Mandatory Data Breach Disclosure and Insider Trading

Abstract

Using the staggered adoption of state-level data breach notification laws, we examine whether mandatory breach disclosure affects insider selling. Trading profits are greater after states require firms to disclose data breaches. The effect is concentrated among firms with a greater ex ante breach risk and those that do not increase investment after the passage of law. Firms that are located in states that implement stricter versions of the law and those that are exposed to a higher breach risk increase their cyber-related investment under the new legal regime. This absence of investment leads to an increase in breach risk, which is associated with more idiosyncratic crashes. These crashes and the lack of cyber-related investments are linked to the profitability of insider sales. Our study reveals some negative capital market externalities of mandatory disclosure laws designed to protect customers and citizens at large.

Keywords: Cybersecurity, Data breach, Regulation, Disclosure, Insider trading

JEL Classification Codes: G18; M41; K22; K24

1. Introduction

The 2019 Global Risks Report by the World Economic Forum ranked cyber risk as one of the top 10 risks in terms of both likelihood and impact. Cybersecurity and its related disclosure have become a significant concern for regulators. For instance, the Security Exchange Commission (SEC) formed a Cyber Unit to investigate cyber-related delinquencies in 2017 and updated its guidelines on cyber risk disclosure in 2018. Successful cyberattacks can have a material effect on target firms (e.g., Kamiya et al. 2020). Cyber risk is a multifaceted threat that can include the destruction of physical assets (e.g., Aramco), the theft of intellectual property (e.g., Nortel), or damage to electronic systems (e.g., Maersk). However, the threat of most concern to the public may be massive data losses that violate individual privacy. From 2005 to 2010, data breaches compromised an estimated 350 million records (Shaw 2010). In 2018 alone, 447 million records were compromised.[1] High-profile data leaks, such as those at Equifax or Marriott, make headlines on a regular basis, and regulators have published a slew of legal instruments to address cyber risk and related disclosure issues.[2] In its 2018 guidelines, the SEC specifically mentions that insider trading based on nonpublic information about cyber risk or cyber incidents is prohibited (SEC 2018).[3] Recent high-profile SEC investigations of data breach-related insider trading further highlight this concern. For instance, the SEC charged executives at Equifax with insider trading related to the data breach in 2017.[4]

Given the relevance of this issue, we examine the effect of breach disclosure regulation in the United States (US). There is a long-held agreement among regulators that "Sunlight is said to be the best of disinfectants."[5] Instead of issuing regulations that require certain

[1] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[2] For example, the European Union recently issued the General Data Protection Regulation, a wide-ranging data protection legislation.

[3] https://www.sec.gov/rules/interp/2018/33-10459.pdf

[4] https://www.lexology.com/library/detail.aspx?g=902fabbe-fab1-4251-afb2-037f64355c02

[5] This quote is attributed to Justice Louis D. Brandeis (https://www.brandeis.edu/legacyfund/bio.html).

behaviors, regulators often believe that they can mandate the disclosure of undesired behaviors to achieve the same goals more efficiently (e.g., Fung, Graham, and Weil 2007). However, the findings of academic studies on the effectiveness of this approach are rather mixed, as regulations often induce unintended behaviors or other externalities.[6] For instance, if sellers of consumer goods are required to disclose negative information after testing the quality of their products, they may choose not to run such tests (Matthews and Postlewaite 1985; Shavell 1994). We consider potential spillovers in the financial market from the regulation of personal data by examining the staggered adoption of mandatory data breach disclosure laws (triggered by state-level actions) on insider and firm behavior.

As of 2021, there is no federal law designed specifically for data breach disclosures. However, all states and the District of Columbia implemented data breach regulations between 2003 and 2018. These laws require organizations to notify affected parties (e.g., consumers or employees) of data breaches after the firm discovers them. As the regulation of financial markets is mostly the purview of the federal government, state regulators did not focus on the potential effects of their data breach laws on SEC-regulated matters. Thus, the staggered adoption of plausibly exogenous state laws provides a quasi-experimental setting in which to test the effects of mandatory breach disclosures on insider trading behaviors.

The effect of these laws on insider trading is undetermined ex ante. On the one hand, the mandated data breach disclosure may prompt opportunistic insider trading, particularly opportunistic sales. Existing studies often link the public revelation of bad news to opportunistic insider sales ahead of negative news announcements (e.g. Ke, Huddart, and Petroni 2003; Dechow, Lawrence, and Ryans 2016; Ryan, Tucker, and Zhou 2016). Thus, it is plausible that mandated data breach disclosures may also increase managers' incentives to sell

[6] See Benston 1973; Fung, Graham, and Weil 2007; Gao, Wu, and Zimmerman 2009; Leuz and Wysocki 2016; Berger 2011.

their shares to avoid potential future losses. Mandating breach disclosures reveals adverse events that may not have surfaced othwerwise. If a manager believes that his or her firm may suffer from a data breach in the future or has already suffered from an undisclosed breach, he or she may sell his or her shares ahead of disclosure to avoid potential losses.

On the other hand, the mandated data breach disclosure may not lead to opportunistic insider trading (nor even to a reduction in insider trading) because the new laws induce additional costs (e.g., reputational or monetary) if a breach is revealed publicly. The additional costs may prompt firms to take preemptive measures to prevent data breaches and mitigate their economic impact if they occur. Under such a scenario, firms may reduce the number of material events that offer an opportunity for insider sales. Further, the additional scrutiny brought by the new regulation may deter managers from engaging in insider trading to exploit their private information on cyber risk.

Using a generalized difference-in-difference (DID) design, we find that insider sales' profits are significantly larger after states implement data breach laws.[7] We verify that the parallel trend test shows no significant difference in selling profits between our treated and control samples in the pretreatment period. Our results hold if we focus on firm headquarters to identify whether the change is affected by a given state's breach law or if we consider the different states in which a firm has significant operations. Our results are also robust to multiple specification checks. For example, they hold if we drop any given state. These findings suggest that the mandated disclosure of data breaches may have the unintended consequence of prompting executives to sell their shares ahead of potential future occurrences, and as a result, of the potential revelation of data breaches. As such, we predict and find that our results are stronger if the ex ante risk of breaches is greater.

[7] In this context, profits are defined as losses avoided by trades.

We consider three placebo tests to further support our results. First, data breach laws may trigger the revelation of mostly bad news but not good news. This gives insiders incentives to avoid possible future losses by selling their stocks, but it should not affect purchases. Consistent with this view, we find that data breach laws impact insider sales but not insider purchases. Second, we estimate our baseline specification for routine and nonroutine sales separately. Previous studies (e.g., Cohen, Malloy, and Pomorski 2012; Ali and Hirshleifer 2017) report that nonroutine trades capture insiders' opportunistic use of nonpublic information in their trading strategies and earn significantly higher profits for executives. Consistent with this view, the effect of the law on insider selling profits is significant only in the sample of nonroutine sales. Third, financial institutions are covered by a specific federal regulation (i.e., the Gramm–Leach–Bliley Act of 1999) and are thus typically exempt from additional state-level requirements. We expect that data breach laws should not affect executives working in the financial sector.

Finally, we investigate the mechanisms that explain our findings. Prior literature (e.g., Hilary, Segal and Zhang (2016)) find a statistically significant but economically small market reaction around the announcements of all data breaches. In contrast, Kamiya, Kang, Kim and Milidonis Stulz (2020) document an economically significant effect of hacking on firm operations. Importantly, Florackis et al. (2020) find that cyber-risk can be predicted using a textual analysis from 10K filings, suggesting that insiders and possibly savy investors have a long term vision of the risk faced by a firm. In this context, the effect of data breaches on stock prices may be smoothed over long periods of time. As a result, managers from high risk firms may either work on mitigating the underlying risk or engage in insider selling when states mandate disclosures of data breaches. Consistent with this view, we find that firms that are located in states that implement stricter versions of the breach laws and those that are exposed to a higher breach risk increased their cyber-related investment under the new legal regime.[8] In contrast, we find the effect of disclosure laws on insider trading is concentrated among firms that do not increase investment after the passage of the laws. This absence of incremental investment is associated an increase in revealed data breaches.[9] Firms that have a greater ex ante risk of breaches or suffer from a breach ex post are more likely to also suffer from an idiosyncratic crash. These crashes and the lack of cyber-related investments are linked to the profitability of insider sales.

