar to our main analysis, which reinforces the notion that state-level industry concentration is not a threat to inferences in the first place.

Second, in our main analysis, we cluster by state because our treatment events are at the state level (Armstrong et al. 2012). To ensure that our results are robust to any within-year correlation, we rerun our main analysis while double clustering by state and by year. We find the coefficient on *LAW* continues to be negative and significant ($p \leq 0.05$; see Column (2)).

Third, Goodman-Bacon (2021) notes that early-treated observations in generalized difference-in-differences models serve as controls for later-treated observations and the observed coefficient estimate of the treatment variable may be biased when treatment effects are not homogenous across treatment events. There are two particular concerns: (1) that the observed coefficient estimate is in the opposite direction of the "true" effect and (2) even if the observed coefficient estimate is in the correct direction, it may still be economically overstated relative to the true effect. Given that our results suggest an on-average statistically significant negative coefficient, in our setting, the concern about this sort of bias is (1) that the true effect is actually positive or (2), barring the sign flip, that the true effect is economically less negative than what we observe. We address this concern in the following manner.

We first conduct a diagnostic analysis to determine whether biased coefficient estimate due to time-varying treatment effects is a legitimate concern in our setting. More specifically, we rerun our main analysis but, rather than including all treatment events at the same time, we stepwise add in each treatment event. We start by conducting an analysis of years 2001 to 2002 (first treatment event), then expand the analysis to 2001–2005 (first and second treatment event), and so on. We present this analysis in Table C2 and note three important takeaways, all of which suggest that a biased coefficient is not a material threat to inferences: (1) we observe that the treatment effect is statistically negative in the first estimation window ($p \leq 0.01$), where there are not any potentially problematic early-treated observations serving as controls for later-treated observations; (2) the treatment effect is statistically negative across all stepwise regressions ($p \leq 0.05$ or lower)—it is never statistically positive; and (3) although the coefficient estimate understandably fluctuates as we modify the sample, the coefficient estimate is not monotonically more negative as we expand our sample.

Even though the diagnostic analysis suggests that this particular concern does not exist in our sample, we go one step further and nonetheless apply a corrective technique suggested by Baker, Larcker, and Wang (2022) and Barrios (2021) and as implemented by Cengiz, Dube, Lindner, and Zipperer (2019)—the "stacked regression." More specifically, we first create event-cohort datasets restricted to two years around each treatment date (one year pre, one year post)—one dataset for the 2002 group that contains observations for 2001 and 2002, one for the 2005 group that contains observations for 2004 and 2005, and so on. In each event-cohort dataset, the treatment firms are the ones headquartered in the states that are treated for that cohort and the control firms are the firms that are untreated by that point. For example, for the 2005 dataset, the treatment firms are the firms in the states that passed the law in 2005 and the control firms are the firms in the states that have not passed the law by 2005 (and the firms in the states that passed the law prior to 2005 are excluded in the 2005 dataset). We then combine all event-cohort datasets into one dataset and rerun our analysis using the same model as our main analysis, except we now fully saturate the model with indicators for each event-cohort (Baker et al. 2022; Barrios 2021). As shown in Column 3 of Panel B in Table 5, the coefficient on *LAW* continues to be statistically negative ($p \leq 0.01$) and is economically similar to our main analysis.

Fourth, the staggered adoption of the laws and our difference-in-differences research design mitigate the likelihood that correlated omitted variables are the underlying driver of our results. However, a lingering concern may be that some unobserved macroeconomic changes happen to coincide with the passage of the laws and are the true drivers of the reduction in cost of equity. To directly address this concern, we follow Cornaggia, Mao, Tian, and Wolfe (2015) and randomly assign each observation a law-passage date of a different state but one that is not in the same year as the firm's home state. For example, if Firm A is based in New York, we randomly assign Firm A a law-passage date that is not in 2005. This enables us to retain the timing of these laws to test whether unobserved macroeconomic events drive our effect. In particular, major data breaches tend to attract significant national media attention, and therefore, one would expect that firms across the country—rather than firms in the specific state where the breach happened—would respond to the breach. Thus, if firms are really responding to data breaches that coincide with the passage of the laws rather than the laws themselves, then we should continue to observe a negative coefficient in this randomized-dates analysis. For this analysis, we replace *LAW* in our *COE* model with *PLACEBO_LAW* (equals 1 if firm *i*'s year *t* is after firm *i*'s

randomly assigned placebo date and 0 otherwise). Consistent with the notion that our effect is *not* driven by unobserved macroeconomic factors, we find *PLACEBO_LAW* is *not* statistically associated with *COE* (p = 0.90; see Column 4).

Fifth, we calculate cost of equity using an alternative methodology. There is considerable debate in the literature regarding "the best" proxy for implied cost of equity (e.g., Botosan and Plumlee 2005; Ogneva, Subramanyam, and Raghunandan 2007; Monahan and Easton 2010; Botosan, Plumlee, and Wen 2011; Dhaliwal et al. 2016). There is a stream of the literature that focuses on the methodology for computing a firm's cost of equity (e.g., Botosan et al. 2011). We do not speak to this body of evidence. Instead, we use cost of equity measures to answer an economic question of how data breach disclosure laws affect shareholder risk. Therefore, in our primary analyses, we follow extant literature, such as Hail and Leuz (2006) and Dhaliwal et al. (2016), and calculate cost of equity as the average of the measures by Claus and Thomas (2001); Gebhardt et al. (2001); modified Easton (2004); and Ohlson and Juettner-Nauroth (2005). To provide further evidence that our results are not sensitive to our choice of cost of equity proxy, we study the impact of the laws on a firm's cost of equity as proxied by Easton's (2004) unmodified PEG model (*COE_PEG*), a measure recommended by Botosan et al. (2011). We find *LAW* is significantly negatively associated with *COE_PEG* ($p \leq 0.01$; see Column 5).

Sixth, calculating implied cost of equity for a firm requires an expectation of the firm's future earnings. Consistent with a large extant literature (e.g., Dhaliwal et al. 2016), in our main analysis, we utilize analysts' forecasted earnings as a proxy for firms' expected future earnings when calculating *COE*. One concern with utilizing analyst forecasts is potential bias in those forecasts (e.g., Goh et al. 2016). There is no strong conceptual reason to expect analyst forecast bias to be correlated with our *LAW* variable, especially given our staggered adoption research design. Nonetheless, we address this concern by predicting future earnings based on historical accounting information as a proxy for expected future earnings (Hou, van Dijk, and Zhang 2012; Li and Mohanram 2014). Following the advice of Li and Mohanram (2014), we estimate firms' future earnings using the cross-sectional residual income model. We then use these data to calculate *COE_RI*, which is calculated the same as our main *COE* variable, except we use predicted earnings based on the cross-sectional residual income model as our expectation of firms' future earnings rather than analyst forecasts. The coefficient on *LAW* remains negative and significant ($p \leq 0.05$; see Column 6).

Finally, some firms may be required by GLBA and HIPAA to disclose the occurrence of a data breach. Ultimately, our research question is regarding whether consumer protection disclosure mandates can benefit shareholders; thus, our theory continues to hold—and our inferences remain the same—regardless of whether firms are responding to the mandatory disclosure requirements of GLBA and HIPAA or state-level data breach disclosure laws. Nonetheless, the presence of GLBA/HIPAA may be introducing some measurement error in our main variable *LAW*. We address this concern by rerunning our main analysis with *LAW_GLBA&HIPAA*, which equals 1 if firm *i*'s home state has passed a data breach disclosure law by firm *i*'s year *t*, if firm *i* is a finance firm and firm *i*'s year *t* is after GLBA instituted its breach disclosure requirement, or if firm *i* is a healthcare firm and firm *i*'s year *t* is after HIPAA instituted its breach disclosure requirement (0 otherwise). Inferences remain consistent ($p \leq 0.01$; see Column 7).

Sensitivity Analysis: Parallel Trends Assumption

A necessary condition for our difference-in-differences analysis is a valid parallel-trends assumption before the passage of the laws. Given that we exploit multiple law passages in our study, it is less likely that the parallel-trends assumption is violated. Nonetheless, consistent with extant literature (e.g., Bertrand and Mullainathan 2003 and Bourveau et al. 2018), for our final sensitivity analysis, we directly address the parallel trends concern by replacing the *LAW* variable in our main analysis with an indicator for the year before the passage of the law in firm *i*'s home state (year $t-1$ [*LAW t−1*]), an indicator for the year of (year *t* [*LAW t*]), an indicator for the year after (year $t+1$ [*LAW t+1*]), and a catchall indicator for all the years after that (years $t+2 \ldots n$ [*LAW t+2 … n*]). We present this analysis in two specifications: (1) *LAW t−1* in the same regression as our main variable *LAW* and (2) all four variables *LAW t−1*, *LAW t*, *LAW t+1*, and *LAW t+2 … n* in the same regression with our main variable *LAW* excluded (due to collinearity). An insignificant coefficient for year $t-1$ would suggest that the parallel-trends assumption is reasonable, which is exactly what we find in Panel C of Table 5 (p = 0.32 or higher).

