KeAi
CHINESE ROOTS
GLOBAL IMPACT

Available online at www.sciencedirect.com

ScienceDirect

The Journal of Finance and Data Science 8 (2022) 202–213

http://www.keaipublishing.com/en/journals/jfds/

Are there trade-offs with mandating timely disclosure of cybersecurity incidents? Evidence from state-level data breach disclosure laws

Musaib Ashraf, John (Xuefeng) Jiang*, Isabel Yanyan Wang

Michigan State University, Business Complex 632 Bogue St Rm N270, East Lansing, MI 48824, USA

Received 18 August 2022; accepted 29 August 2022
Available online 9 September 2022

Abstract

On March 23, 2022, the SEC proposed that firms publicly disclose their cybersecurity incidents within four days of discovery. In the U.S., state-level data breach disclosure laws require firms to disclose the occurrence of a data breach, with some mandating disclosure within a deadline while others do not. Exploiting this state-level variation in disclosure deadlines, we find that, when facing a deadline, firms disclose a data breach 90 percent faster but are 58 percent less likely to disclose breach details. Investors respond negatively to delayed breach disclosures but are forgiving of a delay when it is used to gather more breach details. Our study highlights the trade-offs of mandating a disclosure deadline for cybersecurity incidents.

JEL classification: K24; M28; M40

Keywords: Cybersecurity; Data breach; Disclosure; Regulation; Disclosure deadline; U.S. Securities and Exchange Commission (SEC); Data breach disclosure laws; Information technology

1. Introduction

Cybersecurity risks "pose grave threats to investors [and] our capital markets" (ref. [1]; p.1), with firms facing a rapidly evolving cybersecurity landscape.[2] Accordingly, 4,446 CEOs surveyed across 89 countries in 2021 view cyber risks as *the* top threat to company growth (PwC 2022). Echoing the importance of cybersecurity, the U.S. Congress recently passed the Strengthening American Cybersecurity Act of 2022, requiring critical infrastructure companies to provide private disclosure of cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours. The U.S. Securities and Exchange Commission (SEC) has also emphasized policymaking related to cybersecurity. For example, former SEC Chairman Jay Clayton noted that "it is important that investors are sufficiently informed about the material cybersecurity risks affecting the companies in which they invest" (ref. [3]; p.8).

* *Corresponding author.*
E-mail address: jiangj@msu.edu (J.(X. Jiang).
Peer review under responsibility of China Science Publishing & Media Ltd.

https://doi.org/10.1016/j.jfds.2022.08.001

In its latest round of policymaking and prompted by the need to better inform investors on firms' cybersecurity risk exposure, on March 23, 2022, the SEC proposed a new rule that requires public firms to disclose material cybersecurity incidents publicly within four business days of discovery through an 8-K filing.[4] In contrast, the SEC's existing guidance on cybersecurity disclosures only requires public companies to "provide timely and ongoing information" in periodic filings such as the 10-K and 10-Q,[1] without imposing any deadline for when firms must disclose material cybersecurity incidents. In this study, we examine the potential trade-offs with mandating a disclosure deadline for cybersecurity incidents, using the setting of state-level data breach disclosure laws. Given the increasing emphasis on cybersecurity-related disclosures, understanding the trade-offs with requiring a disclosure deadline can offer insight that may affect the direction of policymaking.

Two opposing arguments lead to competing predictions about the effect of a disclosure deadline on disclosure outcomes. On the one hand, mandating a deadline could highlight the importance of disclosure and encourage *more* timely disclosure of cybersecurity incidents (relative to allowing managers to decide on their own when to disclose). Timeliness is the primary rationale behind the SEC's proposal, noting that "existing reporting may not be sufficiently timely" and that the proposal will result in "[more] timely and relevant disclosure to investors and other market participants" (ref. [4]; p.20, p.21). On the other hand, a disclosure deadline may lead to *less* timely disclosures because firms may delay disclosures by using the deadline under the law as a safe harbor. This argument stems from the notion that managers may gravitate to and manage around bright-line thresholds (e.g., ref. [5]). For example, a firm that is capable of disclosing a data breach within 30 days may end up taking the whole 60-day period allowed under the law.

Relatedly, firms face a trade-off between the timeliness and quality of the disclosure of cybersecurity incidents. It takes time to fully understand cybersecurity incidents: what happened, how it happened, who was impacted, and how to remediate. This process is complicated and time consuming. Explicitly requiring firms to disclose a cybersecurity incident within a certain timeline may limit their ability to properly investigate and respond to the incident.[6,7] Even if a deadline leads to faster disclosures, firms may have to sacrifice the quality of the disclosures given a lack of time to gather full or reliable information, especially if the information could have legal implications. Anecdotally, in an unstructured interview, a national law firm partner with specialization and extensive experience in cybersecurity laws noted to us that firms often face this timeliness and quality trade-off because sufficient time is necessary to fully investigate cybersecurity incidents.