Our findings make several contributions. First, the SEC is concerned with insiders using nonpublic information to trade on cyber risks, as well as actual data breach incidents. To improve cyber risk disclosure, the SEC issued guidelines in 2011 and 2018. However, a number of senators and house representatives have repeatedly introduced the Data Security and Breach Notification Act as a bill.[10] Our results show that strict breach disclosure laws can have real effects on firm behavior by providing incentives to invest more in cyber security programs. Our results also demonstrate the possible effects of these laws on the behavior of informed agents. Trading on nonpublic information is one of the most significant threats to the SEC's goal of "leveling the playing field" for different investors in the capital market. Our study informs the SEC of how insider traders use cyber-related nonpublic information and how such behavior might be affected by other noncapital market disclosure regulations.

Second, previous studies of insider trading have examined the issues: (1) the existence and determinants of insider trading (e.g., Acharya and Johnson 2010; Ke, Huddart, and Petroni 2003; Marin and Olivier 2008; Jin and Kothari 2008; Bernile, Hu, and Tang 2016; Alldredge

[8] As of 2018, every state has adopted data breach laws, but there are some key differences between states. In particular, the laws vary in regard to their requirements and specificity. We form indexes that rank these laws based on their stringency.

[9] Existing studies demonstrate that public disclosures of data breaches increase substantially after a state implements a data breach law (e.g., Romanosky, Telang, and Acquisti 2011; Ashraf and Sunder 2018).

[10] For instance, one was introduced in 2013 by Sen. John D. Rockefeller, and another was introduced by Rep. Marsha Blackburn in 2015.

and Cicero 2015; Gao and Huang 2016; Lin, Sapp, Ulmer, and Parsa 2020),[11] (2) the effects or consequences of insider trading (e.g., Jenter 2005; Ahern 2017; Piotroski and Roulstone 2005), and (3) the disciplinary mechanisms that can restrict insider trading (e.g., Garfinkel 1997; Bettis, Coles, and Lemmon 2000; Lenkey 2014; Jagolinzer, Larcker, and Taylor 2011). Our study is related most closely to the third stream of research. For example, prior studies suggest that opportunistic insider trading is reduced when insider trading regulations are implemented; when firms set restrictions, such as blackout windows, for insider trading; when insiders are required to disclose their trading faster than before; and when the media disseminates the disclosure (e.g., Brochet 2010; Dai, Parwada, and Zhang 2015; Jagolinzer, Larcker, and Taylor 2011). Our findings also indicate that weak legal designs may exacerbate the problems and lead to negative unintended consequences.

The remainder of this study is organized as follows: Section 2 introduces the institutional background, Section 3 discusses the data and descriptive statistics, Section 4 presents the research design and the main empirical results, Section 5 presents additional empirical analysis, and Section 6 concludes the study.

2. Institutional Background

As of 2020, there is no comprehensive US federal law governing the disclosure of data breaches.[12] However, in 2002, California was the first state to adopt a data breach law, which became effective in 2003. Between 2002 and 2018, all states adopted such laws, which are broadly consistent in their approaches, but vary regarding the establishment of specific provisions. Many of these laws contain provisions pertaining to the definition and coverage of breaches, required notification details, notification timelines, penalties, and enforcement. Aside

[11] For example, Lin et al. (2020) finds some insider trading activities 55 to 72 days before the breach announcements. Our study does not focus on disclosed breach events in the post period. Rather, we investigate the impact of the mandatory disclosure regulations itself.

[12] However, firms under the jurisdiction of the SEC or those falling under specific statutes (e.g., Health Insurance Portability and Accountability Act of 1996) may have additional specific requirements.

from some relatively minor variations, the first dimension is largely similar across states. A data breach is generally defined as a situation in which an unauthorized person or entity obtains sensitive information. The breached entity is liable to notify the affected parties of the incident and, in some cases, third parties, such as credit agencies or the Attorney General must also be notified.

Although the content of the notification varies significantly across states, the basic requirement is similar. It typically includes a general description of the incident, such as the date of the breach and the information that was leaked. However, some states may require more detailed disclosures. For instance, California requires that any delay in disclosure caused by a law enforcement request be disclosed, and Florida requires the disclosure of firm policies regarding breaches and their remedies. States can require breached entities to either disclose the incident as soon as possible (e.g., District of Columbia) or to do so before a specific deadline (e.g., no later than 45 days in Ohio). While some states do not specify penalties for violating the law (e.g., Georgia), others do (e.g., Alaska). These penalties vary significantly across states. The last major dimension—enforcement—also varies greatly across states. At one end of the spectrum, some states disallow private rights of action (e.g., Florida), while at the other extreme, some states (e.g., Iowa) specifically require entities to disclose breaches to the Attorney General and allow this office to bring lawsuits against entities that violate the law.

From the regulators' perspective, the *intent of breach disclosure* requirement is to make the incidents publicly known to induce firms to invest more in improving their data protection (e.g., through better cybersecurity) and to allow victims to remedy their situations more swiftly. The effect on financial markets is not a primary concern, although these laws can have material effects on the integrity of financial markets.

3. Data and Descriptive Statistics

Table 1 summarizes our sample selection procedure. Our initial sample includes the insider transactions of firms listed on the NYSE, AMEX, or NASDAQ that are covered in the Thomson Reuters Insider Filings (Form 4) for the 2000 to 2017 period.[13] The sample begins three years before California implemented its data breach law in 2003 and ends three years after Florida and Kentucky implemented their data breach laws in 2014. Our implementation timeline by state is consistent with Kamiya et al. (2020) and is presented in Appendix A.

The insider transaction data contains insider trading information from directors, officers, and beneficial owners with holdings greater than 10% of a firm's stock. Until August 2002, all of these insider transactions were subject to disclosure requirements, as defined in Section 16 of the Exchange Act of 1934, and subsequently to the requirements of Section 403 of the Sarbanes–Oxley (SOX) Act.[14] Our analyses focus on insiders' open market sales; hence, we exclude option exercises, private transactions, and open-market purchases from our main tests (e.g., Cohen, Malloy, and Pomorski 2012; Dai et al. 2016).

We further limit the sample by requiring that share codes in the CRSP database be 10 or 11, and we exclude the following transactions from the sample: (1) transactions with fewer than 100 shares or those with trading prices less than $2, (2) transactions with traded prices outside the range between the daily low and high prices reported in CRSP, (3) transactions in which the number of shares exceeds the total number outstanding in CRSP, (4) transactions in which the number of shares traded exceeds the total daily trading volume in CRSP, and (5) those involving regulated firms in the financial or utility industries (firms with SIC codes between 6000 and 6999 or between 4900 and 4999; Dai et al. 2016).[15]

[13] Three states (New Mexico, Alabama, and South Dakota) implemented the data breach law in 2017 and 2018.

[14] In a robustness check, we exclude the observations before 2002 and obtain qualitatively similar results.

[15] Adding utilities back to the sample does not affect our conclusions.

These restrictions result in a sample of 31,249 firm-year observations. We combine the initial sample with COMPUSTAT/CRSP data. After merging and deleting observations with missing data, we obtain a final sample of 28,039 firm-year observations.[16]

< INSERT TABLE 1 >

We define our variables in Appendix B. *Sell Profits* is the profitability of insider sales defined as the losses avoided by selling shares. If insiders' trades reflect information already impounded in stock prices, average insider trading profitability should be zero. In contrast, insider trading profitability will be greater than zero when managers trade on their private information. Similar to Skaife, Veenman, and Wangerin (2013), we measure insider trading profits as the one-year buy-and-hold abnormal return on the stock multiplied by the value of the trade (in millions of dollars) multiplied by minus one. This approach allows us to incorporate the effect of trade materiality, whereas focusing on trading intensity alone (i.e., returns) would ignore the predictive ability of this materiality with respect to future stock price performance. We aggregate individual transactions at the firm-year level (to account for the fact that breaches are firm-level incidents).

The descriptive statistics for our main variables are presented in Panel A of Table 2. As shown in the table, 67% (33%) of the firm-year observations in our sample are after (before) the implementation of a data breach law. The mean of *Sell Profits* is around 200,000 dollars. The average *Size* of firms in our sample is 6.7 in market capitalization (which translates to 5,695 million in market capitalization). The mean of stock return volatility is 0.03, and the mean *Book-to-Market Ratio* is 0.5. We find that 30% of the observations are from firms reporting a loss (*Loss*=1), and 56% are from firms reporting non-zero research and development (R&D) expenditures (*R&D Dummy*). In general, the magnitude of our variables

[16] Variations in data requirements across tests lead to different sample sizes in some ancillary tests.

is consistent with the literature (e.g., Skaife, Veenman, and Wangerin 2013; Chi, Pincus, and Teoh 2014).