Cross-Sectional Analyses of the Effect of Data Breach Disclosure Laws on Cost of Equity

We next provide evidence to bolster our argument that the observed effect on the cost of equity is through the real-effects mechanism. We argue that the laws prompt firms to make real investments in cybersecurity. It follows, then, that firms that already invested in cybersecurity prior to the laws should experience smaller benefits from the laws, if any, and this should manifest as a weaker (less negative) effect on the cost of equity. We examine this assertion in Table 6.

TABLE 6

Cross-Sectional Analysis: Effect of Data Breach Disclosure Laws on Cost of Equity for Firms that Already Took Real Actions to Manage Cyber Risk prior to the Laws

		Dependent Variable: *COE*			
		X = PRIOR_CYBER_CAPEX		*X = PRIOR_IT_OFFICER*	
Independent Variables	**Pred.**	**(1)**		**(2)**	
Test Variables:					
LAW	−	−0.0021	**	−0.0023	**
[t-stat] (p-value)		[−1.88]	(0.033)	[−2.28]	(0.014)
*LAW * X*	+	0.0036	***	0.0014	**
[t-stat] (p-value)		[2.84]	(≤0.01)	[1.69]	(0.048)
Control Variables:					
SIZE	−	−0.0040	***	−0.0040	***
LEVERAGE	+	0.0168	***	0.0176	***
ROA	?	−0.0052	**	−0.0007	
MTB	−	−0.0002	**	−0.0002	***
MOMENTUM	−	−0.0031	***	−0.0031	***
VW_BETA	+	0.0011	**	0.0009	*
DISPERSION	+	0.0249	***	0.0279	***
LT_GROWTH	+	0.0553	***	0.0545	***
RISK	+	0.0075	***	0.0081	***
Firm Fixed Effects		Yes		Yes	
Year Fixed Effects		Yes		Yes	
n/Adjusted R^2		16,879/61.96%		19,700/61.91%	
H_0: *LAW + LAW * X = 0*	?	0.0015		−0.0009	
[t-stat] (p-value)		[0.82]	(0.414)	[−0.70]	(0.489)

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests when the sign of prediction matches the sign of coefficient estimate (if applicable) and two-tailed tests otherwise (Badolato et al. 2014; Ashraf et al. 2020).
This table presents the results of studying the cross-sectional variation in the effect of *LAW* on *COE* for firms that already took real actions to manage cyber risk prior to the laws versus the rest of the sample, using two different proxies. The results are estimated using OLS regressions with robust standard errors clustered by state.
All variables are defined in Appendix A.

We use two proxies to identify firms that prioritized cybersecurity prior to the passage of the laws. First is *PRIOR_CYBER_CAPEX*, which equals 1 if firm *i* invested in cybersecurity during its pre-*LAW* period (0 otherwise). We identify investments in cybersecurity by counting the number of times a firm discusses cybersecurity software packages within ten words of keywords that indicate capital expenditure in the MD&A section of 10-K filings.[31] Firms are required to disclose material capital commitments in the MD&A section of 10-K filings (Securities and Exchange Commission (SEC) 2018b). Consequently, *PRIOR_CYBER_CAPEX* is a proxy of firms that invested in cybersecurity prior to the laws. Our second proxy is *PRIOR_IT_OFFICER* (equals 1 if firm *i* had a Chief Information Officer, Chief Technology Officer, Chief Information Security Officer, or Chief Security Officer on the top management team during its pre-*LAW* period [0 otherwise]). Arguably, firms with an IT officer on the top management team are more likely to have prioritized or invested in cybersecurity relative to other firms. We interact both *PRIOR_CYBER_CAPEX* and

[31] In other words, we search the MD&A section in the 10-Ks filed by a firm in its pre-*LAW* period. We count words in the MD&A that are associated with common types of cybersecurity software—antivirus, firewall, intrusion detection, logs or records management, and encryption—and also search for common enterprise cybersecurity software vendors, such as McAfee and Kaspersky (Beal 2010; Easttom 2012; AV-Comparatives 2021; AV-Test 2021). We search for these words within ten words of keywords that indicate investment, such as "install," "upgrade," and "invest." *PRIOR_CYBER_CAPEX* is defined in detail in Appendix A.

TABLE 7

Additional Analysis: Effect of Data Breach Disclosure Laws on Cybersecurity-Related Capital Expenditures

Independent Variables	Pred.	Dependent Variable: *CYBER_CAPEX* (1)	
Test Variable:			
LAW	+	0.0195	***
[t-stat] (p-value)		[3.18]	(≤0.01)
Control Variables:			
SIZE	+	0.0078	***
LEVERAGE	?	0.0082	
ROA	?	−0.0003	
MTB	?	−0.0002	*
FIRM_AGE	?	−0.0002	
INST_OWNERSHIP	?	−0.0181	
SEGMENTS	?	−0.0002	
FOREIGN	?	−0.0203	*
ACQUISITION	?	0.0062	
RESTRUCTURE	?	−0.0036	
10 K_LENGTH	+	0.0270	***
Firm Fixed Effects		Yes	
Year Fixed Effects		Yes	
n/Adjusted R^2		57,202/47.66%	

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests when the sign of prediction matches the sign of coefficient estimate (if applicable) and two-tailed tests otherwise (Badolato et al. 2014; Ashraf et al. 2020).
This table presents the results of estimating the effect of *LAW* on cybersecurity-related capital expenditures. The results are estimated using an OLS regression with robust standard errors clustered by state.
All variables are defined in Appendix A.

PRIOR_IT_OFFICER with *LAW* in Table 6.[32,33] As expected, the coefficient on *LAW* is significantly negative ($p \leq 0.05$) and the interaction terms are significantly *positive* ($p \leq 0.05$ or lower) in both columns. Taken together, these results provide support for the real-effects mechanism.

Additional Analyses: Evidence of Real Actions in Response to Data Breach Disclosure Laws

To provide further evidence that firms react to the laws by taking real actions to prioritize cybersecurity, we conduct two additional analyses. First, we study whether firms increase cybersecurity investments in response to the laws. For this analysis, the dependent variable is *CYBER_CAPEX* (the number of times firm *i* discusses cybersecurity software packages within ten words of keywords that indicate capital expenditure in the MD&A section of year *t*'s 10-K filing; the bag of words is the same as *PRIOR_CYBER_CAPEX* and is defined in detail in Appendix A). The results of this analysis are presented in Table 7. The coefficient on *LAW* is positive and significant ($p \leq 0.01$), suggesting that firms increase cybersecurity investments after the passage of the laws.

Second, we study whether firms are more likely to have an IT officer on the top management team after a state passes a data breach disclosure law. The results of this analysis are presented in Table 8, where the dependent variable in Columns 1–3 is the probability of either *IT_OFFICER* (equals 1 if a Chief Information Officer, Chief Technology Officer, Chief Information Security Officer, or Chief Security Officer is on the top management team for firm *i* in year *t*

[32] We exclude the "main effect" of *PRIOR_CYBER_CAPEX* and *PRIOR_IT_OFFICER* in Table 6, because the two variables are collinear with firm fixed effects since they do not vary over our sample.

[33] The sample sizes in Table 6 differ from our main analysis for two reasons. First, a firm must be present in the pre-*LAW* period in order to calculate *PRIOR_CYBER_CAPEX* and *PRIOR_IT_OFFICER*; firms without observations in the pre-*LAW* period are excluded from both columns. Second, we programmatically extract the MD&A section from 10-K filings in order to calculate *PRIOR_CYBER_CAPEX*, and we exclude observations in Column 1 for which we cannot extract the MD&A. Similarly, we require BoardEx coverage to calculate *PRIOR_IT_OFFICER*, and we exclude observations in Column 2 not covered by BoardEx.