We empirically test these arguments in a generalized difference-in-differences research design that utilizes variations among state-level data breach disclosure laws. Data breach disclosure laws are U.S. state-level consumer protection disclosure mandates that dictate firms must disclose the occurrence of a data breach to people whose personal information is leaked in a breach.[8] While these laws mandate private disclosure to data breach victims to help protect them from identity theft, the laws result in de facto public disclosures because news about a breach is difficult to contain once it is disclosed to thousands (potentially, millions) of people.[9] All states in the U.S. have passed a data breach disclosure law over the past two decades, and the laws are similar because they all require disclosure to data breach victims. However, some state laws mandate that firms disclose the occurrence of a data breach within a deadline – similar to the rule currently proposed by the SEC – while others have no such deadline. Importantly, these state-level mandates were implemented in a staggered manner at different times, allowing us to exploit this staggered variation at the state level to study the timeliness and information content effects of mandated disclosure deadlines.

Using a sample of data breach incidents that occurred between 2010 and 2020, we document two main findings. First, we find that treatment firms (ones that are mandated by a state law to disclose the occurrence of a data breach by an explicit deadline) report the occurrence of a breach 89.82 percent *faster* than control firms. This result is consistent with the SEC's motivation for imposing a mandatory disclosure deadline[4] and is *in*consistent with literature that suggests bright-line thresholds allow firms to manage around them (e.g., ref.[5]).[1] Second, we find that treatment firms are 57.71 percent *less* likely to disclose details about the breach compared to control firms. This result suggests that there is a trade-off between disclosure timeliness and disclosure quality, highlighting a possible unintended consequence of mandating a deadline for cybersecurity incident disclosures.

We conduct two sensitivity analyses to ensure the robustness of our inferences. First, we rerun our main analysis in a 'stacked regression' design to mitigate the concern regarding potentially biased coefficients in generalized difference-

[1] Descriptively, very few firms in our sample disclose the occurrence of a data breach within four days of discovery, suggesting that, while having a disclosure deadline may result in faster disclosures, the SEC (2022)'s (ref. [4]) four-day threshold may not be feasible or, alternatively, may require firms to invest significant resources to meet the new deadline.

in-differences regression analyses.[10] Second, we rerun our main analysis in a 'dynamic' generalized difference-in-differences model to mitigate concerns regarding violation of the parallel trends assumption. Our inferences continue to hold.

Although our main analyses suggest that there is a timeliness and information content trade-off with having a disclosure deadline, investors may still benefit from a disclosure deadline if they value timeliness more than information content. To test this notion, our additional analysis examines the abnormal returns around the disclosure date of a data breach. We find that firms that delay a data breach disclosure incur stronger negative market reactions. However, investors are more forgiving of a delay if firms provide breach details in the disclosure, suggesting that investors are willing to tolerate a disclosure delay if the delay is (or, appears to be) driven by the need to gather more information about the breach. Interestingly, we find that investors respond negatively to disclosures that contain breach details but are released rapidly after data breach discovery, implying that investors seem concerned about inaccurate or misleading information when firms do not take time to verify the details before disclosing a data breach.

Our study makes several important contributions to the literature. First, we provide evidence regarding the trade-off between timeliness and quality when mandating a disclosure deadline for cybersecurity incidents, such as data breaches. Our evidence should be informative to the SEC in finalizing their current proposal that mandates a disclosure deadline for material cybersecurity incidents within four business days of discovery.[4] The SEC specifically notes its inability "to quantify the potential benefit to investors and other market participants… under the proposed amendments" (ref. [4], p. 68). Our empirical evidence sheds light on the potential magnitude of increased timeliness using data breach disclosures under state-level laws that vary by the presence of a disclosure deadline. Specifically, our findings suggest the SEC may consider utilizing a two-step disclosure regime, wherein firms are required to make rapid skeleton disclosure of the occurrence of a data breach and must follow up with a more detailed disclosure within a more generous deadline.

We also contribute to the nascent literature on the effects of data breach disclosure laws.[8] provide evidence that identity theft decreases in the U.S. after individual states pass data breach disclosure laws, consistent with the primary intention of these laws.[9] study the ex-ante effects of data breach disclosure laws and document a reduced cost of equity. We build upon this literature by expanding our understanding of the specific characteristics (i.e., timeliness and quality) of ex-post disclosures that firms provide after a data breach.

Finally, our study adds to the literature that examines data breaches specifically and cybersecurity incidents in general. Cybersecurity incidents are a growing economy-wide risk. Firms, shareholders, and regulators are all interested in managing this risk[11] (PwC 2022). While there is some debate about whether data breaches materially impact firms (e.g., refs.[12,13]), a stream of studies find data breaches to be costly for firms (e.g.,[14,15]). We extend this literature by providing a unique insight because our evidence suggests that both the timeliness and quality of a data breach disclosure can impact investors' responses.

2. Research design, sample selection, and data

2.1. Research design

To test our research question on the timeliness and quality of data breach disclosures, we estimate the following ordinary least squares model:

$$DAYS\_TO\_DISCLOSE_j \text{ or } BREACH\_DETAILS_J = \beta 1 DISCLOSURE\_DEADLINEj + \Sigma \beta n Controls\ Variables + Fixed\ Effects\ (State_k,\ Industry_{d,}\ Year_t) + e_j \quad (1)$$

where j indexes data breach incident, i indexes firm, k indexes state, d indexes industry, and t indexes year. Our dependent variables are *DAYS_TO_DISCLOSE* and *BREACH_DETAILS*. *DAYS_TO_DISCLOSE* is calculated as the natural log of one plus the number of days between firm i's data breach incident j's discovery date and disclosure date. *BREACH_DETAILS* equals one if firm i's disclosure about data breach incident j contains details about how the breach happened and what information was leaked, and zero otherwise. Our main variable, *DISCLOSURE_DEADLINE*, equals one if firm i's home state k has signed into law a disclosure deadline (i.e., the treatment) on or before the discovery date of data breach incident j, and zero otherwise.