The Pearson correlations are presented in Panel B of Table 2. The correlation between our dependent variable (*Sell Profits*) and our variable of interest (*Post*, an indicator variable that takes the value of 1 after the implementation of data breach laws, and 0 otherwise) is negative. At first glance, this suggests that states' breach laws reduce insiders' opportunistic selling behavior. However, previous studies (e.g., Brochet 2010) show that the enforcement of general anti-insider trading provisions and the speed of Form 4 disclosure have increased over time. After controlling for this trend, the univariate correlation between *Post* and *Sell Profits* becomes significantly positive (at the 10% level). The majority of the control variables are significantly correlated with insider selling profits and have the predicted signs.

< INSERT TABLE 2>

4. Research Design and Main Empirical Results

4.1 Impact of data breach laws on insider trading

We use a DID approach to examine how the implementation of data breach laws affects the insider sale behaviors of executives working for firms headquartered in the affected states. Following previous studies (e.g., Bertrand and Mullainathan 2003), we use the following specification:

$$Sell\ Profits_{j,t} = \alpha + \beta_1 Post_{j,t} + \Sigma\beta_2 Controls_{j,t} + \Sigma\beta_3 Firms\ Fixed\ Effects_{j,t} + \Sigma\beta_4 Year\ Fixed\ Effects_{j,t} + \varepsilon_{j,t}.$$

Our variable of interest is *Post.* We include firm- and year-fixed effects. β_1 essentially captures a DID estimator in which the control group is as follows: firms in states that have not yet implemented a data breach law as of year t nor implemented a data breach law effectively prior to year t (e.g., Bertrand and Mullainathan 2003; Klasa et al. 2018). We cluster standard errors by the state in which the headquarters are located because *Post* is a state-level variable (Klasa et al. 2018). Clustering by firm or industry does not affect our results (untabulated).[17]

We control for firm size (*Size*) because Seyhun (1986) finds that insiders buy more in smaller firms and sell more in larger firms, and Lakonishok and Lee (2001) find that insiders trade more profitably in smaller firms. We also control for the book-to-market ratio (*Book-to-Market Ratio*) because prior research shows that insiders trade more actively in low book-to-market firms (e.g., Rozeff and Zaman 1998). Following Brochet (2010), we include a *Loss* indicator variable to control for a firm's financial performance. Following Aboody and Lev (2000), we control for an R&D indicator variable (*R&D Dummy*) because higher R&D intensity may be associated with greater information asymmetry. We also include *Return Volatility*, the standard deviation of daily stock returns over the fiscal year (e.g., Ravina and Sapienza 2010), and *Dividend*, defined as cash dividend scaled by shareholder equity, to control for growth opportunities (e.g., Chi, Pincus, and Teoh 2014). Following Kallunki et al. (2018), we use firm-fixed effects to control for the effects of possible omitted time-invariant, firm-specific factors that affect insider trading, and we include yearly indicator variables to control for time-specific effects.

The results of our main regression are reported in Panel A of Table 3. The coefficient for *Post* is positive and significant (p-value<0.01), indicating that the implementation of the data breach laws has an impact on the sales behaviors of insiders. The results are robust to controlling for industry*year-fixed effects. The control variables generally have the predicted signs.

Next, we investigate the parallel trend assumption embedded in our DID design. Although the assumption is theoretically untestable, Roberts and Whited (2013) suggested a

[17] Our untabulated results can be found in our Internet Appendix at https://docdro.id/MqVrGvL.

parallel trend test which can provide supporting evidence for the assumption. Essentially, we investigate when the changes in insider selling behavior occur relative to the implementation of the data breach laws. To this end, we create a series of indicator variables, *Effective* indexed t+i from t-2 to t+2, with t=0 being the year of implementation of a data breach law in the state in which the firm is headquartered. The variables take the value of 1 if a law is passed within t-i. We report the results in Panel B of Table 3. We find that the coefficients on $\textit{Effective}^{-2}$ and $\textit{Effective}^{-1}$ are statistically insignificant, whereas the coefficients on $\textit{Effective}^{0}$, $\textit{Effective}^{+1}$, and $\textit{Effective}^{+2}$ are all consistently positive and statistically significant. Overall, these results support the validity of the parallel trend assumption in our setting.

< INSERT TABLE 3>

Next, we investigate whether firms that are expected (ex ante) to be more affected by the law are indeed more affected ex post. To do this, we create two new variables—*Relevance* and *BreachRisk* —that measure the firm's exposure to technology risk. We define *Relevance* as an indicator variable that takes the value of 1 if the Information Technology Officer (i.e., Chief Technology Officer, Chief Information Officer, or Chief Security Officer) is among the top management team tracked by ExecuComp, and 0 otherwise. This is the case for approximately 27% of our sample (4,613 out of 16,918 based on available data from ExecuComp).[18] We define *Breach Risk*, a binary variable, in the following way. We first identify a list of data breach disclosures in year t from the Private Rights Clearinghouse database.[19] We identify peer firms based on Hoberg and Phillips (2016)'s products similarity measure (calibrated at the three-digit SIC code level). For a given year, we classify firms that have been breached in a window starting 3 years before and ending three years after as well as their peer firms as high risk firms (*Breach Risk* = 1). We classify the remaining firms as low

[18] We remove firms that are not covered by Execucomp for the tests that involve *Relevance* .

[19] See http://www.privacyrights.org/data-breach

risk firms (*Breach Risk* = 0). We report the results of this analysis in Table 4. Consistent with our expectations, the results indicate that the effect of the law on insider trading is concentrated among firms for which technology is an important issue and those that suffer from a greater ex ante risk of being breached.

< INSERT TABLE 4>

4.2 Placebo tests

We conduct different placebo tests to support our main findings. First, we consider routine and nonroutine trades separately. We expect the effect of the laws to be concentrated among nonroutine trades, as these are more likely to capture information-based opportunistic transactions. To test this conjecture, we follow previous studies (e.g., Cohen, Malloy, and Pomorski 2012). We categorize an insider as a routine trader if he or she has been trading in the same month for at least the past three consecutive years. We categorize the other insiders who sell in the period under consideration as opportunistic (i.e., nonroutine) traders. We then aggregate insider trading profits at the firm-year level. The results reported in column 1 of Panel A of Table 5 show that, as expected, the laws do not affect routine transactions (the untabulated results show that *Post* continues to be significant in the sample of opportunistic trades).

Second, both significant data breach risk and actual data breaches are bad news for firms. If insiders possess related nonpublic information and trade based on this, it should prompt insiders to sell their shares to avoid loss. The same rationale does not apply to insider purchases, as it is unlikely that the laws will generate unexpected good news for firms. Thus, we expect that state breach laws should not affect insider purchases. The results reported in column 2 of Panel A of Table 5 confirm this intuition, showing that breach laws have no significant impact on insider purchases.

Finally, the Gramm–Leach–Bliley Act of 1999 created a federal regulation that addresses data protection requirements for financial institutions. As this federal law predated the state breach laws, financial institutions are typically exempted from state law coverage. Thus, we expect that these laws should not affect insider trading behaviors among financial institutions. The results reported in column 3 of Panel A of Table 5 confirm this prediction.

4.3 Robustness tests

We also conduct a series of robustness checks to validate our main findings. First, we restrict our definition of insiders to officers and directors, excluding large shareholders. Arguably, officers and directors might have firsthand information about their firm. Thus, they may better assess the risk of future breaches, the occurrence of extant breaches, and their possible consequences. This may not be the case for large shareholders (i.e., other "external" corporate "insiders," as defined by Thomson Reuters). Our untabulated results indicate that our conclusions hold if we limit our observations to officers and directors.

Second, there may be a concern that a specific state and its idiosyncrasies generate our results. For example, California is the first state to adopt breach laws and is home to many data-driven firms. One concern could be that our results are driven by these firms. Our untabulated results indicate that our conclusions hold if we exclude California, and, indeed, any given state, from our tests.

Third, the SOX Act, enacted by Congress in 2002, substantially modified the corporate environment and disclosure requirements in regard to insider trading (our main sample starts in 2000). In particular, Section 403 requires insiders to report their trades to the SEC on Form

4 within two business days, which significantly increases the timeliness of insider trading reports. Until August 2002, the requirement was to file the form within 10 days of the close of the calendar month in which the transaction had occurred. Our untabulated results indicate that our conclusions hold if we restrict our sample to the post-SOX era.

Fourth, we use firm year–level data to indicate that breaches are occurring at that level. Consequently, we use the effective year rather than the effective date of state laws in our main specification because most controls and cross-sectional partitioning variables are at the firm-year level. To investigate whether this finer partition affects our results, we also estimate our baseline model at the trade level, thus allowing us to use the effective date of the law to measure the treatment period. Our untabulated results indicate that our conclusions hold.