TABLE 8

Additional Analysis: Effect of Data Breach Disclosure Laws on the Composition of the Top Management Team

		Dependent Variable					
Independent Variables	**Pred.**	**Pr(*IT_OFFICER* = 1) (1)**		**Pr(*CIO_CTO* = 1) (2)**		**Pr(*CISO_CSO* = 1) (3)**	
Test Variable:							
LAW	+	0.1532		0.1280		1.5093	***
[t-stat] (p-value)		[0.94]	(0.175)	[0.78]	(0.217)	[2.93]	(≤0.01)
Control Variables:							
SIZE	+	0.3550	***	0.3557	***	0.5225	**
LEVERAGE	?	0.3351		0.2645		0.4769	
ROA	?	−0.3276	***	−0.3353	***	−1.3587	***
MTB	?	−0.0070		−0.0062		−0.0273	
FIRM_AGE	?	0.1202		0.1267		0.0275	
INST_OWNERSHIP	?	0.5350	*	0.5166	*	0.3864	
SEGMENTS	?	0.0148		0.0189		0.1893	
FOREIGN	?	0.0477		0.0455		0.6046	
ACQUISITION	?	−0.0365		−0.0319		−0.5214	*
RESTRUCTURE	?	0.1336	**	0.1335	**	−0.1328	
Firm Fixed Effects		Yes		Yes		Yes	
Year Fixed Effects		Yes		Yes		Yes	
n/Pseudo R^2		20,572/12.30%		20,485/11.80%		1,545/34.43%	

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests when the sign of prediction matches the sign of coefficient estimate (if applicable) and two-tailed tests otherwise (Badolato et al. 2014; Ashraf et al. 2020).
This table presents the results of estimating the effect of *LAW* on the composition of the top management team. The results are estimated using conditional logistic regressions grouped by firm (i.e., firm fixed effects) with robust standard errors clustered by state. Sample sizes vary between the three columns because firms with no variation in the dependent variable are excluded in nonlinear models (Wooldridge 2010).
All variables are defined in Appendix A.

and 0 otherwise), *CIO_CTO* (just Chief Information Officer or Chief Technology Officer), or *CISO_CSO* (just Chief Information Security Officer or Chief Security Officer), respectively.[34] The coefficient on *LAW* is positive but insignificant in Columns 1 and 2 (p = 0.18 and 0.22, respectively). However, the coefficient on *LAW* is positive and significant in Column 3 (p ≤ 0.01). These results suggest that firms are more likely to have a CISO or CSO on the top management team after their home state passes a data breach disclosure law, but there is no significant association between the laws and having a CIO or CTO on the top management team. This result is not entirely surprising, as CISOs and CSOs are hired specifically for the purposes of cybersecurity, whereas CIOs and CTOs are responsible for cybersecurity but likely perform other roles as well and thus need not necessarily be directly associated with the laws.

Additional Analysis: Stock Price Reaction to Data Breach Disclosure Laws

Our tests so far have focused on how shareholder risk is affected by the laws. Decreases in shareholder risk should increase shareholder value, all else equal. However, to reduce the risk of a breach, firms also must make significant cash outlays to improve cybersecurity. All else equal, cash outlays reduce shareholder value. Thus, the net effect of the laws on shareholder value is unclear. We therefore study abnormal returns for firms around four key dates related to the laws

[34] Firm fixed effects in regular logit models may cause biased coefficients due to the incidental parameters problem (Greene 2004). Therefore, we run a conditional logit instead of a regular logit for this analysis. Conditional logit grouping upon firm is equivalent to a logit with firm fixed effects but without biased estimates (Allison 2012). The maximum likelihood for firms or years with no dependent-variable variation in our sample does not exist in a conditional logit grouped upon firm with year fixed effects; thus, those firms and years are dropped from the analysis (Wooldridge 2010). This is why the sample varies between the columns in Table 8. Results remain consistent if we run the analyses in a linear probability model (instead of a conditional logit), which does not impose the same dependent-variable requirement and, therefore, the sample in all columns retains firms and years that never possess an IT officer, CIO and CTO, or CISO and CSO, respectively (untabulated). Likewise, results remain consistent if we run the analysis in a rare event logistic model without firm or year fixed effects but with a time trend variable (untabulated); not including firm and year fixed effects ensures that the full sample is utilized in the analysis.

TABLE 9

Additional Analysis: Market Reaction to the Passage of Data Breach Disclosure Laws

Panel A: Univariate Analysis

Event	Pred.	*CAR*	
LAW_DATES	?	0.0009	***
[t-stat] (p-value)		[3.15]	(≤0.01)
LAW_PROPOSED	?	−0.0001	
[t-stat] (p-value)		[−0.26]	(0.794)
LAW_PASSED	?	0.0011	***
[t-stat] (p-value)		[2.72]	(≤0.01)
LAW_SIGNED	?	−0.0001	
[t-stat] (p-value)		[−1.47]	(0.141)
LAW_EFFECTIVE	?	0.0036	***
[t-stat] (p-value)		[5.34]	(≤0.01)

Panel B: Regression Analysis

		Dependent Variable: *CAR*			
Independent Variables	**Pred.**	**(1)**		**(2)**	
Test Variables:					
LAW_DATES	?	0.0010	**		
[t-stat] (p-value)		[2.49]	(0.016)		
LAW_PROPOSED	?			−0.0004	
[t-stat] (p-value)				[−0.32]	(0.749)
LAW_PASSED	?			0.0014	**
[t-stat] (p-value)				[2.34]	(0.023)
LAW_SIGNED	?			−0.0006	
[t-stat] (p-value)				[−0.53]	(0.601)
LAW_EFFECTIVE	?			0.0037	***
[t-stat] (p-value)				[2.79]	(≤0.01)
Firm Fixed Effects		Yes		Yes	
Year Fixed Effects		Yes		Yes	
n/Adjusted R^2		753,372/0.97%		753,372/0.97%	
H_0: *LAW_PROPOSED* + *LAW_PASSED* + *LAW_SIGNED* + *LAW_EFFECTIVE = 0*	?			0.0041	*
[t-stat] (p-value)				[1.74]	(0.088)

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests when the sign of prediction matches the sign of coefficient estimate (if applicable) and two-tailed tests otherwise (Badolato et al. 2014; Ashraf et al. 2020).
This table presents the results of estimating cumulative abnormal returns for firms around key dates related to the passage of data breach disclosure laws. Panel A is a univariate analysis using a sample of treatment observations. Panel B is an OLS regression analysis with robust standard errors clustered by state and by day using a sample of treatment and control observations.
All variables are defined in Appendix A.

in each state: (1) the date the data breach disclosure bill is first proposed in the state legislature (*LAW_PROPOSED*), (2) the date that this bill is passed in the state legislature (*LAW_PASSED*), (3) the date that this bill is signed into law (*LAW_SIGNED*), and (4) the date the law becomes effective (*LAW_EFFECTIVE*). We also capture all the dates in one variable with *LAW_DATES* (which loads as a one for all of the four dates).

We use Event Study by Wharton Research Data Services (WRDS) to calculate *CAR* (firm's daily raw return minus the Center for Research in Security Prices [CRSP] index for that day, summed over the [−1,1] event window) for

treatment and control firms on each of the dates. We first present univariate results (treatment firms only) and then regression results with firm and year fixed effects and double clustering by state and by day (in a pooled sample of treatment and control firms). The results of these analyses are presented in Table 9.[35] *CAR* is positive and significant for *LAW_DATES*, *LAW_PASSED*, and *LAW_EFFECTIVE* in both Panels A and B ($p \leq 0.05$ or lower). This suggests that, on average, investors view the laws favorably and the value-enhancing effect of reduced shareholder risk dominates the adverse cash-flow effect.

V. CONCLUSION

In this study, we examine whether shareholders can benefit from consumer protection disclosure mandates. Specifically, we analyze how state-level data breach disclosure laws impact shareholder risk, as proxied by firms' cost of equity capital. Although the intended purpose of these laws is to protect people whose personally identifiable information is leaked in data breaches, we argue that the laws help reduce shareholder risk by incentivizing managers to take real actions to reduce firms' exposure to cyber risk and the likelihood of experiencing a data breach.

We find evidence that suggests shareholders perceive the laws as reducing their risk: the cost of equity is lower after the passage of these laws, on average. We also provide evidence that supports our argument that cost of equity is reduced through real effects. Finally, we document positive abnormal returns for firms around key dates related to the passage of the laws in each state.

Our evidence is important for two reasons. First, cybersecurity is a growing economy-wide risk that multiple stakeholders are interested in mitigating (e.g., Securities and Exchange Commission (SEC) 2018a; PwC 2018). Thus, evidence on how data breach disclosure laws incentivize managers to take real actions to reduce firms' exposure to cyber risk is timely and relevant. Second, we answer a call for research by Leuz and Wysocki (2016), who contend that consumer protection disclosure mandates can serve a governance role. They note the importance of this evidence if disclosure mandates are to be used in lieu of regulation that explicitly prohibits undesirable behavior, and they highlight the need for this evidence in the literature. We provide such evidence.

Finally, our findings should be viewed with two important caveats. First, as we have discussed previously, the laws are written from the perspective of state residents rather than a firm's home state. Due to data limitations, in our analyses, we assign exposure to the laws based on firm's home state. This research design choice adds noise to our inferences. Second, we study the primary disclosure characteristic that is the focus of all these laws (Shaw 2010). However, as we have previously discussed, there are secondary implementation characteristics for the laws that differ between states. Our inferences on the effects of these secondary implementation characteristics are limited, and we encourage future research to pursue this line of inquiry.

REFERENCES

Abadie, A., S. Athey, G. W. Imbens, and J. M. Wooldridge. 2022. When should you adjust standard errors for clustering? *The Quarterly Journal of Economics* (forthcoming). https://doi.org/10.1093/qje/qjac038

Accenture. 2014. High performers in IT: Defined by digital. https://www.accenture.com/in-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_4/Accenture-HPIT-Research-Report-Defined-by-Digital.pdf

AIG. 2016. *Is cyber risk systemic?* https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyber-risk-systemic-final.pdf

Allison, P. D. 2012. *Logistic Regression Using SAS: Theory and Application*. Cary, NC: SAS Institute.

