City Hall Has Been Hacked!
The Financial Costs of Lax Cybersecurity*

Filippo Curti† Ivan Ivanov‡ Marco Macchiavelli§
Tom Zimmermann¶

October 13, 2023

Abstract

State and local governments are attractive cybercrime targets because of inadequate cybersecurity and ample access to sensitive information. We show that external data breaches translate to higher financing costs for governments, including negative abnormal bond returns in the secondary market and higher offering yields and bond pricing uncertainty in the primary market. We also find that governments increase total spending around cyberattacks, suggesting higher operating costs as the likely channel behind the spike in financing costs. Exploiting state-level variation in the timing of both breach notification and data security laws, we show that they have not significantly strengthened cybersecurity.

JEL classification: H72, H74, G38.

Keywords: Cyberattacks, financing costs, municipal debt, cybersecurity regulation.

*We thank seminar and conference participants at Brandeis University, Office of Financial Research (Treasury), UT El Paso, Federal Reserve System Cyber Monitoring Committee, 2023 Fixed Income and Financial Institutions Conference, and the Workshop on Cyber Risk to Financial Stability (Columbia/NY Fed) for helpful comments. We thank Ethan Butler, Kate Lassiter, and Thomas Leistikow for excellent research assistance. The views expressed in this paper are those of the authors and do not necessarily represent those of the Federal Reserve Bank of Chicago, the Federal Reserve Bank of Richmond, or the Federal Reserve System.

†Federal Reserve Bank of Richmond, 530 East Trade Street, Charlotte, NC 28202, USA. Email: filippo.curti@rich.frb.org.

‡Federal Reserve Bank of Chicago, 230 S La Salle Street, Chicago, IL 60604, USA. Email: ivan.ivanov@chi.frb.org.

§Isenberg School of Management, University of Massachusetts, Amherst, 121 Presidents Drive, Amherst, MA 01003, USA. Email: mmacchiavelli@isenberg.umass.edu.

¶University of Cologne, 24, Building 101, 50937 Cologne, Germany. Email: tom.zimmermann@uni-koeln.de.

1 Introduction

State and local governments in the United States provide essential services to citizens and are responsible for the majority of infrastructure spending on roads, rail, aviation, and water resources (CBO, 2018). In doing so, they collect and store a wide array of sensitive personal information such as tax, voter, and healthcare records (Kavanagh, Roque and Takai, 2022). Their extensive access to sensitive data combined with a lack of adequate cybersecurity makes governments attractive targets for cyberattacks, particularly, data breaches (Brooks, 2023; SecurityScorecard, 2018; Norris et al., 2018, 2021; FitchRatings, 2022). Naturally, the 2021 State Chief Information Officer survey characterizes cyber risk as a primary area of focus for governments (NASCIO, 2021). Cyberattacks impose substantial remediation and litigation costs on governments, which may adversely affect their municipal bond valuations and external financing costs. Lax cybersecurity may therefore be a significant source of risk for bond holders and the associated costs may divert funding from public infrastructure and services (NFMA, 2020).

In this paper we rely on a comprehensive data set of external data breaches since the early 2000s to provide the first empirical exploration of cybersecurity risk and associated financial costs in the cross section of state and local governments. External data breaches represent the most common source of cyber risk for governments in our sample with states facing the highest probability of external breaches.[1]

We document substantial adverse capital market consequences of data breaches. Bond prices in the secondary market decline between 15 to 22 basis points (bps) within 30 days of a data breach. Similarly, primary market yields are persistently higher by 10 to 13 bps after a data breach, which represents up to a 5% increase relative to the average bond yields in our sample. Uncertainty in bond issue pricing outcomes also increases as affected issuers are more likely to negotiate the pricing of bond offerings instead of raising capital through auctions. We also find that cyberattacks increase operating costs, the likely channel through which data breaches affect financing costs. Finally, we show that state-level data breach notification laws as well as data security laws have failed to curb cyber risk for local governments.