Finally, our baseline model uses the location of the headquarters (identified from the firm's 10K reports) to determine whether a firm has been affected by a data breach law.[20] We adopted this design choice for two reasons. First, courts often favor the law of the state in which the headquarters are located. Second, most state laws require disclosures only when the number of affected records exceeds certain thresholds in the state (e.g., Jones 2014; Steinmeyer and Freeman 2016). It is more probable for these thresholds to be exceeded in the states in which the data are likely to be stored. To mitigate the potential effect of this assumption, we use subsidiary data from Exhibit 21 to identify firms' business locations.[21] These data capture the states and countries in which a firm discloses material subsidiaries, as required by the SEC.[22] In this alternative specification, we use the first affected state, instead of the headquarter state, as our identification strategy.

[20] Our main results hold if we use the location from Compustat instead of the one reported in the 10K reports.
[21] The SEC requires firms to disclose the name and jurisdiction of incorporation for all significant subsidiaries locations in Exhibit 21 of the Form 10-K, providing the most granular publicly available disclosure of the company's operations.
[22] Item 601 of SEC Regulation S-K (§229.601), cited as 17 CFR 229.601(b) (21), requires that registrants list all of their significant subsidiaries in Exhibit 21 of their 10K filling. The data are available until 2014.

To validate our approach, we identify a list of data breaches using the Private Rights Clearinghouse's Chronology of Data Breaches (e.g., "Privacy Database," hereafter, Romanosky, Hoffman, and Acquisti 2014).[23] We merge this list with our sample of firms for which we have an Exhibit 21 and insider trading data. In support of our approach, close to two-thirds of the breaches occurred in the state in which the firms are headquartered, and the vast majority (80%) of the breaches happened in a state referenced in an Exhibit 21. Further, the average number of leaked records is 10 times larger if the breach occurs in a state that is flagged in Exhibit 21 compared with breaches in unflagged states.

We then replicate our baseline specification using an alternative definition of *Post*. We define *Post 21* as an indicator variable equal to 1 if the firm's headquarters or a material subsidiary are located in a state that has implemented the data breach law, and 0 otherwise. The results are reported in the first column of Panel B of Table 5

Consistent with the idea that the location of the headquarters plays a disproportionate role, our baseline finding continues to hold but is weaker in this alternative approach. Next, we create a variable that better captures the importance of the laws for a firm. To this end, we define a continuous variable—*Post 21 Weight*—as the proportion of affected states' population over all operating states' population. The denominator is the sum of the population of all states in which a firm reports material subsidiaries. The numerator is the population in states that have already implemented the laws and in which the firm reports material subsidiaries. The results reported in column two indicate that our baseline finding continues to hold.

< INSERT TABLE 5>

5. Channels

[23] The data can be found at http://www.privacyrights.org/data-breach. Sources for the database include the Open Security Foundation listserve, Databreaches.net, Personal Health Information Privacy, National Association for Information Destruction, and the California Attorney General.

5.1 Cyber-investment.

One intended objective of data breach notification laws is to encourage firms to improve their cybersecurity posture and thus to reduce cyber-related risks. We expect this to be true when firms have greater incentives to correct the underlying risk. We next investigate whether firms increase cyber investment once a data breach law has been passed. We use SEC filings and press releases to capture firms' investments in cybersecurity. Appendix C lists the specific keywords we use.[24]

To measure the legal incentives to engage in this investment, we measure the strictness of law. As discussed in Section II, data breach laws vary in their stringency and specificity. The strictness of breach laws can have a differential impact on insiders' incentives or opportunities to avoid losses stemming from the disclosure of data breaches (e.g., Meyer and Rowan 1977; Fung, Graham, and Weil 2007). Building on past research (e.g., Joerling 2010; Peters 2014; Romanosky, Teland, and Acquisti 2011; Shaw 2010), we consider four key dimensions: (a) whether a law explicitly allows enforcement by the state Attorney General, (b) whether a law imposes an explicit deadline by which firms must disclose a data breach after it has been discovered, (c) whether a law specifies explicit penalties for violating it, and (d) whether a law specifies the disclosure items in details.[25] We first create an indicator for the different categories and assign a value of 1 to each indicator when the relevant condition is met (0 otherwise). We then construct an index (*Law Index*) by totaling the four indicators. We then create two indicator variables, *Strict Post* (equals 1 if *Post* equals 1 and *Law Index* is equal to

[24] We assume that a firm continues to engage in a material cyber-investment in the three years following its announcement.

[25] Some of the laws have been amended since their original implementation. To avoid adding noise and confounding factors, we focus on data breach laws at their first effective dates and in the forms in which they are first implemented, rather than their amended editions.

or greater than the median, and 0 otherwise) and *Weak Post* (equals 1 if *Post* equals 1 and *Law Index* is lower than the median, and 0 otherwise).

Column 1 of Panel A of Table 6 shows that data breach laws increase cyber investments, but the effect is significant only for firms that are located in states with more stringent versions. We find no similar effect for those located in states with less stringent laws. This result suggests that firms covered by strong laws internalize the cost of privacy breaches and respond by improving their security posture. This was the intended objective of these laws.

Furthermore, we investigate whether firms that have greater exposure to breach risk are more likely to increase their cyber investments under the new regime. We expect that these firms are more sensitive to the potential revelation of future breaches. As a result, they should have higher incentives to improve their cyber security hoping to reduce future breach incidents and related news disclosures. As expected, results presented in columns (2) and (3) show that firms with greater breach risk (captured by *Post Breach Risk* and *Post Relevance*) have more cyber investment after the implementation of the breach laws. Finally, the last column shows that that trading profits are higher for firms that do not increase their cyber-investment after the passage of the laws.

< INSERT TABLE 6>

5.2. Channels

We then connect our different findings by investigating the associations between cyber investment, (ex ante) breach risk, (ex post) breaches, price skewness, and insider trading profits.

We report the results of this analysis in Panel B of Table 6. In columns 1 and 2, we use *Breach* as defined above (i.e., those identified in the Private Rights Clearinghouse database).

For these tests, we restrict the sample to the post-2005 period, as the data on breaches are not available prior to that year. Breaches measure the manifestations of realized risk that impact prices, but we note that changes in risk perception—for example, if peer firms are breached—can have a similar effect. We continue to use *Relevance* and *Breach Risk* to measure the ex ante risk. We investigate the effect of (ex post) breaches and of the (ex ante) risk on prices by considering the skewness of the distribution.[26] To this end, we define *Ncskew* as the third moment of firm-specific weekly returns for each sample year (multiplied by minus one) and divided by the standard deviation of firm-specific weekly returns raised to the third power (e.g., Chen, Hong, and Stein 2001). Finally, we connect sudden drops in prices (measured by the distribution's skewness) with insider trading profit.

Our results in Column 1 indicate that the likelihood of a breach occurring is higher when firms do not announce an increase in their cyber investment. Columns 2, 3, and 4 indicate that breaches and breach risk affect returns and lead to idiosyncratic crashes (this result is consistent with Florackis et al. (2020) who find that 10K discussions of breach risk is associated with a higher likelihood of future idiosyncratic crashes), which in turn translate into trading opportunities (column 5). Untabulated results indicate that *Relevance* is significantly associated with the presence of breaches (*Breach Risk* is mechanically correlated with *Breach*). As discussed above, Table 4 shows that trading profitability is higher when the firm-level breach risk is higher in the cross-section while Florackis et al. (2020) show that breach risk affects prices in the time series. Taken together, these findings suggest that state-level breach regulations influence managers' trading behavior through their effect on firms' cyber investments and return distributions.

6. Conclusions

[26] We do not include firm-fixed effects when *Relevance* and *Breach Risk* are the dependent variables as these variables are slow moving. We do include them when we consider *Breach*.

The growing frequency and size of data breaches in recent years have increased regulators' concerns about information security and disclosure. Recent cases of data breaches followed by insider trading on related nonpublic information have also raised concerns that insiders might trade on their private information about cyber risks and data breaches (e.g., Equifax). Using the staggered adoption of data breach laws across different states, we test whether the mandated disclosure of bad news affects insiders' selling behavior. Our findings indicate that mandated data breach disclosures have prompted insiders to sell their shares to avoid future losses, likely due to the fear that breach disclosures will put downward pressure on stock prices. Firms that are located in states in which the laws are relatively stricter have experienced an increase in cyber security investment. In essence, these different results suggest that strong laws incentivize firms to take corrective actions to minimize the risk of data leakages. However, these disclosure laws were not designed to enhance the functioning of financial markets but, rather, to help consumers and citizens to better handle the perils of data breaches. Interestingly, they had some negative consequences on the integrity of financial markets.