Table 1
Chronology of states mandating a disclosure deadline of data breach incidents.

Treatment State	Deadline (Days)	Treatment Date
Alabama	45	3/28/2018
Arizona	45	4/11/2018
Colorado	30	5/29/2018
Connecticut	90	6/11/2015
Delaware	60	8/17/2017
Florida	45	6/20/2005
Florida	30	6/20/2014
Maine	7	5/19/2009
Maine	30	6/28/2019
Maryland	45	5/4/2017
New Mexico	45	4/6/2017
Ohio	45	12/29/2006
Oregon	45	6/10/2015
Rhode Island	45	6/26/2015
South Dakota	60	3/21/2018
Tennessee	45	4/4/2017
Texas	60	6/14/2019
Vermont	45	5/8/2012
Washington	45	4/23/2015
Washington	30	5/7/2019
Wisconsin	45	3/16/2006

Data breach disclosure laws are crafted from the viewpoint of the state resident whose information is leaked rather than the home state of the breached firm. In other words, firms are exposed to the laws based on the states where they have operations, not just their home state. Due to data limitations, we cannot observe firms' state-by-state operations. Thus, we follow prior literature[9,15,16] and assign our main variable 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., ref.[17]). Therefore, firms should conceptually respond to a disclosure deadline mandate passed in their home state. However, to the extent that firms may have exposure outside their home state and respond to other states' disclosure deadline mandates prior to their home state passing such a mandate, our measured response will capture the lower bound of the total effect of these mandates, because the impact on our dependent variables should be weaker if a firm started responding to the mandates prior to the firm's home state passing its own mandate. Put another way, the noise in our treatment variable likely biases findings towards zero, not away from zero. Main results remain consistent if we drop retail firms (untabulated).

Table 1 lists the treatment states and associated treatment dates, which suggests that revisions to data breach disclosure laws (which were generally passed in their initial forms prior to 2010) tend to include a disclosure deadline.[2] For the analysis of disclosure timeliness, a negative coefficient on *DISCLOSURE_DEADLINE* suggests that firms disclose more quickly when mandated to disclose within a deadline; a positive coefficient would suggest the opposite. For the analysis of disclosure quality, a negative coefficient on *DISCLOSURE_DEADLINE* suggests that firms disclose fewer details when mandated to disclose under a deadline; a positive coefficient suggests the opposite.

We include state and year fixed effects in our model and, because our treatment is the passing of a state-level law, $\beta 1$ can be interpreted as a coefficient from a generalized difference-in-differences model.[22] State fixed effects also help mitigate the concern that firms self-select into the state they want to be headquartered in. We also include industry fixed effects to account for between-industry time-invariant heterogeneity. We do not include firm fixed effects in our analyses because our unit of analysis is data breach incidents, and our sample is not panel data – most of the firms are in our sample only once. We cluster the robust standard errors by state because our treatment is at the state level.[23]

The control variables in our model are based on prior literature. Following Amir et al.[24] and Kamiya et al.[15], we control for firm characteristics including *SIZE*, *FIRM_AGE*, *TOBINS_Q*, *ROA*, *SALESGROWTH*, *STOCK_RETURN*,

[2] California has a limited-scope disclosure deadline for healthcare information. However, all healthcare breaches are already covered by HIPAA, which introduced a disclosure deadline in 2009.[18–21] Thus, there is no between-state variation, and we include industry fixed effects in all analyses.

LEVERAGE, *RET_VOLATILITY*, *INST_OWNERSHIP*, *R&D*, *CAPEX*, *INTANGIBLE*, *FORTUNE500*, *SOX404_AUDIT*, *MATERIAL_WEAKNESS*, and *ANALYST_FOLLOWING*. To ensure that our treatment effect is orthogonal to litigation risk, we also control for *LIT_RISK* using the measure developed by Huang et al.[25] All of these firm-year variables are calculated using the most recent firm-year data prior to the discovery date of the data breach incident *j*. Appendix A provides detailed variable definitions We do not include number of records breached as a control variable in our analyses due to lack of data availability: the majority of observations in our sample are missing data on number of breached records.

2.2. Sample and data

Table 2, Panel A presents our sample selection. We utilize Audit Analytics' cybersecurity dataset that collects data from "SEC filings, state documents, and the press."[27] We begin with 804 data breach incidents disclosed between 2010 and 2020. We eliminate 109 incidents related to foreign firms and 370 incidents without sufficient data to calculate our dependent variables. Our initial sample includes 325 data breach incidents. Fig. 1 breaks down this sample by state (where the 'other' group is all the states with fewer than five incidents). To construct the sample for our regression

Table 2
Sample selection and descriptive statistics.