The impact of cybersecurity risk on governments' capital market outcomes is an

[1]Between 2003 and 2019, governments in our sample faced over 2,500 successful external data breaches as compared to about 230 ransomware attacks. While we focus on external data breaches, we report some results for ransomware attacks in Section 5.3.

empirical question. Prior research shows that the municipal bond market may ignore investor-relevant information due to the historic dominance of retail investors and substantial investor segmentation (Cornaggia, Cornaggia and Israelsen, 2017, 2020; Cornaggia, Hund and Nguyen, 2022; Babina et al., 2021; MSRB, 2022). On the other hand, "informed" institutional investors have become increasingly important in the municipal market, leading to more efficient pricing outcomes (Adelino et al., 2021; Ben-Rephael, Choi and Goldstein, 2021; Chernenko and Doan, 2022; Giannetti and Jotikasthira, 2022; Falato et al., 2021; Li, O'Hara and Zhou, 2022). Overall, bond prices may not fully incorporate price-relevant news, rendering our estimates a lower bound on the true pricing impact of breaches.

We calculate abnormal returns using the method of repeat sales regressions (Goetzmann and Spiegel, 1995; Cornaggia, Hund and Nguyen, 2022; Auh et al., 2022). Specifically, we first compute bond returns for affected governments from thirty days before to thirty days after a cyberattack. We then arrive at abnormal returns for each bond by subtracting the contemporaneous return on an index comprised of bonds in the same maturity and rating categories. We show that governments face negative abnormal returns of approximately 18 bps in the sixty-day window around data breaches, which is substantial given the low-interest rate environment during most of our sample period. State and county governments exhibit the most adverse bond market reaction, while city and district governments have a smaller response. We use the same methodology to show that cyberattacks translate to roughly $1.77 billion in mark-to-market losses to investors on the $870 billion in outstanding bonds affected by external data breaches between 2010 and 2019. This estimate is likely a lower bound of the true costs to investors because many bonds affected by cyberattacks may be illiquid and not trade in the sixty-day window required to compute abnormal returns.

We also examine the effect of data breaches on governments' primary market outcomes. This analysis is most applicable to large and frequent issuers such as states and major cities given the typical issuer raises bond financing only infrequently. Issuers that are large and that choose to raise financing after data breaches may also have better cybersecurity, potentially facing less costly data breaches. Despite the potential for a muted primary market response, we find significant adverse effects on the offering yields of affected issuers of between 10 and 13 basis points relative to similar unaffected issuers.

Moreover, these effects are persistent, lasting for over three years following data breaches.

The increase in primary market yields among affected issuers is accompanied by substantially higher issue uncertainty. Governments hit by data breaches are 3 to 6 percentage points more likely to negotiate the pricing of bond offerings, a financing tool governments use in times of high market or issue uncertainty (Sorensen, 1979; Smith, 1987; Garrett and Ivanov, 2023). These estimates imply a 10 to 20% increase in the probability of negotiations relative to the average propensity to negotiate municipal bond offerings during our sample period. Finally, we do not find any consistent evidence that data breaches affect bond offering amounts. Overall, both secondary and primary market effects indicate that cyber risk translates to large incremental financing costs for state and local governments.

Next, we provide evidence on the likely channel through which cybersecurity risk translates to the documented increase in financing costs for state and local governments. Specifically, we show that total government expenditures increase substantially and permanently in the aftermath of data breaches. Within a year of data breaches, total expenditures jump by 2.8% and continue rising to up to roughly 5% three years after the event. This result is consistent with data breaches increasing governments' operating expenses such as remediation costs to restore computer networks or litigation costs associated with fines and damages resulting from the data breach. For example, a global survey of corporations shows that data breaches translate to increases in insurance premiums, external hiring, staff training, legal costs and fines, and improvements in IT systems (Kaspersky, 2018).

In response to the increasing threats posed by cyberattacks, most U.S. states have enacted some form of cybersecurity regulation since the early 2000s that applies to state and local governments. These laws belong to two major groups, data breach notification and data security laws. We estimate the effects of breach notification laws and data security laws on government spending and the probability of future cyberattacks. We use the difference-in-differences imputation method of Borusyak, Jaravel and Spiess (2021) to estimate dynamic treatment effects of these two sets of laws. The procedure compares outcomes of local governments "treated" with laws to the predicted outcomes of governments in "untreated" or "yet to be treated" states. We do so because standard two-way fixed effects estimates may be biased due to a "bad comparison problem" that

arises when treatment is staggered adoption and most states enter treatment by the end of the sample period (Baker, Larcker and Wang, 2022).