References

Acharya, V. V., and T. C. Johnson. 2010. "More Insiders, More Insider Trading: Evidence from Private-Equity Buyouts." *Journal of Financial Economics*.

Ahern, K. R. 2017. "Information Networks: Evidence from Illegal Insider Trading Tips." *Journal of Financial Economics* 125, 1, 26-47.

Ali, Usman, and David Hirshleifer. 2017. "Opportunism as a Firm and Managerial Trait: Predicting Insider Trading Profits and Misconduct." *Journal of Financial Economics* 126(3), 490-515.

Alldredge, Dallin M., and David C. Cicero. 2015. "Attentive Insider Trading." *Journal of Financial Economics* 115(1), 84-101.

Amir, E., S. Levi, and T. Livne. 2019. *Insider Trading and Disclosure: The Case of Cyberattacks*. Unpublished working paper. Tel Aviv University.

Ashraf, M., and J. Sunder. 2019. *Consumer Protection Regulation and the Cost of Equity: Evidence from Data Breach Disclosure Laws*. Unpublished working paper.

Badertscher, Brad A., S. Paul Hribar, and Nicole Thome Jenkins. 2011. "Informed Trading and the Market Reaction to Accounting Restatements." *Accounting Review*.

Benston, G. J. 1973. "Required Disclosure and the Stock Market: An Evaluation of the Securities Exchange Act of 1934." *American Economic Review* 63: 132–55.

Berger, Philip G. 2011. "Challenges and Opportunities in Disclosure Research: A Discussion of 'The Financial Reporting Environment: Review of the Recent Literature.'" *Journal of Accounting and Economics*.

Bernile, Gennaro, Jianfeng Hu, and Yuehua Tang. 2016. "Can Information Be Locked Up? Informed Trading Ahead of Macro-News Announcements." *Journal of Financial Economics*.

Bertrand, Marianne, and Sendhil Mullainathan. 2003. "Enjoying the Quiet Life? Corporate Governance and Managerial Preferences." *Journal of Political Economy* 111(5), 1043-1075.

Bettis, J. C., J. L. Coles, and M. L. Lemmon. 2000. "Corporate Policies Restricting Trading by Insiders." *Journal of Financial Economics* 57(2), 191-220.

Brochet, Francois. 2010. "Information Content of Insider Trades before and after the Sarbanes–Oxley Act." *Accounting Review* 85(2), 419-446.

Chen, Chen, Xiumin Martin, and Xin Wang. 2013. "Insider Trading, Litigation Concerns, and Auditor Going-Concern Opinions." *Accounting Review*.

Chi, Sabrina S., Morton Pincus, and Siew Hong Teoh. 2014. "Mispricing of Book-Tax Differences and the Trading Behavior of Short Sellers and Insiders." *Accounting Review* 89(2), 511-543.

Cohen, Lauren, Christopher Malloy, and Lukasz Pomorski. 2012. "Decoding Inside

Information." *Journal of Finance* 67(3), 1009-1043.

Dai, Lili, Renhui Fu, Jun Koo Kang, and Inmoo Lee. 2016. "Corporate Governance and the Profitability of Insider Trading." *Journal of Corporate Finance* 40, 235-253.

Dai, Lili, Jerry T. Parwada, and Bohui Zhang. 2015. "The Governance Effect of the Media's News Dissemination Role: Evidence from Insider Trading." *Journal of Accounting Research* 53(2), 331-366.

Dechow, P. M., Lawrence, A., & Ryans, J. P. (2016). SEC comment letters and insider sales. *Accounting Review*.

Denis, David J., and Jin Xu. 2013. "Insider Trading Restrictions and Top Executive Compensation." *Journal of Accounting and Economics*.

Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michael Weber. 2020. "Cybersecurity Risk." *SSRN Electronic Journal*.

Fung, Archon, Mary Graham, and David Weil. 2007. *Full Disclosure: The Perils and Promise of Transparency*. *Full Disclosure: The Perils and Promise of Transparency*.

Gao, Feng, Ling Lei Lisic, and Ivy Xiying Zhang. 2014. "Commitment to Social Good and Insider Trading." *Journal of Accounting and Economics*.

Gao, Feng, Joanna Shuang Wu, and Jerold 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.

Gao, M., and J. Huang. 2016. "Capitalizing on Capitol Hill: Informed Trading by Hedge Fund Managers." *Journal of Financial Economics* 121, no. 3: 521–545.

Garfinkel, Jon A. 1997. "New Evidence on the Effects of Federal Regulations on Insider Trading: The Insider Trading and Securities Fraud Enforcement Act (ITSFEA)." *Journal of Corporate Finance* 3 (2), 89-111.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-Risk Disclosure: Who Cares? In SSRN.

Hoberg, G., and G. Phillips. 2016. "Text-Based Network Industries and Endogenous Product Differentiation." *Journal of Political Economy* 124, no. 5: 1423–1465.

Huddart, Steven J., and Bin Ke. 2007. "Information Asymmetry and Cross-Sectional Variation in Insider Trading." *Contemporary Accounting Research*.

Jagolinzer, Alan D., David F. Larcker, and Daniel J. Taylor. 2011. "Corporate Governance and the Information Content of Insider Trades." *Journal of Accounting Research*.

Jenter, Dirk. 2005. "Market Timing and Managerial Portfolio Decisions." *Journal of Finance* 60(4), 1903-1949.

Jin, Li, and S. P. Kothari. 2008. "Effect of Personal Taxes on Managers' Decisions to

Sell Their Stock.” *Journal of Accounting and Economics*.

Joerling, Jill. 2010. "Data breach notification laws: an argument for a comprehensive federal law to protect consumer data." *Wash. UJL & Pol'y 32, 467.*

Jones, H. 2014. *Pitfalls of Choice of Law Clauses in Employment Contracts*. HR.BLR.com, Brentwood, TN. https://hr.blr.com/HR-news/Staffing-Training/Employment-Contracts/Pitfalls-of-choice-of-law-clauses-in-employment-co/Jones 2014/

Kallunki, Juha Pekka, Henrik Nilsson, and Jörgen Hellström. 2009. “Why Do Insiders Trade? Evidence Based on Unique Data on Swedish Insiders.” *Journal of Accounting and Economics* 130(1), 135–165.

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. Stulz, 2020. “Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms.” *Journal of Financial Economics* (forthcoming).

Ke, Bin, Steven Huddart, and Kathy Petroni. 2003. “What Insiders Know about Future Earnings and How They Use It: Evidence from Insider Trades.” *Journal of Accounting and Economics* 35(3), 315-346.

Klasa, Sandy, Hernán Ortiz-Molina, Matthew Serfling, and Shweta Srinivasan. 2018. “Protection of Trade Secrets and Capital Structure Decisions.” *Journal of Financial Economics* 128(2), 266-286.

Lakonishok, Josef, and Inmoo Lee. 2001. “Are Insider Trades Informative?” *Review of Financial Studies* 14(1), 79-111.

Lenkey, Stephen L. 2014. “Advance Disclosure of Insider Trading.” *Review of Financial Studies* 27(8), 2504-2537.

Leuz, Christian, and Peter D. Wysocki. 2016. “The Economics of Disclosure and Financial Reporting Regulation: Evidence and Suggestions for Future Research.” *Journal of Accounting Research*.

Lin, Zhaoxin, Travis R.A. Sapp, Jackie Rees Ulmer, and Rahul Parsa. 2020. “Insider Trading Ahead of Cyber Breach Announcements.” *Journal of Financial Markets*.

Loughran, T., and B. McDonald. 2011. “When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks.” *The Journal of Finance* 66, no. 1: 35–65.

Marin, Jose M., and Jacques P. Olivier. 2008. “The Dog That Did Not Bark: Insider Trading and Crashes.” *Journal of Finance*.

Matthews, S., and A. Postlewaite. 1985. “Quality Testing and Disclosure.” *Rand Journal of Economics* 16: 328–340.

Massa, Massimo, Wenlan Qian, Weibiao Xu, and Hong Zhang. 2015. “Competition of the Informed: Does the Presence of Short Sellers Affect Insider Selling?” *Journal of Financial Economics*.

Meyer, John W., and Brian Rowan. 1977. “Institutionalized Organizations: Formal

Structure as Myth and Ceremony." *American Journal of Sociology* 83(2), 340-363.

Peters, R. M. 2014. "So You've Been Notified, Now What: The Problem with Current Data-Breach Notification Laws." *Arizona Law Review* 56, no. 4: 1171–1202.