American Bankers Association. 2018. Data security & customer notification requirements for banks. https://web.archive.org/web/20170729034710/http:/www.aba.com/Tools/Function/Technology/Pages/datasecuritynotification.aspx

American Institute of Certified Public Accountants (AICPA). 2015. Security regains place as top technology priority for CPAs, North American survey finds. https://www.aicpa.org/press/pressreleases/2015/security-regains-place-as-top-technology-priority-for-cpas-north-american-survey-finds.html

Amir, E., S. Levi, and T. Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies* 23 (3): 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Armstrong, C. S., K. Balakrishnan, and D. Cohen. 2012. Corporate governance and the information environment: Evidence from state antitakeover laws. *Journal of Accounting and Economics* 53 (1–2): 185–204. https://doi.org/10.1016/j.jacceco.2011.06.005

[35] The number of observations in Panel B of Table 9 does not match the number of observations in our cost of equity tables, because the sample consists of both treatment and control observations for each event date for each state law. Put another way, Panel B is a pooled sample of event-firm observations where a firm may appear more than once (but only once per event date).

Ashbaugh-Skaife, H., D. W. Collins, W. R. Kinney, and R. Lafond. 2009. The effect of SOX internal control deficiencies on firm risk and cost of equity. *Journal of Accounting Research* 47 (1): 1–43. https://doi.org/10.1111/j.1475-679X.2008.00315.x

Ashraf, M. 2021a. Potentially unintended consequences of the SEC restricting managerial discretion: Evidence from peer data breaches and cyber risk factors. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3807487

Ashraf, M. 2021b. The market-wide implications of cyber risk: Evidence from customers and data breaches. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3802846

Ashraf, M. 2022. The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review* 97 (2): 1–24. https://doi.org/10.2308/TAR-2019-1033

Ashraf, M., P. N. Michas, and D. Russomanno. 2020. The impact of audit committee information technology expertise on the reliability and timeliness of financial reporting. *The Accounting Review* 95 (5): 23–56. https://doi.org/10.2308/accr-52622

AV-Comparatives. 2021. Main enterprise test-series vendors. https://www.av-comparatives.org/enterprise/vendors/

AV-Test. 2021. The best Windows antivirus software for business users. https://www.av-test.org/en/antivirus/business-windows-client/

Badolato, P. G., D. C. Donelson, and M. Ege. 2014. Audit committee financial expertise and earnings management: The role of status. *Journal of Accounting and Economics* 58 (2-3): 208–230. https://doi.org/10.1016/j.jacceco.2014.08.006

Baker & Hostetler LLP. 2017. Data breach charts. https://www.bakerlaw.com/files/Uploads/Documents/Data Breach documents/Data_Breach_Charts.pdf

Baker, L. B., and J. Finkle. 2011. Sony PlayStation suffers massive data breach. https://www.reuters.com/article/us-sony-stolden-data/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB20110427

Baker, A. C., D. F. Larcker, and C. C. Y. Wang. 2022. How much should we trust staggered difference-in-differences estimates? *Journal of Financial Economics* 144 (2): 370–395. https://doi.org/10.1016/j.jfineco.2022.01.004

Balakrishnan, K., M. B. Billings, B. Kelly, and A. Ljungqvist. 2014. Shaping liquidity: On the causal effects of voluntary disclosure. *The Journal of Finance* 69 (5): 2237–2278. https://doi.org/10.1111/jofi.12180

Barrios, J. M. 2021. Staggeringly problematic: A primer on staggered DiD for accounting researchers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794859

Beal, V. 2010. What is security software? https://www.webopedia.com/definitions/security-software/

Beckage. 2021. Upcoming national data breach notification legislation. https://www.beckage.com/breach-response/upcoming-national-data-breach-notification-legislation/

Bennear, L. S., and S. M. Olmstead. 2008. The impacts of the "right to know": Information disclosure and the violation of drinking water standards. *Journal of Environmental Economics and Management* 56 (2): 117–130. https://doi.org/10.1016/j.jeem.2008.03.002

Bernile, G., A. Kumar, and J. Sulaeman. 2015. Home away from home: Geography of information and local investors. *The Review of Financial Studies* 28 (7): 2009–2049. https://doi.org/10.1093/rfs/hhv004

Bertrand, M., and S. Mullainathan. 2003. Enjoying the quiet life? Corporate governance and managerial. *Journal of Political Economy* 111 (5): 1043–1075. https://doi.org/10.1086/376950

Biddle, G. C., and G. Hilary. 2006. Accounting quality and firm-level capital investment. *The Accounting Review* 81 (5): 963–982. https://doi.org/10.2308/accr.2006.81.5.963

Biddle, G. C., G. Hilary, and R. S. Verdi. 2009. How does financial reporting quality relate to investment efficiency? *Journal of Accounting and Economics* 48 (2-3): 112–131. https://doi.org/10.1016/j.jacceco.2009.09.001

Botosan, C. A., and M. A. Plumlee. 2005. Assessing alternative proxies for the expected risk premium. *The Accounting Review* 80 (1): 21–53. https://doi.org/10.2308/accr.2005.80.1.21

Botosan, C. A., M. Plumlee, and H. J. Wen. 2011. The relation between expected returns, realized returns, and firm risk characteristics. *Contemporary Accounting Research* 28 (4): 1085–1122. https://doi.org/10.1111/j.1911-3846.2011.01096.x

Bourveau, T., Y. Lou, and R. Wang. 2018. Shareholder litigation and corporate disclosure: Evidence from derivative lawsuits. *Journal of Accounting Research* 56 (3): 797–842. https://doi.org/10.1111/1475-679X.12191

Cameron, A. C., and D. L. Miller. 2015. A practitioner's guide to cluster-robust inference. *Journal of Human Resources* 50 (2): 317–372. https://doi.org/10.3368/jhr.50.2.317

Campbell, J. L., D. S. Dhaliwal, and W. C. Schwartz. 2012. Financing constraints and the cost of capital: Evidence from the funding of corporate pension plans. *Review of Financial Studies* 25 (3): 868–912. https://doi.org/10.1093/rfs/hhr119

Cengiz, D., A. Dube, A. Lindner, and B. Zipperer. 2019. The effect of minimum wages on low-wage jobs. *The Quarterly Journal of Economics* 134 (3): 1405–1454. https://doi.org/10.1093/qje/qjz014

Chen, K. C. W., Z. Chen, and K. C. J. Wei. 2011. Agency costs of free cash flow and the effect of shareholder rights on the implied cost of equity capital. *Journal of Financial and Quantitative Analysis* 46 (1): 171–207. https://doi.org/10.1017/S0022109010000591

Cho, Y. J. 2015. Segment disclosure transparency and internal capital market efficiency: Evidence from SFAS no. 131. *Journal of Accounting Research* 53 (4): 669–723. https://doi.org/10.1111/1475-679X.12089

Christensen, H. B., E. Floyd, and M. Maffett. 2020. The only prescription is transparency: The effect of charge-price-transparency regulation on healthcare prices. *Management Science* 66 (7): 2861–2882. https://doi.org/10.1287/mnsc.2019.3330

Christensen, H. B., E. Floyd, L. Y. Liu, and M. Maffett. 2017. The real effects of mandated information on social responsibility in financial reports: Evidence from mine-safety records. *Journal of Accounting and Economics* 64 (2-3): 284–304. https://doi.org/10.1016/j.jacceco.2017.08.001

Christensen, H. B., L. Hail, and C. Leuz. 2016. Capital-market effects of securities regulation: Prior conditions, implementation, and enforcement. *Review of Financial Studies* 29 (11): 2885–2924. https://doi.org/10.1093/rfs/hhw055

Cisco. 2017. *2017* Annual cyber security report. https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

Claus, J., and J. Thomas. 2001. Equity premia as low as three percent? Evidence from analysts' earnings forecasts for domestic and international stock markets. *The Journal of Finance* 56 (5): 1629–1666. https://doi.org/10.1111/0022-1082.00384

Clayton, C. J. 2018. SEC rulemaking over the past year, the road ahead and challenges posed by Brexit. https://www.sec.gov/news/speech/speech-clayton-120618

Conley, T., S. Gonçalves, and C. Hansen. 2018. Inference with dependent data in accounting and finance applications. *Journal of Accounting Research* 56: 1139-1203. https://doi.org/10.1111/1475-679X.12219

Cornaggia, J., Y. Mao, X. Tian, and B. Wolfe. 2015. Does banking competition affect innovation? *Journal of Financial Economics* 115 (1): 189–209. https://doi.org/10.1016/j.jfineco.2014.09.001

Crosignani, M., M. Macchiavelli, and A. F. Silva. 2021. Pirates without borders: The propagation of cyberattacks through firms' supply chains. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3664772

Cutler, D. M., R. S. Huckman, and M. B. Landrum. 2004. The role of information in medical markets: An analysis of publicly reported outcomes in cardiac surgery. *American Economic Review* 94 (2): 342–346. https://doi.org/10.1257/0002828041301993