We find that both data breach notification laws and data security laws do not attenuate the incidence of future external data breaches. We also document that government expenditures increase temporarily following the enactment of both sets of laws. The increase in expenditures is consistent with governments increasing spending to ensure compliance and improve cybersecurity in response to the new regulation. Thus, despite the potential investment in cybersecurity infrastructure, the insignificant effect of the laws on the incidence of future data breaches suggests that these laws may not provide sufficient incentives for governments to bolster cybersecurity. That said, our empirical tests do not allow us to rule out the possibility that notification and data security laws, while not affecting the future incidence of cyberattacks, may still mitigate their severity, namely the amount and sensitivity of the data obtained in the breach.

We extend the literature that studies emerging risks in the municipal debt market. Painter (2020); Goldsmith-Pinkham et al. (2019) document that municipalities exposed to sea level rise face higher bond spreads. Gao, Lee and Murphy (2020) shows that the rapid decline of local newspapers in recent years has led to significant increases in local governments' financing costs. Ivanov and Zimmermann (2023); Ivanov, Zimmermann and Heinrich (2022) shows how the rapid growth of private borrowing of governments in recent years combined with the poor disclosure environment leads to substantial risks for municipal bondholders. Finally, (Farrell et al., 2023; Bagley et al., 2023) find that financial statement complexity and interaction of monetary and fiscal policy may adversely have affected municipal bond yields in recent years. We complement these studies by showing that cybersecurity risk is economically large in the cross section of governments and has adverse implications for governments' financing costs and public sector debt valuations.

Our paper also contributes to the growing literature on cybersecurity risk in economics and finance. Prior research shows that cyberattacks may have negative consequences for financial stability (Kashyap and Wetherilt, 2019; Duffie and Younger, 2019; Aldasoro et al., 2020; Eisenbach, Kovner and Lee, 2021; Kotidis and Schreft, 2022) or propagate through production networks (Crosignani, Macchiavelli and Silva, 2023). Moreover, firms' exposure to cyber risk has implications for asset prices, firms' decisions, and reputation (Jamilov, Rey and Tahoun, 2021; Florackis et al., 2023; Kamiya et al., 2021; Ahnert

et al., 2022; Scherbina and Schlusche, 2023; Akey, Lewellen and Liskovich, 2021; Amir, Levi and Livne, 2018). We extend this literature by documenting that cyber risk may also be costly to taxpayers and investors in public sector debt. Moreover, we show that the most prevalent types of cybersecurity regulations at the state-level—data breach notification laws and data security laws—do not appear to reduce cybersecurity risks, suggesting these costs are likely to increase in the near future.

2 Institutional Background

The FBI estimates cybercrime to cost businesses, households, and governments billions of dollars each year (FBI, 2021). Cybercriminals rely on information system vulnerabilities to obtain personal identifiable information (PII) and illicitly gain money from activities such as credit card fraud, tax refund fraud, opening fraudulent bank accounts, or illicitly gaining access to existing bank accounts. Cybercriminals tend to specialize in different parts of this process. Some develop malware to breach computer networks, others implement the data breach, and still others purchase the compromised data to steal and launder money (DiMaggio, 2022).

In addition to selling PII obtained from data breaches, cybercriminals have other ways to monetize the cyber vulnerabilities of targets. They also engage in ransomware attacks—using malware to encrypt an entity's networks and then requesting a ransom payment to deliver the decryption key or email compromises—impersonating the entity's executives via social engineering to illicitly access bank accounts. As state and local governments collect large amounts of data that may be poorly protected, cybercriminals may be able to increasingly exploit system vulnerabilities to steal and monetize PII.[2]