Piotroski, Joseph D., and Darren T. Roulstone. 2005. "Do Insider Trades Reflect Both Contrarian Beliefs and Superior Knowledge about Future Cash Flow Realizations?" *Journal of Accounting and Economics*.

Ravina, E., and P. Sapienza. 2010. "What Do Directors Know? Evidence from Their Trading." *Review of Financial Studies* 23: 962–1003.

Roberts, M. R., & Whited, T. M. (2013). Endogeneity in Empirical Corporate Finance. *In Handbook of the Economics of Finance.*

Romanosky, S., R. Telang, and A. Acquisti. 2014. "Empirical Analysis of Data Breach Litigation." *Journal of Empirical Legal Studies* 11, no. 1: 74–104.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management* 30(2), 256-286.

Roulstone, Darren T. 2003. "The Relation between Insider-Trading Restrictions and Executive Compensation." *Journal of Accounting Research*.

Rozeff, Michael S., and Mir A. Zaman. 1998. "Overreaction and Insider Trading: Evidence from Growth and Value Portfolios." *Journal of Finance* 53(2), 701-716.

Ryan, Stephen G., Jennifer Wu Tucker, and Ying Zhou. 2016. "Securitization and Insider Trading." *Accounting Review*.

Seyhun, H. Nejat. 1986. "Insiders' Profits, Costs of Trading, and Market Efficiency." *Journal of Financial Economics* 16(2), 189-212.

Shavell, S. 1994. "Acquisition and Disclosure of Information Prior to Sale." *The Rand Journal of Economics* 25: 20–36.

Shaw, Abraham. 2010. "Data Breach: From Notification to Prevention Using PCI DSS." *Columbia Journal of Law & Social Problems* 43, 517-562.

Skaife, Hollis A., David Veenman, and Daniel Wangerin. 2013. "Internal Control over Financial Reporting and Managerial Rent Extraction: Evidence from the Profitability of Insider Trading." *Journal of Accounting and Economics* 55(1), 91-110.

Steinmeyer, P. A., and S. Freeman. 2016. *In Today's Environment, What Is Adequate Consideration for a Restrictive Covenant Signed by an Existing Employee? Epstein Becker & Green, P.C.* https://www.natlawreview.com/article/today-s-environment-what-adequate-consideration-restrictive-covenant-signed-existing

Tian, Xiaoli Shaolee. 2015. "Does Real-Time Reporting Deter Strategic Disclosures by Management? The Impact of Real-Time Reporting and Event Controllability on Disclosure Bunching." *Accounting Review*.

US Securities and Exchange Commission. February 26, 2018. *Commission Statement* *and Guidance on Public Company Cybersecurity Disclosures*. https://www.sec.gov/rules/interp/2018/33-10459.pdf

Veenman, David. 2012. "Disclosures of Insider Purchases and the Valuation Implications of Past Earnings Signals." *Accounting Review*.

Appendix A: Time Distribution of the Implementation of Data Breach Notification Laws by State

Effective Year	*States*
2003	CA
2004	
2005	WA, AR, DE, GA, NY, NC, ND, TN
2006	WI, MN, MT, PA, PR, RI, OH, CO, CT, AZ, ID, IL, IN, NE, NV, NJ, LA, ME
2007	WY, DC, MA, MI, NH, HI, OR, UT, KS
2008	IA, OK, MD, WV,VA
2009	AK, MO, TX, SC
2010	
2011	MS
2012	VT
2013	
2014	FL, KY
2015	
2016	
2017	NM
2018	AL, SD

This table displays the year in which each state originally implemented a data breach law.

Appendix B: Variable Definitions

Variables	Descriptions
Sell Profits	Market-adjusted (CRSP value-weighted index as market portfolio) abnormal return over 12 months following the trade, multiplied by the value of trade (in millions of dollars). We multiply this value by -1.
Post	Equals 1 if firm i's year t is after firm i's home state j has implemented a data breach law, and 0 otherwise.
Post 21	Equals 1 if the firm's headquarters or material subsidiaries are located in a state that mandates the disclosure of data breaches, and 0 otherwise.
Post 21 Weight	A continuous variable that uses the proportion of affected states' population over all operating states' population to measure the coverage of disclosure laws.
Size	Natural log of firm i's market value of equity in the year over which trading is measured.
Book-to-Market Ratio	The book value of equity divided by market capitalization.
Loss	Equals 1 if a firm reports negative net income in year t, and 0 otherwise.
R&D Dummy	Equals 1 if a firm has positive R&D expenses, and 0 otherwise.
Dividend	Cash dividends scaled by shareholders' equity (SEQ).
Return Volatility	The standard deviation of daily stock returns during the fiscal year.
Relevance	Equals to 1 if firm has a chief technology officer, chief information officer, chief security officer, chief information security officer, in the top management team, and 0 otherwise.
Breach Risk	Equals to 1 if the firm is facing a high ex ante risk of databreach, and 0 otherwise. We first identify a list of data breach disclosures in year t from http://www.privacyrights.org/data-breach. We then find each data breach firm's peer firm in data breach disclosure year window [-3, 3] based on Hoberg and Phillips (2016)'s products similarity measure (calibrated to be as granular as three-digit SIC codes). We classify data breach firms and their peer firms as high data breach risk firms in year t, and rest firms as low risk firms.
Law Index	Constructed based on four dimensions of data breach disclosure law intensity: (a) whether a law requires the firm to notify the Attorney General and allows the Attorney General to bring law suits, (b) whether a law imposes an explicit deadline by which firms must disclose a data breach after it has been discovered, (c) whether a law specifies explicit penalties for violating it, and (d) whether a law specifies the details of the disclosure items. We assign each of the above

	dimensions a value of 1 or 0 and total the four indicator variables.
Strict Post	Equals 1 if *Post* equals 1 and *Law Index* is equal to or greater than the median value, and 0 otherwise.
Weak Post	Equals 1 if *Post* equals 1 and *Law Index* is smaller than the median value, and 0 otherwise.
Post Breach Risk	Equals to 1 if *Post* equals 1 and *Breach Risk* equals to 1, and 0 otherwise.
Post Relevance	Equals to 1 if *Post* equals 1 and *Relevance* equals to 1, and 0 otherwise.
Post no Breach Risk	Equals to 1 if *Post* equals 1 and *Breach Risk* equals to 0, and 0 otherwise.
Post no Relevance	Equals to 1 if *Post* equals 1 and *Relevance* equals to 0, and 0 otherwise.
Ncskew	The negative of the third moment of firm-specific weekly returns for each sample year divided by the standard deviation of firm-specific weekly returns raised to the third power (Chen, Hong, and Stein 2001; Kim, Li, and Zhang 2011).
Cyberinvest	Equals 1 for year t to t+2 if a firm announces that it invests in a cyber security-related program in year t, and 0 otherwise.
No Cyberinvest	Equals 1 for year t to t+2 if a firm *does not* announce that it invests in a cyber security-related program in year t, and 0 otherwise.
Post No Invest	Equals to 1 if a firm is headquartered in a state that effectuates the data breach disclosure law but does not increase to invest in cyber security-related issues after the mandates, and 0 otherwise.
Post Invest	Equals to 1 if a firm is headquartered in a state which effectuates the data breach disclosure law and invest in cyber security-related issues after the mandates, and 0 otherwise.
Breach	Equals 1 if a firm experienced a data breach incident in year t+1, and 0 otherwise
Post High Ncskew	Equals 1 if a firm is headquartered in a state that effectuates the data breach disclosure law and experiences a large increase in negative stock price skewness, and 0 otherwise.
Post Low Ncskew	Equals 1 if a firm is headquartered in a state that effectuates the data breach disclosure law and experiences a small increase in negative stock price skewness, and 0 otherwise.

Appendix C

To identify material investment programs in cybersecurity, we use the following search terms: invest in data protection, investment in data protection, investing in data protection, data protection investment, invest in data security, investment in data security, investing in data security, data security investment, invest in cybersecurity, investment in cybersecurity, investing in cybersecurity, cybersecurity investment, invest in cyber, investment in cyber, investing in cyber, cyber investment, invest in hack, investment in hack, investing in hack, hack investment, invest in data breach, investment in data breach, investing in data breach, data breach investment, invest in protecting data, investment in protecting data, investing in protecting data, protecting data investment, invest in protecting information, investment in protecting information, investing in protecting information, protecting information investment, invest in internet security, investment in internet security, investing in internet security, and protecting internet security.