Deloitte. 2015. COSO in the Cyber Age. https://www.coso.org/Shared%20Documents/COSO-in-the-Cyber-Age.pdf

Department of Health and Human Services. 2018. Breach notification rule. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Depository Trust and Clearing Corporation. 2018. The next crisis will be different. http://www.dtcc.com/~/media/Files/Downloads/WhitePapers/Systemic-Risk-White-Paper-962018.pdf

Dhaliwal, D., J. S. Judd, M. Serfling, and S. Shaikh. 2016. Customer concentration risk and the cost of equity capital. *Journal of Accounting and Economics* 61 (1): 23–48. https://doi.org/10.1016/j.jacceco.2015.03.005

Disparte, D. A., and L. Williams. 2017. Cyber security - the next systemic crisis? https://intpolicydigest.org/2017/04/12/cyber-security-next-systemic-crisis/

Donelson, D. C., J. M. McInnis, R. D. Mergenthaler, and Y. Yu. 2012. The timeliness of bad earnings news and litigation risk. *The Accounting Review* 87 (6): 1967–1991. https://doi.org/10.2308/accr-50221

Dranove, D., D. Kessler, M. McClellan, and M. Satterthwaite. 2003. Is more information better? The effects of "report cards" on health care providers. *Journal of Political Economy* 111 (3): 555–588. https://doi.org/10.1086/374180

Duffie, D., and J. Younger. 2019. Cyber runs. (Working paper). https://www.brookings.edu/wp-content/uploads/2019/06/WP51-Duffie-Younger-2.pdf

Easton, P. D. 2004. PE ratios, PEG ratios, and estimating the implied expected rate of return on equity capital. *The Accounting Review* 79 (1): 73–95. https://doi.org/10.2308/accr.2004.79.1.73

Easttom, W. C. 2012. *Computer Security Fundamentals*, 2nd edition. Indianapolis, IN: Pearson.

Ernst & Young. 2011. SEC staff issues guidance on cybersecurity disclosures. https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/assurance/accountinglink/ey-ttpcc0340-10-20-2011.pdf

Esterl, M. 2014. Coca-Cola: Stolen laptops had personal information of 74,000. https://www.wsj.com/articles/cocacola-stolen-laptops-had-personal-information-of-74000-1390596195

Faulkender, M., and J. Yang. 2013. Is disclosure an effective cleansing mechanism? The dynamics of compensation peer benchmarking. *The Review of Financial Studies* 26 (3): 806–839. https://doi.org/10.1093/rfs/hhs115

Field, L., M. Lowry, and S. Shu. 2005. Does disclosure deter or trigger litigation? *Journal of Accounting and Economics* 39 (3): 487–507. https://doi.org/10.1016/j.jacceco.2005.04.004

Florackis, C., C. Louca, R. Michaely, and M. Weber. 2022. Cybersecurity risk. *The Review of Financial Studies* (forthcoming). https://doi.org/10.1093/rfs/hhac024

Foley & Lardner LLP. 2019. State data breach notification laws. https://www.foley.com/en/-/media/18d91d3de9b94e98b526efa2e27c6faa.ashx

Fortune. 2017. Equifax hackers steal personal details of up to 143 million people. http://fortune.com/2017/09/07/equifax-hackers-personal-details-143-million-people/

Fu, F. 2009. Idiosyncratic risk and the cross-section of expected stock returns. *Journal of Financial Economics* 91 (1): 24–37. https://doi.org/10.1016/j.jfineco.2008.02.003

Gao, F., J. S. Wu, and J. Zimmerman. 2009. Unintended consequences of granting small firms exemptions from securities regulation: Evidence from the Sarbanes-Oxley Act. *Journal of Accounting Research* 47 (2): 459–506. https://doi.org/10.1111/j.1475-679X.2009.00319.x

García, D., and Ø. Norli. 2012. Geographic dispersion and stock returns. *Journal of Financial Economics* 106 (3): 547–565. https://doi.org/10.1016/j.jfineco.2012.06.007

Gatzlaff, K., and K. A. McCullough. 2010. The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review* 13 (1): 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Gay, S. 2017. Strategic news bundling and privacy breach disclosures. *Journal of Cybersecurity* 3 (2): 91–108. https://doi.org/10.1093/cybsec/tyx009

Gebhardt, W. R., C. M. C. Lee, and B. Swaminathan. 2001. Toward an implied cost of capital. *Journal of Accounting Research* 39 (1): 135–176. https://doi.org/10.1111/1475-679X.00007

Gervais, A., and J. B. Jensen. 2019. The tradability of services: Geographic concentration and trade costs. *Journal of International Economics* 118: 331–350. https://doi.org/10.1016/j.jinteco.2019.03.003

Gode, D., and P. Mohanram. 2003. Inferring the cost of capital using the Ohlson-Juettner model. *Review of Accounting Studies* 8 (4): 399–431. https://doi.org/10.1023/A:1027378728141

Goh, B. W., J. Lee, C. Y. Lim, and T. Shevlin. 2016. The effect of corporate tax avoidance on the cost of equity. *The Accounting Review* 91 (6): 1647–1670. https://doi.org/10.2308/accr-51432

Goodman, T. H., M. Neamtiu, N. Shroff, and H. D. White. 2014. Management forecast quality and capital investment decisions. *The Accounting Review* 89 (1): 331–365. https://doi.org/10.2308/accr-50575

Goodman-Bacon, A. 2021. Difference-in-differences with variation in treatment timing. *Journal of Econometrics* 225 (2): 254–277. https://doi.org/10.1016/j.jeconom.2021.03.014

Gordon, L. A. 2007. Incentives for improving cybersecurity in the private sector: A cost-benefit perspective. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.549.7147&rep=rep1&type=pdf (last accessed November 1, 2020).

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou. 2018. Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security* 9 (02): 133–153. https://doi.org/10.4236/jis.2018.92010

Granja, J. 2018. Disclosure regulation in the commercial banking industry: Lessons from the national banking era. *Journal of Accounting Research* 56 (1): 173–216. https://doi.org/10.1111/1475-679X.12193

Greene, W. 2004. The behaviour of the maximum likelihood estimator of limited dependent variable models in the presence of fixed effects. *The Econometrics Journal* 7 (1): 98–119. https://doi.org/10.1111/j.1368-423X.2004.00123.x

Hail, L., and C. Leuz. 2006. International differences in the cost of equity capital: Do legal institutions and securities regulation matter? *Journal of Accounting Research* 44 (3): 485–531. https://doi.org/10.1111/j.1475-679X.2006.00209.x

Healy, P. M., A. P. Hutton, and K. G. Palepu. 1999. Stock performance and intermediation changes surrounding sustained increases in disclosure. *Contemporary Accounting Research* 16 (3): 485–520. https://doi.org/10.1111/j.1911-3846.1999.tb00592.x

Hou, K., M. A. van Dijk, and Y. Zhang. 2012. The implied cost of capital: A new approach. *Journal of Accounting and Economics* 53 (3): 504–526. https://doi.org/10.1016/j.jacceco.2011.12.001

Huang, H. H., and C. Wang. 2021. Do banks price firms' data breaches? *The Accounting Review* 96 (3): 261–286. https://doi.org/10.2308/TAR-2018-0643

Identity Theft Resource Center. 2017. ITR data breach overview 2005 to 2017. https://www.idtheftcenter.org/images/breach/Overview20052017.pdf

Janakiraman, R., J. H. Lim, and R. Rishika. 2018. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing* 82 (2): 85–105. https://doi.org/10.1509/jm.16.0124

Jensen, M. C., and W. H. Meckling. 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics* 3 (4): 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Jiang, H., N. Khanna, Q. Yang, and J. Zhou. 2022. The cyber risk premium. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3637142

Jin, G. Z., and P. Leslie. 2003. The effect of information on product quality: Evidence from restaurant hygiene grade cards. *The Quarterly Journal of Economics* 118 (2): 409–451. https://doi.org/10.1162/003355303321675428

Jones Day. 2003. Technology commentaries: California raises the bar on data security and privacy. https://www.jonesday.com/California-Raises-the-Bar-on-Data-Security-and-Privacy-09-10-2003/

Jones, S. K. 2016. Untested cyber coverage remains "volatile," experts say. https://www.insurancejournal.com/news/national/2016/03/04/400878.htm

Jung, B., W. J. Lee, and D. P. Weber. 2014. Financial reporting quality and labor investment efficiency. *Contemporary Accounting Research* 31 (4): 1047–1076. https://doi.org/10.1111/1911-3846.12053

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139 (3): 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kolstad, J. T. 2013. Information and quality when motivation is intrinsic: Evidence from surgeon report cards. *American Economic Review* 103 (7): 2875–2910. https://doi.org/10.1257/aer.103.7.2875

Krebs, B. 2014. Target hackers broke in via HVAC company. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Laube, S., and R. Böhme. 2016. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* 2 (1): 29–41. https://doi.org/10.1093/cybsec/tyw002

Lawrence, A., M. Minutti-Meza, and D. Vyas. 2018. Is operational control risk informative of financial reporting deficiencies? *Auditing: A Journal of Practice & Theory* 37 (1): 139–165. https://doi.org/10.2308/ajpt-51784

Leuz, C., and P. D. Wysocki. 2016. The economics of disclosure and financial reporting regulation: Evidence and suggestions for future research. *Journal of Accounting Research* 54 (2): 525–622. https://doi.org/10.1111/1475-679X.12115

Leuz, C., and R. E. Verrecchia. 2000. The economic consequences of disclosure. *Journal of Accounting Research* 38: 91–124. https://doi.org/10.2307/2672910

Li, K. K., and P. Mohanram. 2014. Evaluating cross-sectional forecasting models for implied cost of capital. *Review of Accounting Studies* 19 (3): 1152–1185. https://doi.org/10.1007/s11142-014-9282-y

Lu, S. F. 2012. Multitasking, information disclosure, and product quality: Evidence from nursing homes. *Journal of Economics and Management Strategy* 21 (3): 673–705.

