Corporate Cybersecurity and the Impact of State-Level Cyber Laws

Jonathan Jona
University of New Mexico
jjona@unm.edu

Chao Li
University of New South Wales
k.li@unsw.edu.au

Naomi Soderstrom
University of Melbourne
198 Berkeley Street, Level 7
Parkville VIC 3000 Australia
naomiss@unimelb.edu.au

Keywords: Cybersecurity awareness; Disclosure; Market valuations; State Laws.

Acknowledgments:
We are grateful to Jackie Cook from CookESG Research for her help in extracting the cybersecurity excerpts. We have gained valuable insights from workshop participants at University of Auckland, University of Melbourne, and University of New South Wales - Canberra. We thank Rachel Solano for research assistance.

Corporate Cybersecurity and the Impact of State-Level Cyber Laws

Abstract

In the United States, laws at the federal level regarding cybersecurity have historically left cybersecurity protection primarily up to individual companies, with regulations focused more on disclosure of cyber events rather than on their prevention. Although the Federal approach to cybersecurity regulation is changing under the Biden administration, specific regulatory changes will take time to be developed and implemented. As a result of the approach to cybersecurity at the federal level, many states have passed their own cybersecurity laws. This paper explores how differences in corporate qualitative disclosures related to cybersecurity awareness impact how the market responds to passage of the laws. We argue that because the expected costs for companies to comply with the laws will vary according to the "business friendliness" of the state, the effect of law passage on market valuation will be stronger for democratic majority ("blue") states since laws in these states are likely to address different aspects of cybersecurity and are more likely to be enforced. Results are consistent with our expectations, with a more positive valuation for firms with existing cyber mitigation and results focused in blue states.

Corporate Cybersecurity and the Impact of State-Level Cyber Laws

1. Introduction

Cybersecurity has become a key issue throughout the world. There are significant increases in cybercrime that have "skyrocketed" during the Covid-19 pandemic.[1] In the US, federal government-driven protection from cybercrime has traditionally focused requirements only at the federal governmental level, leaving companies to develop their own cybersecurity strategies and policies (Barry et al. 2022). In 2023, the Biden administration signaled a shift in strategy at the Federal level, focusing on increased regulation for critical infrastructure owners and operators and software companies. However, this strategy is not fully formulated, and new regulations may take years to write and implement, likely requiring designation of additional authorities to oversee and help develop the new regulatory structure.[2] As a result of this lack of definitive leadership at the Federal level, many states have passed their own laws regarding corporate cybersecurity. In this paper we argue that passage of such laws increases the stock market's focus on cybersecurity for companies headquartered in the affected states. Depending on the nature of the laws, companies may face both direct and indirect costs. Laws focused at the business level can result in direct costs related to compliance with specific regulatory requirements. Laws focused at the government level can result in indirect costs as the laws signal increased attention to cybersecurity, which may result in increased future costs to companies.

Both direct and indirect costs associated with compliance with new laws are likely to be higher for firms that have lower levels of cybersecurity awareness since they will need to invest

[1] https://www.wsj.com/articles/companies-battle-another-pandemic-skyrocketing-hacking-attempts-11598068863
[2] https://cyberscoop.com/biden-national-cybersecurity-strategy-2023/?__hstc=109552666.f5bc7f1b25aaeb4e40fd1a1573c42085.1693204205841.1693204205841.1693204205841.1&__hssc=109552666.1.1693204205841&__hsfp=2067462567

additional resources to meet requirements related to the laws. Following Berkman et al. (2018) and Barry et al. (2022), we measure firm-level cybersecurity awareness through textual analysis of 10-K cybersecurity-related disclosures and find that the market response to passage of the laws is positively related to the firms cybersecurity awareness.

We augment our study of firm-level cybersecurity awareness and cybersecurity legislation by exploring how state-level institutional factors impact the market's perception of the legislation. Berkman et al. (2018) provide evidence that the disclosures reflect an intangible asset related to cybersecurity awareness and Barry et al. (2022) find that country-level institutional factors impact market valuation of the asset. We explore additional variation in the institutional setting within-country, related to state-level introduction of cybersecurity laws.

Political factors have a strong influence on institutional settings (Besley and Case 2003). For example, the approach to government differs significantly between the Republican and Democratic political parties. In general, the Republican approach to government relies more on business to solve societal problems through market mechanisms and incentives, and seeks to reduce the size of government.[3] Further, implementation of laws differs according to the state-level majority party (e.g., Besley and Case 2003; Fredriksson and Wang 2020). We argue that there will be differences in the nature, expected application and enforcement of the laws based upon which party comprises the political majority at the state level. Because they are more likely to rely on government driven solutions to cybersecurity, we expect and find that our results are stronger in Democrat-controlled states.

[3] https://www.pewresearch.org/politics/2020/09/14/americans-views-of-government-low-trust-but-some-positive-performance-ratings/

2. Literature and hypotheses development

2.1. US Cybersecurity Protections

US companies increasingly face cyber-related threats. In 2021, cybercrime cost US businesses and individuals $6.9 billion.[4] In conjunction with increased cyber-related threats, corporate cybersecurity disclosure has increased over time (Berkman et al. 2018). Disclosure increased dramatically following the SEC's 2011 promulgation of CF Disclosure Guidance: Topic No. 2 Cybersecurity. Drawing attention to the material cyber-related risks that many companies face, the guidance noted that companies should increase cyber-related disclosure since they have a duty to disclose information regarding material risks (SEC 2011). The SEC has issued further guidance reinforcing the necessity for companies to disclose material cyber-related risks and events (SEC 2018). In 2023, the SEC added Regulation S-K Item 106, which requires companies to describe the company's processes for assessing, identifying, and managing material risks from cybersecurity threats as well as the role of the Board of Directors and top management in managing cybersecurity risks. In addition to processes, companies must disclose any material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents.[5]