Panel A: Sample Selection	
Initial sample	
Data breach observations from 2010 to 2020 (Audit Analytics)	804
Less: Observations of US-listed foreign firms (Audit Analytics)	(109)
Less: Observations with missing data to calculate dependent variables (Audit Analytics)	(370)
Initial sample of data breach observations	325
Final sample	
Initial sample of data breach observations	325
Less: Observations with missing data for control variables (Compustat; CRSP; Thomson Reuters)	(60)
Less: Singleton observations[26]	(25)
Final sample of data breach observations	240

Panel B: Descriptive statistics

Variable	N	Mean	Std. dev.	25%	Median	75%
Test Variable						
DISCLOSURE_DEADLINE (binary)	325	0.26	0.44	0.00	0.00	1.00
Dependent Variables						
DAYS_TO_DISCLOSE (unlogged)	325	52.37	64.12	14.00	31.00	64.00
BREACH_DETAILS (binary)	325	0.76	0.43	1.00	1.00	1.00
Control Variables						
SIZE (logged)	301	8.49	2.11	7.22	8.44	9.81
FIRM_AGE (logged)	316	3.06	0.76	2.48	3.18	3.58
TOBINS_Q	279	2.20	1.84	1.12	1.53	2.44
ROA	317	0.01	0.13	0.00	0.03	0.07
SALESGROWTH	310	0.10	0.21	−0.01	0.06	0.16
STOCK_RETURN	294	0.01	0.43	−0.22	−0.02	0.17
LEVERAGE	313	0.27	0.21	0.10	0.24	0.40
RET_VOLATILITY	294	0.02	0.01	0.01	0.02	0.03
INST_OWNERSHIP	316	0.70	0.31	0.53	0.79	0.91
R&D	317	0.03	0.06	0.00	0.00	0.03
CAPEX	317	0.03	0.03	0.01	0.03	0.05
INTANGIBLE	317	0.27	0.23	0.06	0.22	0.42
FORTUNE500 (binary)	317	0.78	0.41	1.00	1.00	1.00
SOX404_AUDIT	317	0.89	0.31	1.00	1.00	1.00
MATERIAL_WEAKNESS	317	0.04	0.21	0.00	0.00	0.00
ANALYST_FOLLOWING	317	12.12	10.28	3.00	10.00	19.00
LIT_RISK	325	0.45	0.21	0.28	0.47	0.67

Panel A presents sample selection and Panel B reports the descriptive statistics. *DAYS_TO_DISCLOSE* is logged in subsequent analyses. Continuous variables are winsorized at the 1st and 99th percentiles. All variables are defined in Appendix A.

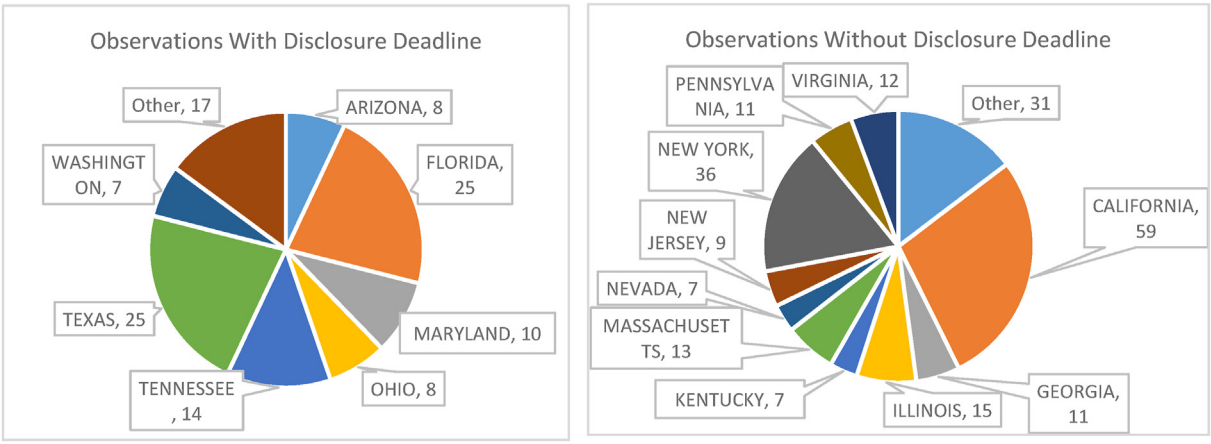

Fig. 1. Distribution of observations across states.

analyses, we lose 60 observations due to missing data for the control variables and another 25 singleton observations.[26] Our final sample consists of 240 data breach incidents.

3. Results

3.1. Descriptive statistics

Panel B of Table 2 reports the descriptive statistics. Twenty-six percent of our sample observations are under a disclosure deadline mandated by a state-level data breach disclosure law. The average firm in our sample takes roughly 52 days to disclose a data breach after its discovery. Finally, 76 percent of the data breach disclosures in our sample include details about how the breach happened and what information was leaked.

3.2. Empirical analyses

Columns 1 and 2 of Table 3 present the regression results for the analysis of disclosure timeliness, *DAYS_TO_DISCLOSE*. Across both columns, the coefficient on *DISCLOSURE_DEADLINE* is negative and significant ($p \leq 0.01$). The results reported in Column 2 suggest that firms under a disclosure deadline mandate tend to disclose the occurrence of a breach 89.82 percent faster than the control group. Columns 3 and 4 of Table 3 report the results for our analysis of disclosure quality, *BREACH_DETAILS*. Again, the coefficient on *DISCLOSURE_DEADLINE* is negative and significant ($p \leq 0.01$). The results reported in Column 4 indicate that treatment firms are 57.71 percent less likely to include breach details in their disclosure (relative to the sample mean). Taken together, these analyses provide evidence of a trade-off between disclosure timeliness and disclosure quality when firms must disclose a breach by a certain deadline mandated by a state law.