A recent study by the Government Finance Officers Association (GFOA) (Kavanagh, Roque and Takai, 2022) reports that state and local governments may be particularly vulnerable to cyberattacks because of insufficient investment in cybersecurity infrastructure, cybersecurity training of employees, or in-house experts. The study also reports that state and local governments may be especially attractive targets for cybercriminals because of the large amounts of sensitive personal data they collect. Standard & Poor's

[2] https://www.gao.gov/podcast/federal-government-collects-large-amounts-personal-data.-how-it-protected
https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2022/data-centric-government.html

Ratings reports that the effects of cyberattacks on governments' bottom lines may be substantial and lead to credit quality deterioration.[3]

While governments face substantial cybersecurity risks, we know little about the associated financing costs as disclosure related to these risks is virtually nonexistent. A recent study by the National Federation of Municipal Analysts argues cybersecurity risks could adversely impact both governments' capital raising costs and the secondary market pricing and volatility of municipal bonds (NFMA, 2020). The study also recommends a minimal level of disclosure to mitigate potential adverse financing effects. Our study attempts to fill this void by examining the impact of cyberattacks on governments' primary and secondary financial market outcomes.

Most U.S. states have enacted data breach notification laws that apply to state and local governments in response to the high levels of cybersecurity risk.[4] Data breaches are defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. The definition of personal information varies across states and typically includes name, social security number, driver license number, address, email, phone number, credit or debit card number, and medical information. Requirements to notify the parties affected by the breach also vary by state—some states require that each affected person is notified, while others only require that the state's Attorney General is notified. In many instances, governments may be subject to fines or liable for monetary damages when they fail to notify the affected parties. However, given low sophistication and cyber awareness, governments may not always be aware of data breaches.

In addition to data breach notification laws, many states currently also have data security laws that mandate specific data security standards for covered state and local governments.[5] These data security laws generally create oversight bodies tasked with setting security standards and policies for government entities, as well as conducting audits and employee training. State data security laws have been enacted more recently than data breach notification laws.

[3] `https://www.bondbuyer.com/news/amid-rising-online-security-threats-issuers-protect-credit-quality`

[4] See `https://www.ncsl.org/technology-and-communication/security-breach-notification-laws` for additional detail.

[5] See also `https://www.ncsl.org/technology-and-communication/data-security-laws-state-government` for additional detail.

3 Data

We obtain information on cybersecurity incidents such as external data breaches, denial-of-service, and ransomware attacks from Advisen, a Zywave Company. The vendor compiles these data from public sources such as media, legal, or government records. The data set covers the timing of each cyber incident, including incident and announcement dates, as well as the identity of the parent organization of each entity targeted in the cyber incident. Finally, Advisen links incidents affecting multiple organizations simultaneously through related cases mapping. Albeit less frequently, the database may also include information on direct financial losses or litigation as a result of the cyber attack. While many cyber events may go undetected or unreported, to the best of our knowledge, these data represents the most comprehensive source of cybersecurity incidents.

Most cybersecurity incidents in Advisen are external data breaches—those caused by external cyberattacks. The data also cover internal data breaches—instances in which an employee compromises sensitive information, typically by accident or negligence. We limit the sample to external data breaches because of our focus on cybercrime activity.

We obtain balance sheet information on government cybercrime targets in Advisen from the Census of Governments conducted by the U.S. Census Bureau.[6] The Census surveys the full set of state and local governments in years ending in "2" and "7"; in all other years the survey probability is increasing in entity population. Each surveyed government provides financial statement information for the survey year. We match the governments in Advisen to all entities that appear in all complete Censuses since 2002. We do so by using string matching techniques combined with manual verification of each potential match, described in Appendix B. We keep municipalities with at least 4 consecutive years of data resulting in a total of 28,217 entities with information on total government expenditures, revenues, and outstanding debt out of a total of 87,986 governments.

To shed light on the financial costs of cyberattacks, we use data from the Mergent Municipal Securities Database (Mergent) and the Municipal Rulemaking Standards Board (MSRB). As municipal offerings typically comprise of multiple underlying bonds (bond series), Mergent details the contract terms of all municipal bond series since at least the late 1990s. These include the offering date, bond principal amount, type, maturity,

[6] `https://www.census.gov/programs-surveys/cog/data/tables.All.html`

yield, as well as option provisions (if any). We merge government issuers in Mergent to the cyber events in Advisen using the Census ID of each government and the Mergent-Census bridge of local governments from Ivanov, Zimmermann and Heinrich (2022).[7] This results in a sample of 9,625 unique local governments that have at least one municipal bond offering since 2003.