Regulations in the US have largely been based upon a 'free internet' approach, which prioritizes allowing the flow of information across national borders and cultural barriers (Aftergood 2017; Klimburg 2017). The regulatory approach relies on individual companies to manage their cybersecurity. Federal laws primarily focus on governmental entities and regulated industries such as telecommunications and defense (Fischer 2014) rather than more generally on

[4] See https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[5] See https://www.sec.gov/files/rules/final/2023/33-11216.pdf

corporations.[6] While this approach is changing under the Biden administration, the initial focus is on owners and operators of critical infrastructure such as oil and natural gas pipelines, aviation, rail, and water systems, and increasing liability related to software products and services. Other aspects of the regulatory approach are under development and will require a significant investment of time and resources to come into fruition.[7]

Based upon the historical cybersecurity strategy at the Federal level, states have played an important role in the overall cybersecurity regulatory environment. For example, they have served as innovators in privacy law, informing the development of broader federal privacy protections. The continuing importance of state-level initiatives is clear. For example, while some advocates believe federal privacy legislation should include the right of private persons to sue ("private right of action"), a comprehensive privacy law has thus far failed to secure bipartisan support at the federal level.[8] Due to the lack of regulation at the federal level, over the past couple of years multiple states have enacted new privacy laws.[9]

Cyber-related state-level initiatives have forged baseline privacy norms related to privacy policies, data-breach notification, consumer choice, use restrictions, youth privacy, sexual privacy, and telephone privacy (Citron 2016). Further, state-level legislation and litigation have changed how companies respond to inadequate data security and have required some firms to implement physical and cybersecurity policies to protect electronic information and records. Notification of breaches has allowed both state and federal enforcers to investigate whether inadequate security

[6] Some states have passed cybersecurity regulations focused on corporations, however. For example, in 2017, New York passed New York 23NYCRR § 500, which focuses on financial services firms.
[7] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[8] https://iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation/
[9] https://www.natlawreview.com/article/state-us-state-privacy-laws-comparison

was responsible for corporate data leaks. Cohen and Nussbaum (2018) note that the breadth, scope, and scale of state cyber efforts vary widely.

2.2. Market Reaction to Changes in State-Level Cybersecurity Regulation

Cybersecurity incidents carry significant costs (including remediation, lost revenue, litigation, insurance premiums, reputation, and competitive concerns). Because cybersecurity awareness can help companies avoid such incidents, market valuations are positively associated with corporate disclosure regarding cybersecurity (Berkman et al. 2018).

A recent paper by Barry et al. (2022) finds that a company's institutional setting impacts market valuation of cybersecurity disclosures. Because of the leading role of state-level cybersecurity regulation and enforcement (Citron 2016), state-level laws have a strong influence on the cybersecurity-related institutional environment for companies headquartered in each state.[10] Passage of state-level laws increases the stock market's focus on cybersecurity. This focus may be associated with direct costs to companies as they comply with specific requirements resulting from the laws. Laws that primarily relate to state-level governmental departments may still result in expected costs to individual companies as they can impose indirect costs through signaling increased attention to cybersecurity, which can result in increased future costs. Both the direct and indirect costs associated with compliance to the new laws are likely to be higher for firms that have lower levels of cybersecurity awareness.

The cybersecurity institutional setting at the state level is constantly changing, with new laws introduced that increase governmental and corporate attention to cybersecurity. Barry et al.

[10] Consistent with the literature, we focus on state-level changes in the states where companies are headquartered (e.g., Reid and Toffel 2009).

(2022) find that changes in perceptions of companies' cybersecurity institutional setting impact how market valuations reflect company cybersecurity disclosures, with higher valuations for companies with higher levels of cybersecurity awareness. We expect that institutional setting changes following from passage of state-level laws will also impact how market valuations reflect company cybersecurity disclosures, with companies disclosing higher levels of cybersecurity awareness gleaning more positive market valuations.

H1: Market response to passage of state-level cybersecurity laws is positively associated with the firm's cyber awareness.

2.3. Political Environment and Market Reaction to Changes in State-Level Cybersecurity Regulation

The impact of laws on the institutional environment is closely related to the political context. When the US Presidency changed from Democratic to Republican upon election of Donald Trump, the stock market response was relatively more positive for polluting companies, who would presumably face less severe regulation under a Republican regime (Berkman et al. 2019).

In the area of cybersecurity, the Republican and Democrat parties employ different approaches. In general, Republicans are more pro-industry, prefer smaller governments, and rely on market mechanisms and incentives rather than other forms of regulation.[11] Consistent with this approach Rep. John Katko (R-N.Y.) expressed concerns about cyber regulations imposed by the Transportation Security Administration on pipeline operations subsequent to the Colonial Pipeline

[11] https://thehill.com/policy/3731872-how-the-cyber-agenda-would-shift-if-the-gop-takes-over-congress/

ransomware attack.[12] Katko argued that the proposed regulations were "unnecessarily burdensome" and did not sufficiently consider input from industry.[13]

Further, IAPP (2019) notes several differences in approaches to privacy legislation at the federal level. For example, the issue appears to be more significant to Democrats as Democrat-sponsored bills comprise the bulk of introduced federal privacy legislation. An attempt at passing federal privacy legislation in 2019 stalled because of party differences. There were two major areas of disagreement: 1) whether the bill should preempt state privacy laws; and 2) whether it should create a "private right of action" allowing individuals to sue companies for violations. In general, Democrats argue against preemption and in favor of a private right of action and Republicans argue the reverse.