Malkiel, B. G., and Y. Xu. 2004. Idiosyncratic risk and security returns. (Working paper). https://personal.utdallas.edu/~yexiaoxu/IVOT_H.PDF

Mitnick, D. 2018. No more waiting: It's time for a federal data breach law in the U.S. https://www.accessnow.org/no-more-waiting-its-time-for-a-federal-data-breach-law-in-the-u-s/

Monahan, S. J., and P. D. Easton. 2010. Evaluating accounting-based measures of expected returns: Easton and Monahan and Botosan and Plumlee redux. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1592518

Ng, J. 2011. The effect of information quality on liquidity risk. *Journal of Accounting and Economics* 52 (2-3): 126–143. https://doi.org/10.1016/j.jacceco.2011.03.004

Ogneva, M., K. R. Subramanyam, and K. Raghunandan. 2007. Internal control weakness and cost of equity: Evidence from SOX section 404 disclosures. *The Accounting Review* 82 (5): 1255–1297. https://doi.org/10.2308/accr.2007.82.5.1255

Ohlson, J. A., and B. E. Juettner-Nauroth. 2005. Expected EPS and EPS growth as determinants of value. *Review of Accounting Studies* 10 (2-3): 349–365. https://doi.org/10.1007/s11142-005-1535-3

Online Trust Alliance. 2017. Cyber incident & breach trends report. https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

Perkins Coie. 2018. Security breach notification chart. https://www.perkinscoie.com/images/content/1/9/v2/197566/Security-Breach-Notification-Law-Chart-June-2018.pdf

Petersen, M. A. 2009. Estimating standard errors in finance panel data sets: Comparing approaches. *Review of Financial Studies* 22 (1): 435–480. https://doi.org/10.1093/rfs/hhn053

Pirinsky, C., and Q. Wang. 2006. Does corporate headquarters location matter for stock returns? *The Journal of Finance* 61 (4): 1991–2015. https://doi.org/10.1111/j.1540-6261.2006.00895.x

Ponemon Institute. 2017a. 2017 cost of data breach study: United States. https://www.ncsl.org/documents/taskforces/IBM_Ponemon2017CostofDataBreachStudy.pdf

Ponemon Institute. 2017b. The impact of data breaches on reputation & share value. https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf

Premkumar, G., and K. Ramamurthy. 1995. The role of interorganizational and organizational factors on the decision mode for adoption of interorganizational systems. *Decision Sciences* 26 (3): 303–336. https://doi.org/10.1111/j.1540-5915.1995.tb01431.x

PricewaterhouseCoopers (PwC). 2016. PwC data breach notification: 10 ways GDPR differs from US privacy model. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html

PricewaterhouseCoopers (PwC). 2018. 2018 global investor survey. https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf

Reeve, T. 2015. Cyber insurance not trusted by business, KPMG claims. https://web.archive.org/web/20190807044336/https://www.scmagazineuk.com/cyber-insurance-not-trusted-business-kpmg-claims/article/1478868

Richardson, V. J., R. E. Smith, and M. W. Watson. 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems* 33 (3): 227–265. https://doi.org/10.2308/isys-52379

Romanosky, S., R. Telang, and A. Acquisti. 2011. Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management* 30 (2): 256–286. https://doi.org/10.1002/pam.20567

Ronaldson, N. 2019. Hacking: The naked age cybercrime, clapper & standing, and the debate between state and federal data breach notification laws. *Northwestern Journal of Technology and Intellectual Property* 16 (4): 305–321.

Scholes, M., and J. Williams. 1977. Estimating betas from nonsynchronous data. *Journal of Financial Economics* 5 (3): 309–327. https://doi.org/10.1016/0304-405X(77)90041-1

Schwartz, P. M., and E. J. Janger. 2006. Notification of data security breaches. *Michigan Law Review* 913: 913–984.

Securities and Exchange Commission (SEC). 2011. CF Disclosure Guidance: Topic No. 2. Washington, DC: SEC.

Securities and Exchange Commission (SEC). 2018a. Commission statement and guidance on public company cybersecurity disclosures. https://federalregister.gov/d/2018-03858

Securities and Exchange Commission (SEC). 2018b. TOPIC 9 – management's discussion and analysis of financial position and results of operations (MD&A). https://www.sec.gov/corpfin/cf-manual/topic-9

Securities and Exchange Commission (SEC). 2022. Proposed rule: cybersecurity risk management, strategy, governance, and incident disclosure. https://www.sec.gov/rules/proposed/2022/33-11038.pdf

Shaw, A. 2010. Data breach: From notification to prevention using PCI DSS. *Columbia Journal of Law and Social Problems* 43 (4): 517–562.

Sheneman, A. 2017. Cybersecurity risk and the cost of debt. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3406217

Skinner, D. J. 1994. Why firms voluntarily disclose bad news. *Journal of Accounting Research* 32 (1): 38–60. https://doi.org/10.2307/2491386

Skinner, D. J. 1997. Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics* 23 (3): 249–282. https://doi.org/10.1016/S0165-4101(97)00010-4

Skinner, T. H. 2003. California's database breach notification security act: The first state breach notification law is not yet a suitable template for national identity theft legislation. *Richmond Journal of Law & Technology* 10 (1): 1–41.

Smith, T., J. Higgs, and R. Pinsker. 2019. Do auditors price breach risk in their audit fees? *Journal of Information Systems* 33 (2): 177–204. https://doi.org/10.2308/isys-52241

Spiegel, M. I., and X. Wang. 2005. Cross-sectional variation in stock returns: Liquidity and idiosyncratic risk. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=709781

Tomunen, T. 2021. Failure to share natural disaster risk. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3525731

U.S. Treasury Department. 2013. Report to the President on cybersecurity incentives pursuant to Executive Order 13636. https://www.treasury.gov/press-center/Documents/Supporting Analysis Treasury Report to the President on Cybersecurity Incentives_FINAL.pdf

Welker, M. 1995. Disclosure policy, information asymmetry, and liquidity in equity markets. *Contemporary Accounting Research* 11 (2): 801–827. https://doi.org/10.1111/j.1911-3846.1995.tb00467.x

Wooldridge, J. M. 2010. *Econometric Analysis of Cross Section and Panel Data*. Cambridge, MA: MIT Press.

World Economic Forum. 2016. Understanding systemic cyber risk: Global Agenda Council on Risk & Resilience. http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf

APPENDIX A

Variable Definitions

Variable		Definition (Data Source)
10K_LENGTH	=	natural log of the number of words in firm *i*'s 10-K filing for year *t* (10-K Filings).
ACQUISITION	=	1 if there is an acquisition by firm *i* in year *t* that contributes to sales or net income (Compustat).
CAR	=	firm *i*'s raw return on day *d* less the CRSP index on day *d*, aggregated over [−1,1] window relative to the date of event *j* (Event Study by WRDS).
CIO_CTO	=	1 if a Chief Information Officer or Chief Technology Officer is on the top management team for firm *i* in year *t* and 0 otherwise (BoardEx).
CISO_CSO	=	1 if a Chief Information Security Officer or Chief Security Officer is on the top management team for firm *i* in year *t* and 0 otherwise (BoardEx).
COE	=	implied cost of equity calculated following Dhaliwal et al. (2016), less the 10-year Treasury bonds rate; Dhaliwal et al. (2016) take the average of Claus and Thomas (2001); Gebhardt et al. (2001); Easton (2004); and Ohlson and Juettner-Nauroth (2005) (I/B/E/S, Federal Reserve Bank; see Appendix A in Dhaliwal et al. (2016) for more detail).
COE_PEG	=	implied cost of equity calculated following unmodified Easton (2004), less the 10-year Treasury bonds rate (I/B/E/S, Federal Reserve Bank).
COE_RI	=	implied cost of equity measure calculated the same as the *COE* variable, except we estimate future earnings using the cross-sectional residual income model (Li and Mohanram 2014) instead of analysts' forecasted future earnings (Compustat, Federal Reserve Bank).