Next, we conduct two sets of sensitivity analyses to address concerns raised by the literature about difference-in-differences research designs. First, Goodman-Bacon[10] argues that, in generalized difference-in-differences models, early-treated observations 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. To overcome this issue[28], and Barrios[29] recommend a stacked regression research design. Consequently, we create individual event-cohort datasets for each of the treatment cohorts in our dataset, where a treatment cohort includes all the states that signed into law a disclosure deadline mandate for data breaches in the same year. In each event-cohort dataset, we retain observations in states that are treated for that cohort and observations that are never treated during our sample period;

Table 3
Regression analyses of disclosure timeliness and information content.

	Dependent variable: *DAYS_TO_DISCLOSE*				Dependent variable: *BREACH_DETAILS*			
Independent variables	No control variables		Full model		No control variables		Full model	
	(1)		(2)		(3)		(4)	
Test variable:								
DISCLOSURE_DEADLINE	**−0.6201**	***	**−0.8982**	***	**−0.2888**	***	**−0.4386**	***
[t-stat] (*p*-value)	[–3.01]	(≤0.01)	[–2.97]	(≤0.01)	[–3.26]	(≤0.01)	[–3.93]	(≤0.01)
Control variables:								
SIZE			−0.2229	*			0.0251	
FIRM_AGE			−0.1871				−0.0099	
TOBINS_Q			−0.0562				−0.0232	
ROA			−0.1963				0.0773	
SALESGROWTH			0.1647				0.1691	
STOCK_RETURN			0.2150				0.1202	**
LEVERAGE			−0.5390				−0.0690	
RET_VOLATILITY			−4.7492				−4.7587	
INST_OWNERSHIP			−0.2792				−0.0563	
R&D			−0.3178				0.6780	
CAPEX			0.9649				1.5699	
INTANGIBLE			0.7079				0.0279	
FORTUNE500			0.4338				0.1006	
SOX404_AUDIT			0.5688				0.0708	
MATERIAL_WEAKNESS			−0.2010				−0.1351	
ANALYST_FOLLOWING			0.0008				−0.0125	***
LIT_RISK			6.3014	***			−0.1999	
State fixed effects	YES		YES		YES		YES	
Industry fixed effects	YES		YES		YES		YES	
Year fixed effects	YES		YES		YES		YES	
N	325		240		325		240	
Adjusted R-squared	6.45%		16.35%		14.28%		8.67%	

This table presents the analysis of the effect of state-level mandated deadlines to disclose the occurrence of a data breach on (i) the number of days between the date a firm discovers a data breach and the date the firm discloses the occurrence of the breach (*DAYS_TO_DISCLOSE*) and (ii) whether a firm includes details about the data breach in its disclosure (*BREACH_DETAILS*). All variables are defined in Appendix A. All models are ordinary least squares regressions with robust standard errors clustered by state. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using two-tailed tests.

we exclude observations that are either treated before or after the treatment year of the particular cohort. We then combine all the event-cohort datasets into one dataset and rerun our main analysis, ensuring to fully saturate the model with indicators for each event-cohort.[28,29] Panel A of Table 4 present the results of this analysis.[3] Our inferences remain the same ($p \leq 0.05$ or lower).

Second, inferences from a difference-in-differences model are contingent on a valid parallel trends assumption. We address this concern by following prior literature (e.g., [22,30]) and rerunning our main analyses in a dynamic difference-in-differences model. We replace the *DISCLOSURE_DEADLINE* variable with indicators for the year before (*DISCLOSURE_DEADLINE t-1*), the year of (*DISCLOSURE_DEADLINE t*), and the year after the passage of disclosure deadline in firm *i*'s home state (*DISCLOSURE_DEADLINE t+1*), along with a catchall indicator for all the years after that (*DISCLOSURE_DEADLINE t+2…n*). We present this analysis with *DISCLOSURE_DEADLINE t-1* in the same regression as our main variable *DISCLOSURE_DEADLINE* and with all *DISCLOSURE_DEADLINE t-1*, *DISCLOSURE_DEADLINE t*, *DISCLOSURE_DEADLINE t+1*, and *DISCLOSURE_DEADLINE t+2…n* in the same regression. An insignificant coefficient for the year $t-1$ indicator would suggest that the parallel trends assumption is reasonable in our setting, which is what we find ($p = 0.36$ or higher) (see Panel B of Table 4).[4]

[3] The number of observations in Panel A of Table A exceeds the number of observations in Table 2 because some observations are repeated across event-cohort datasets. However, fully saturating the model with event-cohort indicators ensures t-stats are not artificially inflated.

[4] The coefficient on *DISCLOSURE_DEADLINE t+1* is negative but insignificant in Column 2. This is likely due to low power that results from separating our treatment variable into multiple separate treatment variables, especially given our small sample size.

Table 4
Sensitivity analyses.