Based upon differences in state-level political environments, there is likely to be variation across states in the costs of compliance to cybersecurity laws. Republican states are more pro-industry and would be less likely to pass laws that impose significant costs on companies. They also would be more likely to leave the specifics of cybersecurity measures up to individual companies. We also expect that a pro-industry environment will lead to less stringent enforcement in Republican states. As a result, we expect that the benefit related to existing corporate cybersecurity awareness will be larger in Democratic states since it is in these states where there will be the greatest costs associated with compliance with the new laws.

H2: The significance of the association between the market response to passage of state-level cybersecurity laws and the firm's level of cybersecurity awareness will be stronger in Democrat-leaning states.

[12] https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
[13] cited in https://www.washingtonpost.com/politics/2021/11/11/top-republican-is-warning-against-new-cyber-regulations/

3. Empirical design

3.1. Model Specification

We examine our first hypothesis by regressing stock price reactions over short-term windows surrounding the events associated with passage and ratification of cybersecurity laws across states. The model is specified as follows:

$$CRET = \alpha + \beta_1 Cyber + \beta_2 SIZE + \beta_3 BTM + \beta_4 ROA + \beta_5 BETA + \beta_6 10KWORDS + \varepsilon \quad (1)$$

where *CRET* is the market adjusted daily cumulative abnormal returns measured over three time windows ([-1,+1]; [-2,+2]; and [-3,+3]) relative to events of interest related to passage of the laws, where [-t,+t] refers to t days before and after the event date (day 0). We examine three event dates for each state-level cybersecurity law, including introduction of the proposed law in the state legislature (initiation), passage of the law by the state legislature (approval) and signing of the law by the governor (ratification). For each event date, we calculate *CRET* for firms with headquarters located in states where the proposed bills become laws. Independent variables are measured as of the most recent annual report filed by the firm prior to the event date. The raw cybersecurity disclosure (*CYBER*) is based upon textual analysis of 10-K disclosures, following a dictionary and process developed by Berkman et al. (2018). The dictionary, which combines common cybersecurity terminology from the National Initiative for Cybersecurity Careers and Studies (NICCS) and cyber-related legislative acts, allows us to identify relevant excerpts within 10-K disclosures. Berkman et al. (2018) use machine-based techniques to process each excerpt and develop a score (*CYBER*) based upon the length and relevance of the disclosures in the year prior to the event.[14] *CYBER* is higher when the language used is more directly relevant to cybersecurity.

[14] See Appendix A in Berkman et al. (2018, 522-524) for a more in-depth description of the method for deriving *CYBER*.

To facilitate interpretation of coefficients, we divide the raw value of *CYBER* by 100. The model also includes a set of control variables which might correlate with both *CRET* and *CYBER*. The control variables include: 1) *SIZE*, the natural logarithm of market capitalization in the year prior to the event; 2) *BTM*, computed as the book value of equity divided by the market value of equity in the year prior to the event; 3) *ROA*, equal to income before extraordinary items deflated by total assets in the year prior to the event; 4) *BETA*, the coefficient on market returns in a market model over the window of [-120,-10] with day 0 as an event date; and 5) *10KWORDS* is the number of words in 10Ks in the year prior to the event, divided by 100. We also include both year fixed effects when the sample spans multiple years and industry fixed effects to remove the effects of year/industry level constant factors. Standard errors are clustered by state to mitigate the potential bias in standard errors caused by state-level factors. A positive β_1 provides evidence supporting our first hypothesis, that cybersecurity awareness is positively associated with returns surrounding the events leading the passage of cybersecurity laws.

For tests of our second hypothesis, we partition the sample based on state-level majority party to investigate whether the institutional setting for the laws, measured by the state-level political majority, moderates the association between the awareness of cybersecurity and stock price valuation surrounding our legislative events. To conduct this partition test, we first identity which party gained the majority votes in the state during each presidential election starting in 2000. We categorize each state as "blue" ("red") if in more than half of the presidential elections between election years 2000 and 2020 the Democratic (Republican) candidates receive the majority of votes cast in the state. H2 predicts that the coefficient of β_1 will differ when we estimate equation (1) for the blue and red samples, with a stronger relation between cybersecurity awareness and stock market reaction for companies in blue states.

3.2. Sample

The COVID-19 pandemic resulted in significant changes to the way that government and businesses operated, opening up opportunities for cyber criminals. The FBI reported an increase in complaints of suspected internet crime from 300,000 in 2019 to almost 800,000 in 2020.[15] Legislative efforts to address the increase in cybercrime largely occurred at the state level. Based upon the increased salience of cybersecurity during the COVID period and the number of legislative efforts to address the risk, we focus our sample on bills that were enacted in 2021. Employing data on state-level cybersecurity legislation from the National Conference of State Legislatures (NCSL), we identify 66 bills that were enacted in 2021 across 30 states.[16] We examine three event dates associated with each bill: 1) the date the bill was introduced to the legislature (initiation); 2) the date the bill was passed by the legislature (approval); and 3) the date that the bill was signed by the governor and became law (ratification).

Our company-level data are drawn from the North America Compustat database available in WRDS and comprises companies headquartered and listed in the three main US exchanges (NYSE, AMEX and NASDQ) as of 28th July 2022. There are 3,562 unique gvkey-permnos in the initial sample. Dropping 1,221 firms headquartered in states without cyber risk-related bills in 2021 leaves a sample containing 2,341 unique firms, which corresponds to 7,934 firm-bill observations. We further delete observations with missing information for the variables in equation (1). The final sample consists of 1,456 unique firms and 4,723 firm-bill observations. The sample process in detailed in Panel A, Table 1.