We use municipal bond trading data from the MSRB. In line with prior research, we drop transactions that occur in the primary market, within sixty days of a bond's offering date, or after a bond's maturity date. We also exclude transactions whenever nontransaction-based compensation arrangements are present, the transaction price is a weighted-average price, bond yields are negative, bonds have variable rate-coupons, the coupon information is missing, or coupon rates in the MSRB data differ from those in Mergent (Green, Li and Schürhoff, 2010; Cornaggia, Hund and Nguyen, 2022). If both customer purchase and sales transactions are available for a given bond-date pair, the daily average price for that pair is the midpoint between the maximum customer sale price and the minimum customer purchase price. If customer purchase and sales prices are both unavailable but dealer trades are available, the daily average price is the simple average across all dealer trades. Finally, if only customer purchase or customer sales prices are available on a given date, but not both, the average daily price is the par-value weighted average dollar price across all customer prices.

Finally, we hand collect information on data breach notification and data security laws for each state. 43 states currently have data breach notification laws requiring public entities to notify residents or the state's Attorney General of data breaches. We obtain an initial list of state data breach notification laws as of 2021 from the national conference of state legislatures (NCSL) website. For each state, we then use LexisNexis to obtain the text of all data breach notifications laws and their amendments, associated enactment and effective dates, the types of covered public entities, whether notification violations are subject to fines, damages, or whether the state's Attorney General has the authority to make such determination. 32 states require public entities to pay penalties or damages or allow the state's Attorney General to impose (additional) penalties for such violations in case of notification violation. The remaining 11 states do not require any penalties in case of data breach notification violations. In the empirical analysis we only

[7] Ivanov, Zimmermann and Heinrich (2022) describe the matching procedure in their Appendix A.

consider laws that allow for penalties since the remaining laws may not generate sufficient incentives to improve cybersecurity. We also examine the first data breach notification law for each state to mitigate the potential for anticipation effects. The first initial law we observe is in 2003 and the last one in 2021. One caveat with this empirical setup is that many states amend cybersecurity laws over time and the first law may not accurately reflect the incentives provided by the current version of the law.

In addition to data breach notification laws, some states have also passed data security laws in more recent years. More directly aimed at preventing data breaches from happening in the first place, data security laws provide guidelines to governments on how to secure the data in their possession against breaches. These laws generally establish a state oversight body tasked with setting security standards, conducting security audits, and training employees. A total of 36 states have passed data security laws applying to municipalities.

3.1 Cyber risk in the cross section of governments

We first explore how the incidence of cyberattacks varies in the cross section of governments. Among state and local governments with available balance sheet information, the probability of an external breach between 2004 and 2018 is about 0.6% per year and only about 4% of entities are ever attacked during the sample period. Out of the 1,075 entities that face an external data breach, 855 are attacked once, 111 twice, 42 three times, and the remaining 67 are attacked four or more times. States are the most likely targets—all but one state are attacked at least once, followed by counties and school districts, roughly 10% and 4% of which are attacked at least once. Finally, cities, special districts, and townships have significantly lower probability of being attacked, hovering at around 2% or less.

Figure 1 shows the annualized probability of an external data breach across government size quintiles and government type categories in Panels A and B, respectively. We compute government size quintiles in Panel A based on the annual distribution of total government revenues within each type of government. The probability of an external data breach is monotonically increasing in government size. On average, only 0.1% of governments in the bottom quintile of the total revenue distribution face a data breach in any given year. In contrast, nearly 2% of the largest governments have at least one

external data breach in any given year.

In Panel B we explore heterogeneity in the incidence of external breaches across government type. We focus on local governments in this comparison because states face an annual probability of external data breach exceeding 40%. The figure shows that city and county governments have external data breaches a lot more frequently than township and district governments. While these results are likely attributable to the size differential from Panel A, general-purpose governments maintain a wider array of sensitive personal information and may also face greater cybersecurity risk than special-purpose entities.