Table 1

Insider Trading Sample Selection Process

Description	**Obs.**
Thomson Reuters Insider Trading Database Form 4 open market sales and aggregates at firm-year level (2000–2017)	31,249
Less: Merge with COMPUSTAT	(1,425)
Less: Observations in "NM," "AL" and "SD" states and missing headquarters from 10-K reports	(757)
Less: Missing control variables	(1,028)
Total firm-year observations	28,039
Total number of unique firms	4,892

Table 2
Descriptive Statistics and Correlations

Panel A of Table 2 A reports the summary statistics for the key variables for the full sample for the 2000 to 2017 period. Panel B presents the Pearson correlations, with the correlation coefficients with a significance level of 0.05 or better in bold. All the continuous variables are winsorized to the 1st and 99th percentiles of their distributions. *Sell Profits* is the market-adjusted (CRSP value-weighted index as market portfolio) abnormal return over the 12 months following the trade, multiplied by the value of the trade (in millions of dollars). This value is multiplied by -1 so that the losses avoided on sales have a positive sign. *Post* is an indicator variable equal to 1 if the firm is headquartered in a state that implements the data breach law, and 0 otherwise. *Loss* is an indicator variable that is equal to 1 if a firm reports a negative net income in year t. *R&D Dummy* is an indicator variable that is equal to 1 if a firm has positive R&D expenses. *Book-to-Market Ratio* is the book value of equity divided by market pitalizations. *Size* is the natural log of firm i's market value of equity in the year over which trading is measured. *Dividend* is cash dividend scaled by SEQ. *Return Volatility* is the standard deviation of daily stock returns over the fiscal year.

Panel A: Descriptive Statistics for Insider Trading Sample

Variables	N	Mean	Std. Dev.	Q1	Median	Q3
Test Variable						
Post	28,039	0.675	0.468	0.000	1.000	1.000
Dependent Variables						
Sell Profits	28,039	0.205	5.039	-0.102	0.023	0.408
Control Variables						
Loss	28,039	0.292	0.455	0.000	0.000	1.000
R&D Dummy	28,039	0.565	0.496	0.000	1.000	1.000
Book-to-Market Ratio	28,039	0.476	0.413	0.222	0.394	0.641
Size	28,039	6.672	1.851	5.429	6.603	7.835
Dividend	28,039	0.025	0.066	0.000	0.000	0.023
Return Volatility	28,039	0.032	0.017	0.020	0.027	0.039

Panel B: Pearson Correlation Coefficients (n = 28,039)

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
(1) Sell Profits	1.000							
(2) Post	**-0.044**	1.000						
(3) Loss	**0.034**	**-0.038**	1.000					
(4) R&D Dummy	**0.015**	**0.074**	**0.172**	1.000				
(5) Book-to-Market Ratio	**0.014**	**-0.092**	**0.064**	**-0.158**	1.000			
(6) Size	-0.006	**0.201**	**-0.308**	0.009	**-0.339**	1.000		
(7) Dividend	**-0.014**	**0.068**	**-0.142**	**-0.043**	**-0.153**	**0.220**	1.000	
(8) Return Volatility	**0.085**	**-0.269**	**0.435**	**0.112**	**0.129**	**-0.500**	**-0.188**	1.000

Table 3
Effect of Data Breach Laws on Insiders' Selling Profits

This table reports the results of the ordinary least square (OLS) regressions of insiders' trading behaviors on the indicator for the implementation of the data breach law. Panel A reports the main effect, Panel B reports the results of the parallel trend analysis. *Sell Profits* is the market-adjusted (CRSP value-weighted index as market portfolio) abnormal return over the 12 months following the trade, multiplied by the value of the trade (in millions of dollars). This value is multiplied by -1 so that the loss avoided on sales has a positive sign. *Post* is an indicator variable that is equal to 1 if the firm is headquartered in a state that has implemented the data breach law, and 0 otherwise. *Effective*$^{-2}$, *Effective*$^{-1}$, *Effective*^{0}, *Effective*$^{+1}$, and *Effective*$^{+2}$ are equal to 1 if the firm is headquartered in a state that will implement the data breach law in two years, will implement the law in one year, is implementing the law, implemented the law one year ago, implemented the law two or more years ago, respectively, and 0 otherwise. *Loss, R&D Dummy, Book-to-Market Ratio, Size, Dividend, and Return Volatility* are defined in Appendix B. Firm-fixed and year-fixed effects are included. All the continuous variables are winsorized to the 1st and 99th percentiles. Standard errors are corrected for heteroskedasticity and clustering at the state level (robust standard errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

Panel A: Main Effect of the Breach Laws

Variables	*Sell Profits*
Post	0.282***
	(0.104)
Loss	0.202***
	(0.069)
R&D Dummy	-0.057
	(0.186)
Book-to-Market Ratio	0.735***
	(0.116)
Size	0.869***
	(0.198)
Dividend	-0.014
	(0.695)
Return Volatility	33.198***
	(8.058)
Observations	28,039
R-squared	0.202
Firm FE	YES
Year FE	YES
Cluster at State	YES

Panel B: Parallel Trend Analysis

Variables	*Sell profits*
Effective^{-2}	0.248
	(0.184)
Effective^{-1}	0.095
	(0.248)
Effective^{0}	0.373**
	(0.175)
Effective^{+1}	0.426**
	(0.166)
Effective^{+2}	0.499**
	(0.211)
Loss	0.203***
	(0.070)
R&D Dummy	-0.060
	(0.184)
Book-to-Market Ratio	0.733***
	(0.116)
Size	0.868***
	(0.199)
Dividend	-0.017
	(0.695)
Return Volatility	33.054***
	(8.175)
Observations	28,039
R-squared	0.202
Firm FE	YES
Year FE	YES
Cluster at State	YES

Table 4
Ex Ante Data Breach Risk

This table reports the results of the ordinary least square (OLS) regressions of insiders' trading behaviors on the indicator for the implementation of the data breach law, conditional on firms' ex ante data breach risk. *Relevance* is equal to 1 if firm has a chief technology officer, chief information officer, chief security officer, chief information security officer, in the top management team, 0 otherwise. *Breach Risk* is an indicator variable equal to 1 if the firm is facing a high ex ante risk of data breach, 0 otherwise. A firm is classified as such if it has been breached in years in a window encompassing the prior three years and the subsequent three years or one of its peers has been breached. *Loss, R&D Dummy, Book-to-Market Ratio, Size, Dividend, and Return Volatility* are defined in Appendix B. Firm-fixed and year-fixed effects are included. All the continuous variables are winsorized to the 1st and 99th percentiles. Standard errors are corrected for heteroskedasticity and clustering at the state level (robust standard errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

	Relevance =1	*Relevance =0*	*Breach Risk=1*	*Breach Risk=0*
	Sell Profits	*Sell Profits*	*Sell Profits*	*Sell Profits*
Post	0.928***	0.099	0.576***	0.145
	(0.286)	(0.143)	(0.197)	(0.138)
Loss	0.131	0.261**	-0.018	0.330**
	(0.139)	(0.109)	(0.122)	(0.138)
R&D Dummy	-0.249	0.136	-0.148	-0.083
	(0.595)	(0.225)	(0.504)	(0.197)
Book-to-market Ratio	1.077**	1.063***	0.623***	0.844***
	(0.438)	(0.247)	(0.162)	(0.227)
Size	1.364***	0.993***	0.600***	1.050***
	(0.302)	(0.256)	(0.115)	(0.375)
Dividend	-0.018	0.654	0.506	-0.204
	(1.173)	(1.145)	(0.878)	(0.826)
Return Volatility	82.405***	38.647***	15.802***	32.862***
	(27.469)	(8.703)	(5.313)	(10.622)
	(1)	(2)	(1)	(2)
P-value: (1)-(2)	0.018		0.024	
Observations	4,613	12,305	13,522	14,517
R-squared	0.277	0.151	0.217	0.334
Firm FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Cluster at State	YES	YES	YES	YES

Table 5

Placebo and Robustness Tests

Panel A of Table 5 reports the results of the OLS regressions of our baseline model for routine sales, insider purchases, and financial institutions. Routine insiders are those who have traded in the same month for at least the past three consecutive years, and the remainder are nonroutine insiders. The second column reports the results of the OLS regression of *Buy Profits* on indicators for the mandates of states' data breach laws. *Buy Profits* is the market-adjusted (CRSP value-weighted index as market portfolio) abnormal return over 12 months following the trade multiplied by the value of trade (in millions of dollars). In Panel B of Table 4, we use Exhibit 21 to identify firms' material subsidiaries and the data available until 2014. *Post 21* is an indicator variable that is equal to 1 if the firm's headquarters or material subsidiaries are located in a state that mandates the disclosure of data breaches, and 0 otherwise. *Post 21 Weight* is a continuous variable that uses the proportion of affected states' population over all operating states' population to measure the coverage of disclosure laws. All the continuous variables are winsorized at the 1st and 99th percentiles. Standard errors are corrected for heteroskedasticity and clustering at the state level (robust standard errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