[15] https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics
[16] https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx

Panel B tabulates the sample distribution across the 30 states. There are 18 (12) red (blue) states. Although most of the states only have one cyber risk bills passed, we observe considerable variation in the number of cyber risk bills in different states, with Texas having the maximum of 9 bills. Due to the number of bills and large number of companies headquartered in the state, Texas contributes a large number of observations to our sample.

[Insert Table 1 around here]

3.3. Descriptive Statistics

Table 2 provides descriptive statistics for all the variables used in equation (1). The average 3-day abnormal return equals a positive 30 basis points, implying that, on average, the market reacts positively to the events leading to the enactment of the cybersecurity laws. The market reactions computed over the other two slightly longer windows (5- and 7-days) confirm the positive average market reaction. Mean *CYBER* is 0.63, with considerable variation across firms.[17] The average return on assets is negative, which indicates a large proportion of loss-reporting firms. Mean *BETA* is greater than 1, implying that compared to the market overall, sample companies have higher risk.

[Insert Table 2 around here]

4. Multivariate regression results

4.1. The Association Between Cybersecurity Awareness and Firm Valuation Surrounding Legislative Events

[17] Because some of the bills take more than one year to proceed from initiation to ratification, the reported descriptive statistics for the independent variables are based upon the year of initiation.

Table 3 presents estimates of equation (1), summing returns across different windows surrounding the legislative events related to passage of cybersecurity laws, including initiation, approval, and ratification. In all three columns, the coefficient on *CYBER* is statistically significant, at least at the 10% level. In column (1) which examines the window [-1,+1], the coefficient equals 0.003 ($p < .10$), indicating that a standard deviation increase in the cybersecurity awareness score is associated with a 14 basis point higher cumulative abnormal return. This is economically significant as it comprises 47% of the average abnormal return for the same window. As indicated in columns (2) and (3), the economic significance becomes stronger when we examine longer windows. Employing windows [-2,+2] ([-3,+3]) to measure the market reaction increases the economic significance 3 (5) times. Firm size and the number of bills at the state level consistently have a negative association with market reaction.

[Insert Table 3 around here]

While table 3 reports the results of using market reactions aggregated over all of event dates, it is unclear when uncertainty regarding enaction of the laws will be resolved. We therefore extend the analysis and estimate equation (1) for each of the key milestones associated with the legislation timeline. The dependent variables for the models are the short window [-1,+1] cumulative abnormal returns for each date: initiation (*CRET11_INIT*); approval (*CRET11_APPR*); and ratification (*CRET11_RAT*) of each bill. The models employ the same right-hand-side variables as in equation (1).

Table 4 presents results of estimating models for each milestone. Across the models, the only significant coefficient of *CYBER* occurs when *CRET11_RAT* is the dependent variable.[18] This

[18] The table focuses on cumulative abnormal returns over [-1,+1]. Results are consistent for the longer event windows reported in Table 3.

result suggests that uncertainty regarding whether the legislation will actually become law is not resolved until governors officially sign the bill.

[Insert Table 4 around here]

4.2. Politics and the Association Between Market Response and Cybersecurity Awareness

In H2, we argue that the nature of cybersecurity laws and their associated direct and indirect costs may differ based upon each state's political context, resulting in a more significant stock price effect related to cybersecurity awareness in blue (Democrat majority) states. Because Table 4 reports that the stock market reaction is centered around ratification, we replicate the model reported in column (3) of Table 4, partitioning the sample into observations from blue and red states. Table 5 reports the results of estimating equation (1) for each partition. Column (1) reports results for Democratic majority (blue) states and column (2) reports results for Republican majority (red) states. Consistent with H2, the coefficient of *CYBER* is significant only for the blue state partition.

[Insert Table 5 around here]

Although there has been insufficient time since adoption of the laws to fully investigate factors driving the different response across political settings, we provide some descriptive evidence to identify future areas of research to address the question. Table 6 explores differences in the nature of the laws across the red state/blue state partitions. The two types of states have a majority of bills focused on the governmental level, with 70.4% (51.9%+18.5%) in blue states and 69.2% (56.4%+12.8%) in red states. However, there appears to be a larger focus of regulation for business in the blue states, with 33.3% (14.8%+18.5%) of the bills having at least some focus on regulation for businesses. In contrast, only 25.6% (12.8%+12.8%) of the bills in red states have at

least some focus on regulation for businesses. The topics of the bills also appears to differ across political environments, with bills in the blue states being more privacy or elections focused, and with a much higher percentage of bills including language related to required development and implementation of policies and procedures. These differences are consistent with our expectations regarding differential regulatory approaches between Democrats and Republicans. While table 6 indicates differences in characteristics of the laws across political partitions, untabled results of estimating our market models including consideration of these bill characteristics do not indicate that the characteristics are associated with differential market responses to ratification of the bills.

[Insert Table 6 around here]

Our discussion related to development of H2 also suggests a potential difference in enforcement of the laws over time based on the state's political environment. Expectations about differential enforcement of the laws could lead to differences in market perceptions of the expected costs associated with the new laws. Due to the recency of the legislation, we leave investigation of this potential explanation for our results as an opportunity for future research.