(continued on next page)

APPENDIX A (continued)

Variable		Definition (Data Source)
CYBER_CAPEX	=	the number of times firm *i* discusses cybersecurity software packages within 10 words of keywords that indicate capital expenditure in the MD&A section of year *t*'s 10-K filing (10-K Filings). We search for the following terms, which represent types of cybersecurity software (including the appropriate different forms of these words) and major enterprise cybersecurity software vendors: access control, Acronis, Adaware, AhnLab, AI Max Dev Labs, Alibaba Security, anti-adware, anti-keylogger, anti-malware, anti-ransomware, anti-rootkit, anti-spyware, anti-subversion, anti-tamper, anti-virus, Antiy, Avast, AVG, Avira, Baidu, Barracuda, Bitdefender, BullGuard, Carbon Black, Check Point, Cheetah Mobile, Cisco, Clario, Comodo, computer security, CrowdStrike, cryptography, Cybereason, cybersecurity, Cylance, data security, diagnostic program, Elastic, Emsisoft, encryption, Endgame, endpoint security, Ensilo, eScan, ESET, FireEye, firewall, Fortinet, F-Secure, G Data, Immunet, information security, Intego, intrusion detection system, K7, Kaspersky, log management software, Lookout, MacKeeper, Malwarebytes, McAfee, Microsoft, network security, NOD32, Norton, Palo Alto Networks, Panda Security, PC Matic, PocketBits, Qihoo, Quick Heal, records management, SafeDNS, Saint Security, sandbox, Sangfor, Securion, security event management, security event management, security information and event management, security information management, SentinelOne, Seqrite, Sophos, SparkCognition, steganography, Symantec, Tencent, Total AV, Total Defense, Trend Micro, Trustport, Vipre, Webroot, and ZoneAlarm (Beal 2010; Easttom 2012; AV-Comparatives 2021; AV-Test 2021). We define keywords that indicate capital expenditure as the following (including the appropriate different forms of these words): acquire, adopt, advance, agree, boost, capital resource, capitalize, change, commitment, complete, configure, design, develop, enhance, expand, expenditure, expense, implement, improve, increase, initiate, install, integrate, invest, lease, modernize, modify, move, obtain, plan, project, purchase, replace, spend, upgrade, and use.
DISPERSION	=	the natural log of 1 plus the standard deviation of analysts' earnings per share forecasts scaled by consensus analyst forecasts for firm *i* in year *t*, calculated at the same time as *COE* (I/B/E/S).
FIRM_AGE	=	the age of firm *i* in years as of year *t* (Compustat).
FOREIGN	=	1 if firm *i* exhibits nonzero pretax foreign income in year *t* and 0 otherwise (Compustat).
INST_OWNERSHIP	=	the percentage of firm *i* owned by institutional investors in year *t* (Thomson Reuters).
IT_OFFICER	=	1 if a Chief Information Officer, Chief Technology Officer, Chief Information Security Officer, or Chief Security Officer is on the top management team for firm *i* in year *t* and 0 otherwise (BoardEx).
LAW	=	1 if the fiscal-year end of firm *i*'s year *t* is after firm *i*'s home state *j* (i.e., business headquarters state) has passed a data breach disclosure law (i.e., signed into law) and 0 otherwise (hand collected).
LAW t	=	1 if firm *i*'s year *t* is the year in which firm *i*'s home state *j* has passed a data breach disclosure law (i.e., signed into law) and 0 otherwise (hand collected).
LAW t+1	=	1 if firm *i*'s year *t* is the year after firm *i*'s home state *j* has passed a data breach disclosure law (i.e., signed into law) and 0 otherwise (hand collected).
LAW t+2 … n	=	1 if firm *i*'s year *t* is the second year or later after firm *i*'s home state *j* has passed a data breach–disclosure law (i.e., signed into law) and 0 otherwise (hand collected).
LAW t−1	=	1 if firm *i*'s year *t* is the year before firm *i*'s home state *j* has passed a data breach disclosure law (i.e., signed into law) and 0 otherwise (hand collected).
LAW_BORDER	=	1 if firm *i*'s home state has passed a data breach disclosure law by firm *i*'s year *t* or if any of the states that border firm *i*'s home state have passed a data breach disclosure law by firm *i*'s year *t* (hand collected).
LAW_CUSTOMER	=	1 if firm *i*'s home state has passed a data breach–disclosure law by firm *i*'s year *t or* if the state of firm *i*'s customer has passed a data breach disclosure law by firm *i*'s year *t* (hand collected; FactSet).
LAW_DATES	=	1 when any of the variables *LAW_PROPOSED*, *LAW_PASSED*, *LAW_SIGNED*, and *LAW_EFFECTIVE* equal 1 for firm *i* (0 otherwise) (hand collected).

(continued on next page)

APPENDIX A (continued)

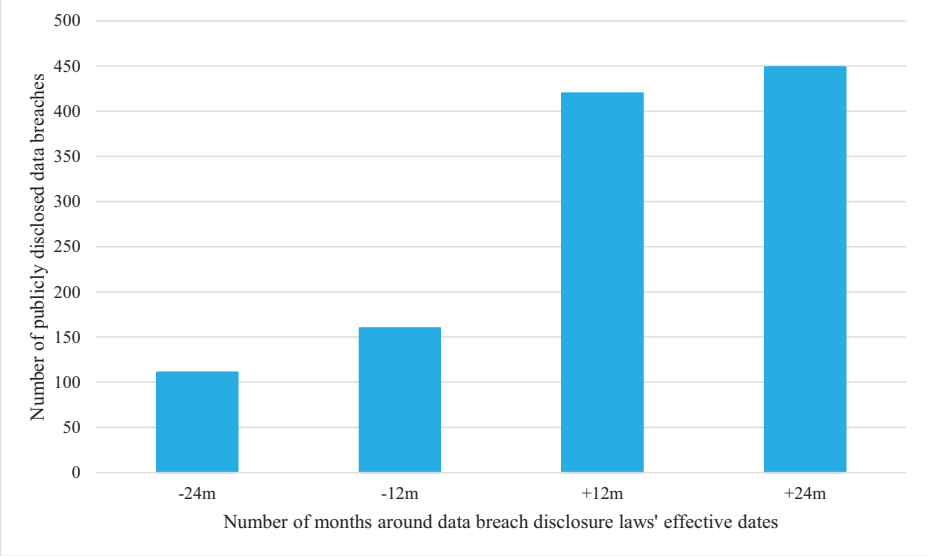
Variable		Definition (Data Source)
LAW_EFFECTIVE	=	1 if event *j* is when the data breach disclosure law becomes effective for firm *i* (0 otherwise) (hand collected).
LAW_GLBA&HIPAA	=	1 if firm *i*'s home state has passed a data breach disclosure law by firm *i*'s year *t or* if firm *i* is a finance firm and firm *i*'s year *t* is after GLBA instituted its breach-disclosure requirement *or* if firm *i* is a healthcare firm and firm *i*'s year *t* is after HIPAA instituted its breach-disclosure requirement and 0 otherwise (hand collected; Compustat).
LAW_HIGHEST	=	1 if firm *i*'s home state has passed a data breach disclosure law by firm *i*'s year *t* or if the state with the most mentions in firm *i*'s year *t*'s 10-K has passed a data breach disclosure law by firm *i*'s year *t* (hand collected; 10-K Filings).
LAW_HIGHEST&CUSTOMER	=	1 when any of the variables *LAW_HIGHEST* and *LAW_CUSTOMER* equal 1 (0 otherwise) (hand collected).
LAW_PASSED	=	1 if event *j* is when the data breach disclosure bill is passed by the state legislature for firm *i* (0 otherwise) (hand collected).
LAW_PROPOSED	=	1 if event *j* is when the data breach disclosure bill is proposed in the state legislature for firm *i* (0 otherwise) (hand collected).
LAW_SIGNED	=	1 if event *j* is when the data breach disclosure bill for the state is signed into law for firm *i* (0 otherwise) (hand collected).
LAW_WEIGHTED	=	*LAW* times how concentrated firm *i* is in its home state in year *t*, where a firm's home state concentration is calculated based on state mentions in the 10-K (hand collected; 10-K Filings).
LEVERAGE	=	long-term debt scaled by total assets for firm *i* in year *t* (Compustat).
LT_GROWTH	=	median analysts' long-term growth rate forecasts for firm *i* in year *t* (I/B/E/S).
MOMENTUM	=	raw stock return for firm *i* during year *t* (CRSP).
MTB	=	market capitalization scaled by book value for firm *i* in year *t* (Compustat).
PLACEBO_LAW	=	1 if firm *i*'s year *t* is after firm *i*'s randomly assigned placebo date and 0 otherwise (random).
PRIOR_CYBER_CAPEX	=	1 if firm *i* invested in cybersecurity during its pre-*LAW* period and 0 if firm *i* did not invest in cybersecurity during its pre-*LAW* period (10-K Filings). We identify cybersecurity investments by searching the MD&A sections in the 10-Ks filed by a firm in its pre-*LAW* period. Our methodology of searching the MD&A section is the same as *CYBER_CAPEX*.
PRIOR_IT_OFFICER	=	1 if firm *i* had a Chief Information Officer, Chief Technology Officer, Chief Information Security Officer, or Chief Security Officer on the top management team during its pre-*LAW* period; equals 0 if firm *i* did not have any of these executives during its pre-*LAW* period (BoardEx).
RESTRUCTURE	=	1 if firm *i* exhibited nonzero restructuring costs in year *t* and 0 otherwise (Compustat).
RISK	=	firm's idiosyncratic risk, measured as the annualized standard deviation of the residual from regressing daily returns for firm *i* over year *t* on contemporaneous value-weighted market returns; this variable is corrected for nonsynchronous trading following Scholes and Williams (1977) (CRSP).
ROA	=	net income scaled by total assets for firm *i* in year *t* (Compustat).
SEGMENTS	=	the number of geographic and business segments for firm *i* in year *t* (Compustat Segments).
SIZE	=	natural log of firm *i*'s market capitalization in year *t* (Compustat).
VW_BETA	=	the coefficient from regressing daily returns for firm *i* over year *t* on contemporaneous value-weighted market returns; this variable is corrected for nonsynchronous trading following Scholes and Williams (1977) (CRSP).