Panel A: Stacked regression analysis				
Independent variables	Dependent variable: *DAYS_TO_DISCLOSE*		Dependent variable: *BREACH_DETAILS*	
	(1)		(2)	
Test variable:				
DISCLOSURE_DEADLINE	**−0.8782**	**	**−0.3852**	***
[t-stat] (*p*-value)	[–2.53]	(0.013)	[–3.47]	(≤0.01)
Control Variables	YES		YES	
State Fixed Effects	YES		YES	
Industry Fixed Effects	YES		YES	
Year Fixed Effects	YES		YES	
N	842		842	
Adjusted R-squared	14.76%		12.43%	

Panel B: Dynamic Difference-in-Differences Analysis								
Independent variables	Dependent variable: *DAYS_TO_DISCLOSE*				Dependent variable: *BREACH_DETAILS*			
	(1)		(2)		(3)		(4)	
Test variables:								
DISCLOSURE_DEADLINE t-1	**0.1152**		**0.1226**		**−0.1295**		**−0.1401**	
[t-stat] (*p*-value)	[0.37]	(0.714)	[0.39]	(0.701)	[–0.88]	(0.385)	[–0.94]	(0.356)
DISCLOSURE_DEADLINE	**−0.8665**	**			**−0.4743**	***		
[t-stat] (*p*-value)	[–2.71]	(0.012)			[–3.51]	(≤0.01)		
DISCLOSURE_DEADLINE t			**−0.9246**	**			**−0.3820**	*
[t-stat] (*p*-value)			[–2.72]	(0.012)			[–1.90]	(0.068)
DISCLOSURE_DEADLINE t+1			**−0.6720**				**−0.5920**	***
[t-stat] (*p*-value)			[–1.12]	(0.275)			[–3.73]	(≤0.01)
DISCLOSURE_DEADLINE t+2…n			**−0.9596**	*			**−0.5243**	**
[t-stat] (*p*-value)			[–1.93]	(0.065)			[–2.36]	(0.026)
Control variables	YES		YES		YES		YES	
State fixed effects	YES		YES		YES		YES	
Industry fixed effects	YES		YES		YES		YES	
Year fixed effects	YES		YES		YES		YES	
N	240		240		240		240	
Adjusted R-squared	15.81%		14.85%		8.21%		7.39%	

This table presents sensitivity analyses. In Panel A, we rerun our main analyses in a stacked regression framework. In Panel B, we rerun our main analyses in a dynamic difference-in-differences framework. All variables are defined in Appendix A. In Panel A, the model is fully saturated with indicators for each event cohort. Control variables are included in all regressions but suppressed for parsimony. All models are an ordinary least squares regression with robust standard errors clustered by state. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using two-tailed tests.

Finally, we examine how investors perceive the timeliness and quality of data breach disclosures. We study the effect of *DAYS_TO_DISCLOSE*, *BREACH_DETAILS*, and the interaction of the two on abnormal returns around breach disclosure dates.[15,24] The dependent variable in this analysis, *BREACH_CAR*, is breached firm *i*'s abnormal returns cumulated over the 3-day window [0,2] for the data breach incident *j* (where day 0 is the date of breach disclosure). Table 3 reports the results of this analysis.

In both columns of Table 5, the coefficients on both *DAYS_TO_DISCLOSE* and *BREACH_DETAILS* are *negative* and significant ($p \leq 0.05$ and $p \leq 0.01$, respectively), the coefficient on the interaction term is *positive* and significant ($p \leq 0.05$), and the 'total effect' of *DAYS_TO_DISCLOSE* + *DAYS_TO_DISCLOSE*BREACH_DETAILS* is insignificant. These results generate three inferences. First, investors penalize firms that delay the data breach disclosure. Second, investors appear forgiving of a delayed disclosure when that delay is presumably due to gathering and reporting more breach details, which may include positive information about the breach that was gathered during the delay. Third, investors react negatively when firms disclose breach details *too* quickly after the discovery, indicating that investors discount the quality of disclosed details when firms rush to provide disclosure.

Table 5
Abnormal returns around data breach disclosure conditional on timeliness and information content.

	Dependent variable: *BREACH_CAR*			
Independent variables	No control variables		Full model	
	(1)		(2)	
Test Variables:				
DAYS_TO_DISCLOSE	**−0.0087**	**	**−0.0087**	**
[t-stat] (*p*-value)	[–2.48]	(0.018)	[–2.57]	(0.017)
BREACH_DETAILS	**−0.0414**	***	**−0.0404**	***
[t-stat] (*p*-value)	[–2.79]	(≤0.01)	[–3.00]	(≤0.01)
*DAYS_TO_DISCLOSE*BREACH_DETAILS*	**0.0088**	**	**0.0083**	**
[t-stat] (*p*-value)	[2.48]	(0.017)	[2.67]	(0.013)
Control Variables:				
SIZE			−0.0014	
FIRM_AGE			0.0000	
TOBINS_Q			0.0027	
ROA			−0.0572	
SALESGROWTH			−0.0140	
STOCK_RETURN			0.0026	
LEVERAGE			0.0029	
RET_VOLATILITY			0.4681	
INST_OWNERSHIP			0.0138	
R&D			−0.0051	
CAPEX			0.0689	
INTANGIBLE			−0.0174	
FORTUNE500			0.0037	
SOX404_AUDIT			0.0571	***
MATERIAL_WEAKNESS			−0.0124	
ANALYST_FOLLOWING			0.0004	
LIT_RISK			−0.0241	
State Fixed Effects	YES		YES	
Industry Fixed Effects	YES		YES	
Year fixed effects	YES		YES	
N	293		239	
Adjusted R-squared	2.35%		7.62%	
*DAYS_TO_DISCLOSE + DAYS_TO_DISCLOSE*BREACH_DETAILS = 0*	**0.0001**		**−0.0004**	
[t-stat] (*p*-value)	[0.00]	(0.984)	[0.17]	(0.865)

This table presents the analysis of the effect of the number of days it takes for a firm to disclose a data breach after discovery (*DAYS_TO_DISCLOSE*) and whether a firm includes details about the data breach in its data breach disclosure (*BREACH_DETAILS*) on abnormal returns for the firm around the data breach disclosure date. All variables are defined in Appendix A. Both models are an ordinary least squares regression with robust standard errors clustered by state. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using two-tailed tests.