4.3. Robustness Test

The sample distribution reported in Table 1, panel B indicates that Texan firms dominate the sample. To mitigate the concern that our results documented are driven by a single state, we drop firms located in Texas from our sample and re-estimate the models in Tables 4 and 5. Table 6 documents the results of this robustness test, which are consistent with the results from the entire sample. In Table 6, panel A the coefficient of *CYBER* is positive and significant, indicating that investors in firms with higher cybersecurity awareness react more positively to legislative events compared with those in firms with lower cybersecurity awareness. Moreover, as we report in Table

6, panel B, omitting observations from Texas does not change our inferences about passage of cybersecurity laws in red states as the coefficient of *CYBER* remains insignificant.[19]

[Insert Table 7 around here]

5. Conclusion

The COVID-19 pandemic, spurred many changes in the way government and businesses operated. The sudden move to remote work increased the salience of cybersecurity risks as cybercriminals found ways to take advantage of weaknesses in company security systems, which were not designed for remote worksites. Cyberattacks were not isolated to the business world; attacks, such as the Solarwinds incident, which breached not only company but also federal and state government systems.[20] Legislative efforts to improve cybersecurity has largely occurred at the state level, with the majority of states enacting bills in 2021 alone.[21]

We find that state-level institutional factors impact the market's valuation of cybersecurity legislation. While Berkman et al. (2018) provide evidence that the disclosures reflect an intangible asset related to cybersecurity awareness, and Barry et al. (2022) find that country-level institutional factors impact market valuation of the asset, we find that there is additional variation related to the institutional setting within a country.

---

[19] Our analysis focuses on the time period of the COVID-19 pandemic because of the dramatic increase in cybercrime and increased legislative activity at the state level in the face of increased societal concerns about cybersecurity. Consistent with the increase in concern about cybersecurity, in un-tabled results, we do not find a significant stock market reaction associated with company cyber awareness for events related to passage of cybersecurity laws in the pre-COVID period.

[20] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 ; https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

[21] https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx

Our paper extends work on the impact of country institutional setting on corporate governance (Griffin et al. 2017) to the state level and recent work focusing on how institutional setting and firm-level cybersecurity disclosure (Barry et al. 2022) relate to market valuations. Our results provide evidence that the political context for US state-level laws impacts the association between stock market valuation and firm-level cybersecurity awareness. We find that the positive association between firm-level cybersecurity disclosures and market response to passage of cybersecurity laws primarily occurs in blue states. These results are important as there is increased attention on cybersecurity issues and on reducing the negative impacts of cybercrime. Our results indicate that the market does not uniformly view the potential effectiveness (and associated costs) of laws that are passed at the state level.

Our multi-disciplinary approach, combining the finance, accounting, and economic literatures allows for greater insights into the growing issue of cybersecurity protection (Falco et al. 2019) at both governmental and firm levels. We provide further evidence that the market's perception of cybersecurity-related legislation: 1) is shaped by corporate-level cybersecurity awareness; and 2) differs according to the firm's institutional setting.

Our study has implications for both business and policy makers. It is clear from our results that the stock market views cybersecurity legislation as having real impacts on businesses, even when the focus of the legislation is at the governmental level. Thus, the market views legislation as imposing both direct and indirect costs on companies, that vary according to state-level political party power. Further, in alignment with prior research, our results provide evidence that the market views corporate cybersecurity awareness as not only mitigating the threat of cybercrime (Berkman et al. 2018), but also as reducing expected costs related to new cyber-related legislation.

References

Aftergood, S. 2017. Cybersecurity: The cold war online. *Nature* 547 (7661):30.

Barry, T., J. Jona, and N. Soderstrom. 2022. The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. *Journal of Accounting and Public Policy* 41 (6):106998.

Berkman, H., J. Jona, G. Lee, and N. S. Soderstrom. 2018. Cybersecurity Awareness and Market Valuations. *Journal of Accounting and Public Policy* 37 (6):508-526.

———. 2019. Digital Insiders and Informed Trading before Earnings Announcements. *Available at SSRN 3180531*.

Besley, T., and A. Case. 2003. Political institutions and policy choices: evidence from the United States. *Journal of Economic Literature* 41 (1):7-73.

Citron, D. K. 2016. The privacy policymaking of state attorneys general. *Notre Dame L. Rev.* 92:747.

Cohen, N., and B. Nussbaum. 2018. Cybersecurity for the States: Lessons from Across America. *Washington, DC: Cybersecurity Initiative, New America. Disponível em: https://www. newamerica. org/cybersecurity-initiative/reports/cybersecurity-states-lessonsacross-america*.

Falco, G., M. Eling, D. Jablanski, M. Weber, V. Miller, L. A. Gordon, S. S. Wang, J. Schmit, R. Thomas, and M. Elvedi. 2019. Cyber risk research impeded by disciplinary barriers. *Science* 366 (6469):1066-1069.

Fischer, E. A. 2014. Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation: Congressional Research Service.

Fredriksson, P. G., and L. Wang. 2020. The politics of environmental enforcement: the case of the Resource and Conservation Recovery Act. *Empirical Economics* 58 (6):2593-2613.

Griffin, D., O. Guedhami, C. C. Kwok, K. Li, and L. Shao. 2017. National culture: The missing country-level determinant of corporate governance. *Journal of International Business Studies* 48 (6):740-762.

IAPP. 2019. IAPP 2022 Tracking the politics of US privacy legislation. https://iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation/.

Klimburg, A. 2017. *The darkening web: The war for cyberspace*: Penguin.

Reid, E. M., and M. W. Toffel. 2009. Responding to public and private politics: Corporate disclosure of climate change strategies. *Strategic Management Journal* 30 (11):1157-1178.