Panel A: Routine Sales, Insider Purchase, and Financial Institutions

Variables	*Routine* *Sell Profits*	*Purchase* *Buy Profits*	*Financial Institutions'* *Sell Profits*
Post	0.129	-0.007	-0.076
	(0.167)	(0.007)	(0.283)
Loss	0.056	-0.022**	0.034
	(0.206)	(0.009)	(0.348)
R&D Dummy	-0.319	-0.024	-0.654***
	(0.309)	(0.020)	(0.082)
Book-to-Market Ratio	0.785***	0.000**	
	(0.215)	(0.000)	
Size	0.524***	-0.006	0.010
	(0.119)	(0.006)	(0.115)
Dividend	0.136	-0.008	0.941
	(1.282)	(0.006)	(1.057)
Return Volatility	16.320	0.133	2.336
	(10.918)	(0.214)	(2.926)
Observations	5,348	17,629	1,861
R-squared	0.260	0.250	0.274
Firm FE	YES	YES	YES
Year FE	YES	YES	YES
Cluster at State	YES	YES	YES

Panel B: Identification Using Subsidiary Data from Exhibit 21

Variables	*Sell Profits*	*Sell Profits*
Post 21	0.103**	
	(0.043)	
Post 21 Weight		0.540**
		(0.205)
Loss	0.172**	0.160**
	(0.070)	(0.072)
R&D Dummy	0.123	0.130
	(0.285)	(0.289)
Book-to-Market Ratio	0.632***	0.629***
	(0.108)	(0.115)
Size	0.889***	0.885***
	(0.190)	(0.189)
Dividend	0.794	0.767
	(0.576)	(0.592)
Return Volatility	31.215***	31.059***
	(7.768)	(7.767)
Observations	19,845	19,845
R-squared	0.253	0.254
Firm FE	YES	YES
Year FE	YES	YES
Cluster at State	YES	YES

Table 6

Channels

Panel A: Effects of Data Breach Laws and Breach Risk on Cyber Investment

This table reports the results of the OLS regressions of *Cyberinvest* on the indicators of the timing of the state's implementations of the data breach law. *Law Index* is constructed based on the following four dimensions of data breach disclosure law intensity: (a) whether a law requires the firm to notify the Attorney General and allows the Attorney General to bring law suits, (b) whether a law imposes an explicit deadline by which firms must disclose a data breach after it has been discovered, (c) whether a law specifies explicit penalties for violating it, and (d) whether a law specifies the details of the disclosure items. We assign the value of 1 or 0 to each of these dimensions and total these four indicator variables. *Strict Post* equals 1 if *Post* equals 1 and *Law Index* is equal to or greater than their medians, and 0 otherwise. Conversely, *Weak Post* equals 1 if *Post* equals 1 and *Law Index* is smaller than the median value, and 0 otherwise. *Cyberinvest* Equals 1 for year t to t+2 if a firm announces that it invests in a cyber security-related program in year t, and 0 otherwise. *Post Breach Risk* is is an indicator variable equal to one if *Post* equals 1 and *Breach Risk* equals to 1, 0 otherwise. *Post no Breach Risk* is is an indicator variable equal to 1 if *Post* equals 1 and *Breach Risk* equals to 0, and 0 otherwise. *Post Relevance* is is an indicator variable equal to one if *Post* equals 1 and *Relevance* equals to one, zero otherwise. *Post no Relevance* is is an indicator variable equal to 1 if *Post* equals 1 and *Relevance* equals to 0, and 0 otherwise. *Post No Invest* is an indicator variable equal to one if *Post* equals 1 but does not increase to invest in cyber security-related issues after the mandates, and 0 otherwise. *Post Invest* is an indicator variable equal to one if *Post* equals 1 and invest in cyber security-related issues after the mandates, and 0 otherwise. All the continuous variables are winsorized at the 1st and 99th percentiles. Standard errors are corrected for heteroskedasticity and clustering at the state level (robust standard errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

Variables	*Cyberinvest*	*Cyberinvest*	*Cyberinvest*	*Sell Profits*
Strict Post	0.010*			
	(0.006)			
Weak Post	0.002			
	(0.006)			
Post Breach Risk		0.018***		
		(0.005)		
Post Relevance			0.022*	
			(0.012)	
Post no Breach Risk		-0.002		
		(0.006)		
Post no Relevance			0.004	
			(0.006)	
Post No Invest				0.355***
				(0.116)
Post Invest				-0.239
				(0.329)
Loss	0.001	0.001	-0.001	0.200***
	(0.003)	(0.003)	(0.004)	(0.069)
R&D Dummy	-0.020**	-0.020**	-0.032**	-0.065
	(0.008)	(0.008)	(0.012)	(0.186)

Book-to-Market Ratio	0.000	-0.000	0.002	0.735***
	(0.006)	(0.006)	(0.010)	(0.116)
Size	-0.004	-0.004	-0.007	0.869***
	(0.003)	(0.003)	(0.006)	(0.198)
Dividend	0.088**	0.088**	0.123*	0.049
	(0.043)	(0.043)	(0.062)	(0.711)
Return Volatility	-0.084	-0.060	-0.165	33.016***
	(0.130)	(0.126)	(0.215)	(8.042)
Observations	28,039	28,039	16,918	28,039
R-squared	0.533	0.533	0.483	0.202
Firm FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Cluster at State	YES	YES	YES	YES

Panel B: Cyber Investment, Data Breach, Crash Risk, and Insider Selling Profits

This table reports results from OLS regressions. We examine the association between cyber-related investments, data breach, price skewness, and insider selling profits under states. The sample period for columns 1 and 2 is from 2005 to 2017 because breach incidents data are available from 2005 only. We define *Ncskew* as the third moment of firm-specific weekly returns for each sample year (multiplied by minus 1) divided by the standard deviation of firm-specific weekly returns raised to the third power. *No Cyberinvest* equals 1 for year t to t+2 if a firm does not announce that it invests in a cyber security-related program in year t, and 0 otherwise. *Breach* equals 1 if a firm experienced a data breach incident in year t+1, and 0 otherwise. *Relevance* is equal to 1 if firm has a chief technology officer, chief information officer, chief security officer, chief information security officer, in the top management team, 0 otherwise. *Breach Risk* is an indicator variable equal to 1 if the firm is facing a high ex ante risk of databreach, 0 otherwise. *Post High Ncskew* equals 1 if a firm is headquartered in a state that effectuates the data breach disclosure law and experiences a significant increase in negative stock price skewness, and 0 otherwise. *Post Low Ncskew* equals 1 if a firm is headquartered in a state that effectuates the data breach disclosure law and experiences a small increase in negative stock price skewness, and 0 otherwise. We correct standard errors for heteroskedasticity and clustering at the year and firm levels from column 1 to column 4, and state level for column 5 (robust standards errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

Variables	*Breach*	*Ncskew*	*Ncskew*	*Ncskew*	*Sell Profits*
No Cyberinvest	0.018**				
	(0.009)				
Breach		0.191***			
		(0.067)			
Relevance			0.033**		
			(0.017)		
Breach Risk				0.049***	
				(0.013)	
Post High Ncskew					0.542***
					(0.168)
Post Low Ncskew					-0.002
					(0.112)

Loss	0.000	0.025	0.005	0.076***	0.200***
	(0.002)	(0.025)	(0.021)	(0.015)	(0.068)
R&D Dummy	-0.002	-0.036	-0.021	-0.002	-0.079
	(0.001)	(0.064)	(0.015)	(0.012)	(0.185)
Book-to-Market Ratio	0.001	0.242***	0.122***	0.109***	0.725***
	(0.004)	(0.037)	(0.024)	(0.016)	(0.114)
Size	-0.001	-0.128***	0.006	0.023***	0.859***
	(0.002)	(0.020)	(0.005)	(0.004)	(0.195)
Dividend	-0.016	0.190	0.307***	0.042	-0.012
	(0.023)	(0.144)	(0.103)	(0.081)	(0.707)
Return Volatility	-0.087	-3.631***	4.183***	0.085	32.987***
	(0.083)	(1.399)	(0.854)	(0.619)	(7.878)
Observations	20,752	20,752	16,918	28,039	28,039
R-squared	0.241	0.197	0.013	0.012	0.202
Firm FE	YES	YES	NO	NO	YES
Year FE	YES	YES	YES	YES	YES
Cluster Firm/State	YES	YES	YES	YES	YES