APPENDIX B

Data Breach Disclosure Laws and Number of Publicly Disclosed Data Breaches

FIGURE B1

Number of Publicly Disclosed Data Breaches before and after States' Data Breach–Disclosure Laws Are in Effect



This figure depicts the number of publicly disclosed data breaches in the periods before and after data breach disclosure laws are in effect, where $t = 0$ is the date a state's data breach–disclosure law is in effect. Incidents of publicly disclosed data breaches are obtained from the Privacy Rights Clearinghouse. Privacy Rights Clearinghouse provides both the date a data breach is first publicly known and the state where the data breach occurred.
(The full-color version is available online.)

APPENDIX C

TABLE C1

Distribution of Cost of Equity Sample by State

State	# of Obs.	Largest Industry
NAICS Industry/# of Obs.		
Alabama	164	finance and insurance/66
Alaska	18	information/14
Arizona	342	manufacturing/91
Arkansas	137	transportation and warehousing/31
California	4,404	manufacturing/1,700
Colorado	514	mining/114
Connecticut	626	manufacturing/187
Delaware	105	manufacturing/29
District of Columbia	103	utilities/26
Florida	1,058	finance and insurance/181

(continued on next page)

TABLE C1 (continued)

State	# of Obs.	Largest Industry
Georgia	692	finance and insurance/135
Hawaii	62	finance and insurance/25
Idaho	73	utilities/15
Illinois	1,385	finance and insurance/301
Indiana	399	finance and insurance/129
Iowa	160	finance and insurance/60
Kansas	151	finance and insurance/36
Kentucky	198	manufacturing/51
Louisiana	192	finance and insurance/39
Maine	32	manufacturing/15
Maryland	428	finance and insurance/132
Massachusetts	1,185	manufacturing/437
Michigan	580	manufacturing/247
Minnesota	814	manufacturing/241
Mississippi	91	finance and insurance/67
Missouri	542	manufacturing/125
Montana	30	finance and insurance/20
Nebraska	125	transportation and warehousing/31
Nevada	175	accommodation and food services/75
New Hampshire	60	retail trade/11
New Jersey	840	finance and insurance/207
New Mexico	34	utilities/14
New York	2,190	finance and insurance/801
North Carolina	545	finance and insurance/107
North Dakota	28	utilities/15
Ohio	1,028	manufacturing/224
Oklahoma	272	mining/98
Oregon	317	manufacturing/128
Pennsylvania	1,261	manufacturing/305
Puerto Rico	49	finance and insurance/46
Rhode Island	86	manufacturing/40
South Carolina	146	finance and insurance/50
South Dakota	40	utilities/17
Tennessee	456	health care and social assistance/80
Texas	2,421	mining/502
Utah	176	manufacturing/40
Vermont	41	manufacturing/16
Virgin Islands	1	real estate rental and leasing/1
Virginia	679	finance and insurance/161
Washington	542	manufacturing/122
West Virginia	46	finance and insurance/39
Wisconsin	417	manufacturing/213
Wyoming	4	mining/4

TABLE C2

Diagnostic Analysis to Determine Whether the Concerns Raised by Goodman-Bacon (2021) are a Material Threat to Inferences

Independent Variables	Pred.	Dependent Variable: *COE*					
		Treatment Events: 2002 (1)		Treatment Events: 2002 and 2005 (2)		Treatment Events: 2002, 2005, and 2006 (3)	
Test Variable:							
LAW	−	−0.0027	***	−0.0014	***	−0.0017	***
[t-stat] (p-value)		[−3.95]	(≤0.01)	[−2.70]	(≤0.01)	[−2.88]	(≤0.01)
Control Variables:							
SIZE	−	0.0072	***	0.0010		0.0002	
LEVERAGE	+	−0.0131	*	0.0087	**	0.0107	***
ROA	?	−0.0225	***	0.0012		−0.0053	
MTB	−	−0.0003		−0.0004	***	−0.0003	**
MOMENTUM	−	−0.0022	***	−0.0015	***	−0.0015	***
VW_BETA	+	0.0022	*	0.0003		−0.0001	
DISPERSION	+	0.0358	***	0.0229	***	0.0227	***
LT_GROWTH	+	0.0619	***	0.0681	***	0.0594	***
RISK	+	−0.0049		0.0078	***	0.0079	***
Firm Fixed Effects		Yes		Yes		Yes	
Year Fixed Effects		Yes		Yes		Yes	
n/Adjusted R^2		3,419/74.89%		9,319/66.88%		11,288/65.31%	

		Treatment Events: 2002, 2005, 2006, and 2007 (4)		Treatment Events: 2002, 2005, 2006, 2007, and 2008 (5)		Treatment Events: 2002, 2005, 2006, 2007, 2008, and 2009 (6)	
Test Variable:							
LAW	−	−0.0016	***	−0.0013	**	−0.0016	***
[t-stat] (p-value)		[−2.42]	(≤0.01)	[−2.08]	(0.022)	[−2.48]	(≤0.01)
Control Variables:							
SIZE	−	−0.0026	***	−0.0031	***	−0.0031	***
LEVERAGE	+	0.0150	***	0.0164	***	0.0160	***
ROA	?	−0.0022		−0.0007		−0.0024	
MTB	−	−0.0002	*	−0.0001	*	−0.0001	*
MOMENTUM	−	−0.0019	***	−0.0014	**	−0.0019	***
VW_BETA	+	0.0010	**	0.0014	***	0.0012	***
DISPERSION	+	0.0303	***	0.0336	***	0.0310	***
LT_GROWTH	+	0.0561	***	0.0552	***	0.0576	***
RISK	+	0.0104	***	0.0138	***	0.0099	***
Firm Fixed Effects		Yes		Yes		Yes	
Year Fixed Effects		Yes		Yes		Yes	
n/Adjusted R^2		13,103/61.85%		14,504/61.25%		16,209/62.02%	

(continued on next page)

TABLE C2 (continued)

		Treatment Events: 2002, 2005, 2006, 2007, 2008, 2009, and 2010 (7)		Treatment Events: 2002, 2005, 2006, 2007, 2008, 2009, 2010, and 2014 (8)	
Test Variable:					
LAW	−	−0.0016	***	−0.0019	**
[t-stat] (p-value)		[−2.47]	(≤0.01)	[−2.14]	(0.019)
Control Variables:					
SIZE	−	−0.0039	***	−0.0044	***
LEVERAGE	+	0.0152	***	0.0173	***
ROA	?	−0.0014		0.0009	
MTB	−	−0.0001	*	−0.0002	**
MOMENTUM	−	−0.0019	***	−0.0032	***
VW_BETA	+	0.0012	***	0.0010	***
DISPERSION	+	0.0289	***	0.0261	***
LT_GROWTH	+	0.0598	***	0.0534	***
RISK	+	0.0099	***	0.0083	***
Firm Fixed Effects		Yes		Yes	
Year Fixed Effects		Yes		Yes	
n/Adjusted R^2		17,950/63.22%		26,464/65.23%	

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests when the sign of prediction matches the sign of coefficient estimate (if applicable) and two-tailed tests otherwise (Badolato et al. 2014; Ashraf et al. 2020).
This table presents the results of estimating the effect of *LAW* on *COE*, in a stepwise manner (i.e., we stepwise add in each treatment event; we start by conducting an analysis of years 2001 to 2002 [first treatment event], then expand the analysis to 2001–2005 [first and second treatment event], then to 2001–2006 [first, second, and third treatment event], and so on). The results are estimated using an OLS regression with robust standard errors clustered by state.
All variables are defined in Appendix A.