SEC. 2011. CF Disclosure Guidance: Topic No. 2. Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

———. 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

Table 1: Sampling process and sample distribution

Table 1, Panel A details the sampling process of this study and Panel B breaks down the final sample across states. *#FIRM_BILL* is the number of firm-bill observations. *# FIRMS* is the number of unique firms. *BLUE_STATE* equals 1 if since 1990s Democrats won over half of the presidential elections, and otherwise. *N_BILL* is the number of bills related to cyber security law at each state during the sample period.

Panel A: Sampling process

	(1) #FIRM-BILL	(2) # FIRMS
US Firms with headquarter information listed in NYSE, AMEX and NASDAQ issuing common shares as of 28th July 2022		3,562
Less: firms with no cyber risk related bills in 2021		-1,221
Original population	7,934	2,341
Less: missing cyber risk related bill event returns	-690	-67
Less: missing cyber risk awareness measure	-2,416	-787
Less: missing control variables	-105	-31
Final sample	**4,723**	**1,456**

Panel B: Sample distribution across states

STATE	(1) BLUE_STATE	(2) N_BILL	(3) #FIRM_BILL	(4) #FIRMS
Alabama	0	1	9	9
Arkansas	0	1	11	11
Florida	0	3	255	85
Georgia	0	2	120	60
Iowa	0	2	25	13
Indiana	0	1	35	35
Kansas	0	1	12	12
Louisiana	0	4	52	13
Missouri	0	1	31	31
Mississippi	0	1	6	6
Montana	0	3	9	3
North Carolina	0	1	50	50
North Dakota	0	3	9	3
Oklahoma	0	1	16	16
Tennessee	0	3	96	32
Texas	0	9	2,133	237
Utah	0	1	22	22
West Virginia	0	1	7	7
Total for Red States		**39**	**2,898**	**645**
California	1	2	656	338
Colorado	1	1	57	57
Connecticut	1	2	78	39
Hawaii	1	1	9	9
Illinois	1	2	207	104
Maryland	1	5	180	36
New Hampshire	1	1	4	4
New Jersey	1	1	73	73
Virginia	1	6	386	66
Vermont	1	2	4	2
Washington	1	3	132	44
Wisconsin	1	1	39	39
Total for Blue States		**27**	**1,825**	**811**
Total Overall		**66**	**4,723**	**1,456**

Table 2: Summary statistics

This table presents the summary statistics of main variables used in this study. *CRETij* is the cumulative daily excess return surrounding an event date with day 0 as the occurrence of the event, with *i* (*j*) representing the *i* (*j*) day before (after) the event date. We compute daily excess return minus value weighted market return on the same day. *CRETij_INIT* is *CRETij* at the bill's introduction date. *CRETij_APPR* is *CRETij* at the bill's approval date, and *CRETij_RAT* is *CRETij* at date that the governor signs the bill into law. *CYBER* is the cyber risk awareness score constructed following Berkman et al. (2018), which considers the length and relevance of cybersecurity-relevant disclosures and the specific language used, divided by 100. *ROA* is income before extraordinary items divided by total assets. *BTM* is the book value of equity divided by the market value of equity. *BETA* is the firm's volatility relative to the market, estimated using daily stock and market returns over [-120,-10] window in a market model with day 0 as an event date. *SIZE* is the natural logarithm of market capitalization. *10KWORDS* is the number of words in 10Ks, divided by 100. All variables are defined in the Appendix with the independent variables reported in the table measured the year prior to bill initiation.

	(1)	(2)	(3)	(4)	(5)	(6)
VARIABLES	**N**	**MEAN**	**SD**	**P25**	**P50**	**P75**
Dependent Variables						
CRET11	4,723	0.003	0.080	-0.040	-0.001	0.041
CRET22	4,723	0.012	0.108	-0.047	0.004	0.062
CRET33	4,723	0.020	0.132	-0.050	0.008	0.075
CRET11_INIT	4,723	0.006	0.053	-0.022	0.003	0.030
CRET11_APPR	4,723	-0.002	0.040	-0.022	-0.002	0.018
CRET11_RAT	4,723	-0.003	0.041	-0.026	-0.005	0.016
Independent Variables						
CYBER	4,723	0.630	0.474	0.280	0.510	0.840
ROA	4,723	-0.053	0.210	-0.071	0.009	0.047
BTM	4,723	0.715	0.345	0.460	0.717	0.972
BETA	4,723	1.508	0.812	0.953	1.355	1.902
SIZE	4,723	7.356	1.961	5.933	7.323	8.626
10KWORDS	4,723	534.6	298.9	379.3	516.2	653.2

Table 3: Baseline results for events related to passage of cybersecurity laws

This table presents the OLS estimation of Model (1). *CRETij* is the sum of cumulative daily excess returns surrounding the three events related to passage of cybersecurity laws (initiation, approval, and ratification), with day 0 as the occurrence of the event, with *i* (*j*) representing the *i* (*j*) day before (after) the event date. We compute daily excess return minus value weighted market return on the same day. Columns (1), (2), and (3) report results for event windows of 3, 5, and 7 days respectively. *CYBER* is the cyber risk awareness score constructed following Berkman et al. (2018), which considers the length and relevance of cybersecurity-relevant disclosures and the specific language used, divided by 100. *ROA* is income before extraordinary items divided by total assets. *BTM* is the book value of equity divided by the market value of equity. *BETA* is the firm's volatility relative to the market, estimated using daily stock and market returns over [-120,-10] window in a market model with day 0 as an event date. *SIZE* is the natural logarithm of market capitalization. *10KWORDS* is the number of words in 10Ks, divided by 100. *N_BILL* is the number of bills related to cyber security law at each state during the sample period. All variables are defined in Appendix. In addition, we control both industry and year fixed effects. T-statistics are computed based on the standard errors clustered at the state-level. ***,** and * denote the significance level (two-tail) at the 1%, 5% and 10% respectively.