4. Conclusion

In this study, we analyze the potential trade-offs with imposing a deadline for cybersecurity incident disclosures. Our research question is motivated by the growing importance of cybersecurity risk and, particularly, the SEC's recent proposal that requires firms to report material cybersecurity incidents within four business days of discovery.[4] Using a generalized difference-in-differences research design that exploits variations in state-level data breach disclosure laws, we find that firms under a mandated disclosure deadline (i) disclose the occurrence of a breach more quickly but (ii) report fewer details. We further find that investors penalize firms that delay breach disclosure but are more forgiving if that delay is used to obtain and report more breach details. We also find that investors appear to discount the disclosures that contain breach details but are disclosed too quickly after a data breach.

Overall, our study contributes to the literature that examines data breach disclosure laws (e.g.,[9]) and the literature on data breaches and cybersecurity incidents in general (e.g.,[15]). Most importantly, the immediate impact of our empirical evidence is that it has implications for the SEC's recently proposed disclosure rule on cybersecurity incidents.[4] While the SEC notes that they do not possess empirical evidence on the effects of this kind of mandate that imposes a short

deadline for cyber incident disclosure, our study offers indirect evidence using the setting of state laws on data breach disclosures – when timeliness is prioritized, disclosure quality may be inevitably compromised.

Conflicts of Interest

All authors have none to declare.

Acknowledgement

All correspondence should be sent to jiangj@msu.edu. We thank Eli Amir, Henry Huang, and Chong Wang for comments and suggestions. We are grateful for the research support provided by the Plante Moran Fellowship, the Eli Broad Professorship, the Deloitte/Michael Licata Professorship, and the Broad College of Business. Any errors are our own. We have no relevant or material financial interests that relate to the research described in this paper.

APPENDIX A

Variable Definitions

Variable		Definition [Data Source]
DISCLOSURE_DEADLINE	=	One if firm *i*'s home state *k* has signed into law a disclosure deadline on or before the discovery date of data breach incident *j* (zero otherwise) [Hand-collected by cross-referencing[31–33]; and the texts of the laws]
DAYS_TO_DISCLOSE	=	The natural log of one plus the number of days between firm *i*'s data breach incident *j*'s discovery date and firm *i*'s disclosure date of data breach incident *j* [Audit Analytics]
BREACH_DETAILS	=	One if the disclosure of firm *i*'s data breach incident *j* includes details about how the attack happened and what was leaked in the breach (zero otherwise) [Audit Analytics]
BREACH_CAR	=	Firm *i*'s raw return on day *t* minus CRSP value-weighted market return on day *t*, cumulated over the [0,2] window, where day 0 is the disclosure date of data breach incident *j* [Audit Analytics; CRSP]
SIZE	=	The natural log of firm *i*'s market capitalization as of the most recent fiscal year end prior to the data breach incident *j* [Compustat]
FIRM_AGE	=	The natural log of one plus the age of firm *i,* calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
TOBINS_Q	=	[(total assets + market capitalization) – (book value of equity + deferred taxes)]/total assets, where all terms are calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
ROA	=	Firm *i*'s net income scaled by firm *i*'s total assets, where all terms are calculated for Firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
SALESGROWTH	=	Firm *i*'s sales in year *t* minus firm *i*'s sales in year *t*-1, all scaled by firm *i*'s sales in year *t*-1, where all terms are calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
STOCK_RETURN	=	Firm *i*'s buy-and-hold abnormal return over year *t*, calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
LEVERAGE	=	Firm *i*'s long-term debt scaled by firm *i*'s total assets, where all terms are calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
LIT_RISK	=	Firm *i*'s litigation risk in year *t*, calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j*.[25] We thank Allen Huang for sharing the data for this measure.
RET_VOLATILITY	=	The standard deviation of firm *i*'s raw return over year *t*, calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
INST_OWNERSHIP	=	The percent of firm *i* owned by institutional investors, calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Thomson Reuters]
R&D	=	Firm *i*'s research & development expenditures scaled by firm *i*'s total assets, where all terms are calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
CAPEX	=	Firm *i*'s capital expenditures scaled by firm *i*'s total assets, where all terms are calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
INTANGIBLE	=	Firm *i*'s intangible assets scaled by firm *i*'s total assets, where all terms are calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]

(*continued on next page*)

(*continued*)

Variable		Definition [Data Source]
FORTUNE500	=	One if firm *i* is a Fortune 500 company in year *t*, calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Compustat]
SOX404_AUDIT	=	One if firm *i* receives an audit for SOX 404 internal controls in year *t*, calculated for Firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Audit Analytics]
MATERIAL_WEAKNESS	=	One if firm *i*'s external audit report for year *t* indicates a weakness in SOX 404 internal controls, calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j* [Audit Analytics]
ANALYST_FOLLOWING	=	The number of analysts following firm *i* in year *t*, calculated for firm *i* in the most recently ended firm-year prior to firm *i*'s data breach incident *j*; this variable is set to zero for firms without analyst following [IBES]