	(1)	(2)	(3)
VARIABLES	***CRET11***	***CRET22***	***CRET33***
CYBER	0.003*	0.009***	0.014***
	(1.93)	(2.85)	(4.16)
SIZE	-0.002**	-0.005**	-0.005**
	(-2.53)	(-2.17)	(-2.17)
ROA	-0.002	0.019*	0.012
	(-0.20)	(1.74)	(0.74)
BTM	-0.018*	-0.019	-0.018
	(-1.98)	(-1.29)	(-1.12)
BETA	0.003	0.006	0.010
	(1.26)	(1.22)	(1.55)
10KWORDS	-0.000*	-0.000	-0.000
	(-1.96)	(-1.50)	(-0.66)
N_BILL	-0.002**	-0.003***	-0.004***
	(-2.24)	(-2.92)	(-3.37)
Constant	0.037**	0.068*	0.073*
	(2.11)	(2.02)	(2.01)
Year FE	YES	YES	YES
Industry FE	YES	YES	YES
Cluster by State	YES	YES	YES
N	4,723	4,723	4,723
Adj-R^2	0.034	0.037	0.045

Table 4: When did investors factor the impacts into share prices?

This table reports the results of estimating Model (1) at the introduction, approval and sign-off dates of cyber security law separately. $CRET_{11}\_INIT$ is the $CRET_{11}$ at the introduction date of a law (Column 1). $CRET_{11}\_APPR$ is the $CRET_{11}$ at the approval date of a law (Column 2), and $CRET_{11}\_RAT$ is the $CRET_{11}$ at date that the governor signs the bill into law (Column 3). $CRET_{11}$ is as defined in Table 3. *CYBER* is the cyber risk awareness score constructed following Berkman et al. (2018), which considers the length and relevance of cybersecurity-relevant disclosures and the specific language used, divided by 100. *ROA* is income before extraordinary items divided by total assets. *BTM* is the book value of equity divided by the market value of equity. *BETA* is the firm's volatility relative to the market, estimated using daily stock and market returns over [-120,-10] window in a market model with day 0 as an event date. *SIZE* is the natural logarithm of market capitalization. *10KWORDS* is the number of words in 10Ks, divided by 100. *N_BILL* is the number of bills related to cyber security law at each state during the sample period. All variables are defined in Appendix. In addition, we control both industry and year fixed effects. T-statistics are computed based on the standard errors clustered at the state-level. ***,** and * denote the significance level (two-tail) at the 1%, 5% and 10% respectively.

	(1)	(2)	(3)
VARIABLES	***CRET11_INIT***	***CRET11_APPR***	***CRET11_RAT***
CYBER	0.000	0.001	0.004***
	(0.16)	(0.56)	(3.92)
SIZE	-0.001**	0.000	-0.001*
	(-2.36)	(0.71)	(-1.71)
ROA	0.002	0.006	-0.005
	(0.21)	(0.62)	(-0.61)
BTM	-0.011**	0.002	-0.007*
	(-2.59)	(0.56)	(-2.03)
BETA	0.003*	-0.002	0.002**
	(1.96)	(-0.87)	(2.58)
10KWORDS	0.000*	-0.000	-0.000***
	(1.88)	(-1.26)	(-3.92)
N_BILL	-0.000	-0.001**	-0.000
	(-0.70)	(-2.09)	(-0.78)
Constant	0.020**	0.002	0.007
	(2.16)	(0.22)	(1.28)
Year FE	YES	YES	NO
Industry FE	YES	YES	YES
Cluster by State	YES	YES	YES
N	4,723	4,723	4,723
Adj-R^2	0.040	0.025	0.043

Table 5: Blue versus Red States

This table reports the results of estimating Model (1) in Blue and Red States (Columns 1 and 2, respectively). Blue States refer to those states in which since 1990s Democrats won over half of the presidential elections. Red States include the remaining states in our sample. $CRET_{11}\_RAT$ is the $CRET_{11}$ at date that the governor signs the bill into law. $CRET_{11}$ is as defined in Table 3. *CYBER* is the cyber risk awareness score constructed following Berkman et al. (2018), which considers the length and relevance of cybersecurity-relevant disclosures and the specific language used, divided by 100. *ROA* is income before extraordinary items divided by total assets. *BTM* is the book value of equity divided by the market value of equity. *BETA* is the firm's volatility relative to the market, estimated using daily stock and market returns over [-120,-10] window in a market model with day 0 as an event date. *SIZE* is the natural logarithm of market capitalization. *10KWORDS* is the number of words in 10Ks, divided by 100. *N_BILL* is the number of bills related to cyber security law at each state during the sample period. All variables are defined in Appendix. In addition, we control both industry and year fixed effects. T-statistics are computed based on the standard errors clustered at the state-level. ***,** and * denote the significance level (two-tail) at the 1%, 5% and 10% respectively.

	(1)	**(2)**
	Blue States	**Red States**
VARIABLES	***CRET11_RAT***	***CRET11_RAT***
CYBER	0.004**	0.002
	(2.80)	(1.62)
SIZE	-0.001	-0.001**
	(-0.43)	(-2.71)
ROA	-0.001	-0.011
	(-0.08)	(-1.23)
BTM	-0.009	-0.005
	(-1.08)	(-1.05)
BETA	-0.001	0.004***
	(-0.32)	(4.45)
10KWORDS	-0.000*	-0.000**
	(-2.04)	(-2.23)
N_BILL	0.002*	-0.001
	(2.02)	(-1.34)
Constant	0.001	0.010
	(0.11)	(0.90)
Industry FE	YES	YES
Cluster by State	YES	YES
N	1,825	2,898
Adj-R^2	0.048	0.069

Table 6: Red and Blue State Bill Characteristics

This table reports explores differences in the nature of the laws for Blue and Red States (Columns 1 and 2, respectively). Business Focused bills include provisions requiring specific actions by companies. Government-focused bills include provisions aimed at requirements for creation, funding, or specific actions by governmental entities. Privacy focused bills aim to protect information on individuals. Elections focused bills include protections or specific actions related to the electoral process. Policy/Process focused bills include specific requirements for government or business to implement. Bills can be represented in more than one of these categories.

	(1)	(2)
CHARACTERISTIC	**Blue States**	**Red States**
Number of Bills	27	39
Only Business Focused (%)	14.8	12.8
Only Government Focused (%)	51.9	56.4
Both Business and Government Focused (%)	18.5	12.8
Privacy Focused (%)	18.5	10.3
Elections Focused (%)	11.1	2.6
Policy/Process focused (%)	37.0	20.5

Table 7: Robustness test for sensitivity of results sensitive to firms in Texas

This table reports the results of estimating Model (1) as in Tables 4 and 5 considering the effect of firms headquartered in Texas. Panel A reports results for the entire sample, omitting observations with bills from Texas. Panel B reports results for Red states only, omitting observations with bills from Texas. $CRET_{11}\_INIT$ is the $CRET_{11}$ at the introduction date of a law (Panel A, Column 1). $CRET_{11}\_APPR$ is the $CRET_{11}$ at the approval date of a law (Panel A, Column 2), while $CRET_{11}\_RAT$ is the $CRET_{11}$ at date that the governor signs the bill into law (Panel A, Column 3 and Panel B, Column 1). $CRET_{11}$ is as defined in Table 3. *CYBER* is the cyber risk awareness score constructed following Berkman et al. (2018), which considers the length and relevance of cybersecurity-relevant disclosures and the specific language used, divided by 100. *ROA* is income before extraordinary items divided by total assets. *BTM* is the book value of equity divided by the market value of equity. *BETA* is the firm's volatility relative to the market, estimated using daily stock and market returns over [-120,-10] window in a market model with day 0 as an event date. *SIZE* is the natural logarithm of market capitalization. *10KWORDS* is the number of words in 10Ks, divided by 100. *N_BILL* is the number of bills related to cyber security law at each state during the sample period. All variables are defined in Appendix. In addition, we control both industry and year fixed effects. T-statistics are computed based on the standard errors clustered at the state-level. ***,** and * denote the significance level (two-tail) at the 1%, 5% and 10% respectively.

Panel A: Entire Sample after omitting observations with bills from Texas

	(1)	(2)	(3)
VARIABLES	***CRET11_INIT***	***CRET11_APPR***	***CRET11_RAT***
CYBER	-0.001	0.001	0.004**
	(-0.25)	(0.82)	(2.69)
SIZE	-0.000	-0.000	-0.000
	(-0.48)	(-0.13)	(-0.34)
ROA	-0.010	0.019	0.007
	(-1.32)	(1.24)	(0.78)
BTM	-0.010	0.009	-0.004
	(-1.32)	(1.36)	(-0.54)
BETA	0.006***	0.001	0.001
	(2.85)	(0.39)	(0.97)
10KWORDS	0.000	-0.000	-0.000***
	(1.52)	(-0.32)	(-2.78)
N_BILL	0.000	-0.002	0.001
	(0.42)	(-0.85)	(1.42)
Constant	0.007	-0.001	-0.003
	(0.55)	(-0.13)	(-0.39)
Year FE	YES	YES	NO
Industry FE	YES	YES	YES
Cluster by State	YES	YES	YES
N	2,590	2,590	2,590
Adj-R^2	0.038	0.048	0.041

Panel B: Observations in Red states omitting observations from Texas

	(1)
VARIABLES	***CRET11_RAT***
CYBER	-0.000
	(-0.11)
SIZE	-0.000
	(-0.23)
ROA	0.034
	(1.71)
BTM	0.016*
	(1.99)
BETA	0.005**
	(2.16)
10KWORDS	0.000
	(0.79)
N_BILL	-0.003
	(-0.69)
Constant	-0.010
	(-0.58)
Industry FE	YES
Cluster by State	YES
N	765
Adj-R^2	0.175

Appendix: Model variable definitions

Variable	Definition
$CRET_{ij}$	cumulative daily excess return surrounding an event date with day 0 as the occurrence of the event, with i (j) representing the i (j) day before (after) the event date.
$CRET_{ij}\_INIT$	the $CRET_{ij}$ at the introduction date of a law.
$CRET_{ij}\_APPRL$	the $CRET_{ij}$ at the approval date of a law.
$CRET_{ij}\_RAT$	the $CRET_{ij}$ at date that the governor signs the bill into law.
CYBER	the cyber risk awareness score constructed following Berkman et al. (2018), which considers the length and relevance of cybersecurity-relevant disclosures and the specific language used in the year prior to the bill's initiation, divided by 100.
ROA	income before extraordinary income divided by total assets in the year prior to the bill's initiation.
BTM	the book value of equity divided by the market value of equity in the year prior to the bill's initiation.
BETA	the firm's volatility relative to the market, estimated using daily stock and market returns over [-120,-10] window in a market model with day 0 as an event date
SIZE	the natural logarithm of market capitalization the year prior to the bill's initiation.
10KWORDS	the number of words in 10Ks in the year prior to the bill's initiation, divided by 100.
N_BILL	number of bills related to cyber security law at each state during the sample period.