References

1. Securities and Exchange Commission (SEC). *Commission statement and guidance on public company cybersecurity disclosures*; 2018:1–25. Retrieved https://federalregister.gov/d/2018-03858.
2. Securities and Exchange Commission (SEC). *CF disclosure guidance: topic No. 2*; 2011:1–6. Retrieved https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
3. Clayton CJ. SEC rulemaking over the past year, the road ahead and challenges posed by Brexit, LIBOR transition and cybersecurity risks. Retrieved https://www.sec.gov/news/speech/speech-clayton-120618; 2018.
4. Securities and Exchange Commission (SEC). *Proposed rule: cybersecurity risk management, strategy, governance, and incident disclosure*; 2022. Retrieved https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
5. Folsom D, Hribar P, Mergenthaler RD, Peterson K. Principles-based standards and earnings attributes. *Manag Sci*. 2017;63(8):2592–2615.
6. Pierson C. When to disclose a data breach. Retrieved https://www.darkreading.com/risk/when-to-disclose-a-data-breach; 2007.
7. Tsukayama H. *Why it can take so long for companies to reveal their data breaches*; 2017. Retrieved https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/why-it-can-take-so-long-for-companies-to-reveal-their-data-breaches/?utm_term=.ebf76710cd98.
8. Romanosky S, Telang R, Acquisti A. Do data breach disclosure laws reduce identity theft? *J Pol Anal Manag*. 2011;30(2):256–286.
9. Ashraf M, Sunder J. *Can shareholders benefit from consumer protection disclosure mandates? evidence from data breach disclosure laws and the cost of equity*. 2022 [Working paper].
10. Goodman-Bacon A. Difference-in-differences with variation in treatment timing. *J Econom*. 2022;225(2):254–277. https://doi.org/10.1016/j.jeconom.2021.03.014.
11. PricewaterhouseCoopers (PwC). *2018 global investor survey*; 2018:1–29. Retrieved https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf.
12. Rajgopal S, Srinivasan S. Why the market yawned when yahoo was hacked. *Wall St J*; 2016:1–3. Retrieved https://www.wsj.com/articles/why-the-market-yawned-when-yahoo-was-hacked-1475537076.
13. Richardson VJ, Smith RE, Watson MW. Much ado about nothing: the (lack of) economic impact of data privacy breaches. *J Inf Syst*. 2019;33(3):227–265.
14. Foerderer J, Schuetz S. Data breach announcements and stock market reactions: a matter of timing? *Manag Sci*. 2022. https://doi.org/10.1287/mnsc.2021.4264. In preparation.
15. Kamiya S, Kang JK, Kim J, Milidonis A, Stulz RM. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *J Financ Econ*. 2021;139(3):719–749.
16. Huang HH, Wang C. Do banks price firms' data breaches? *Account Rev*. 2021;96(3):261–286. https://doi.org/10.2308/TAR-2018-0643.
17. Pirinsky C, Wang Q. Does corporate headquarters location matter for stock returns? *J Finance*. 2006;61(4):1991–2015.
18. Bai G, Jiang J, Flasher R. Hospital risk of data breaches. *JAMA Intern Med*. 2017;177(6):878–880.
19. Department of Health and Human Services. *Breach notification rule*; 2018:1–4. Retrieved https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.
20. Jiang J, Bai G. Evaluation of causes of protected health information breaches. *JAMA Intern Med*. 2019;179(2):265–267.
21. Jiang JX, Bai G. Types of information compromised in breaches of protected health information. *Ann Intern Med*. 2020;172(2):159–160.
22. Bertrand M, Mullainathan S. Enjoying the quiet life? Corporate governance and managerial. *J Polit Econ*. 2003;111(5):1043–1075.
23. Abadie A, Athey S, Imbens G, Wooldridge J. *When should you adjust standard errors for clustering?*. 2017.
24. Amir E, Levi S, Livne T. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Rev Account Stud*. 2018;23(3):1177–1206.
25. Huang A, Hui KW, Li R. Federal judge ideology: a new measure of ex ante litigation risk. *J Account Res*. 2019;57(2):431–489.
26. Correia S. *Singletons, cluster-robust standard errors and fixed effects: a bad mix*. 2015.
27. Audit Analytics. Audit Analytics cybersecurity data. Retrieved https://www.auditanalytics.com/doc/AA_Cybersecurity_ds.pdf; 2022.
28. Baker A, Larcker DF, Wang CCY. How much should we trust staggered difference-in-differences estimates? *J Financ Econ*. 2022;144(2):370–395.
29. Barrios JM. *Staggeringly problematic: a primer on staggered DiD for accounting researchers*. 2021.
30. Bourveau T, Lou Y, Wang R. Shareholder litigation and corporate disclosure: evidence from derivative lawsuits. *J Account Res*. 2018;56(3):797–842.

31. BakerHostetler. Breach notification law interactive map. Retrieved https://www.bakerlaw.com/BreachNotificationLawMap; 2022.
32. Perkins C. Security breach notification chart. (September). Retrieved https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html; 2021.
33. Schwartz, Ballen LLP. Summary of state laws requiring notification of a security breach of personal information. Retrieved http://www.schwartzandballen.com/Memos 2017/State Security Breach Chart 020717.pdf; 2017.