In Table 1 we show that governments facing external data breaches are substantially larger in terms of total revenues and also have higher expenditures relative to revenues. The largest entities tend to be general purpose governments—the higher spending relative to revenues is consistent with the wider array of services they offer, making them more attractive targets for cybercriminals. Furthermore, governments facing data breaches have significantly larger debt-to-revenue ratios, raise more financing in the municipal bond market, and have lower municipal bond yields, consistent with larger entities having greater access to the municipal bond market as documented in prior research (Ivanov, Zimmermann and Heinrich, 2022). These results imply that cyber risk may have significant potential to disrupt the operations of governments that are of core importance for activity in each state and, in turn, may have significant implications for their financial market outcomes.

Figure 2 shows the enactment timing of the data breach notification laws across states. We focus on the first enactment of breach notification laws in each state that imposes penalties on governments in case of violations. In most states, the laws become effective shortly after the enactment date, but it is not uncommon for the legislation to become effective more than 9 months after enactment. While the first enactment dates of breach notification laws range between as early as 2003 and as late as 2018, most states enact their first version of breach notification laws between 2005 and 2008.[8]

[8]Appendix Figures C.1, C.2, and C.3 show the timing of each state's first breach notification law that applies to local governments, that applies to state and local governments but prescribes penalties for violation, and to local governments but prescribes penalties for violation, respectively.

4 Empirical Strategy

4.1 Cyberattacks and bond prices

We first examine the municipal bond pricing implications of cyberattacks by estimating abnormal bond returns around external data breach notifications. We estimate abnormal municipal bond returns to data breaches using an event study within a 60-day window centered at the external breach notification date. As trading in the secondary market for municipal bonds in infrequent, we use the method of repeat sales regressions from Cornaggia, Hund and Nguyen (2022) to construct duration-adjusted returns between two adjacent trades s and k as $r_{b,s,k} = (D_{b,s} \cdot y_{b,s} - D_{b,k} \cdot y_{b,k})$, where $D_{b,t}$ is the duration of bond b at time t and $y_{b,t}$ is the yield to maturity of bond b and time t. Next, we construct bond return indexes R_t^l based on remaining maturity and credit ratings, where the superscript l denotes a combination of remaining maturity and credit rating groups. We include 6 maturity categories (up to 2 years, 2-5, 5-10, 10-15, 15-20, and more than 20 years) and 4 rating categories (AAA-AA, A, BBB or lower, and unrated). The abnormal municipal bond return is then defined as $ar_{b,s,k} = r_{b,s,k} - \sum_{t=k+1}^{s} R_t^l$ for bond b belonging to group l. We then estimate abnormal returns around each cyberattack notification as follows:

$$ar_{b,e} = \alpha + \epsilon_{b,e} \tag{1}$$

where $ar_{b,e}$ is the abnormal return of bond b in basis points (bps) around each data breach notification event date e (trades s and k fall on the opposite side of event e), α is the average abnormal bond return around data breach notifications, and $\epsilon_{b,e}$ is the error term. We double cluster the standard errors at the trade date and issuer CUSIP level.

We expect abnormal bond returns around external data breaches to be negative because litigation and remediation costs associated with cyberattacks are likely to reduce governments' net cash flow by increasing operating costs. Nevertheless, the event study estimates may be attenuated because of the significant presence of non-sophisticated retail investors in the municipal market. These estimates may, therefore, represent a lower bound to the true effect of cyberattacks on bond prices.

We examine heterogeneity in abnormal bond returns across government type, collateral type, as well as debt priority. General purpose governments such as states,

cities, and counties offer a wider array of services, making them more attractive targets for cybercriminals. Consequently, abnormal bond returns around cyberattacks may be more negative for these entities.

Collateral type may also be an important determinant of bond returns around cyberattacks. For example, revenue bonds pledge a specific revenue stream, general obligation (GO) bonds pledge a government's tax revenues for repayment purposes, and double-barreled bonds have both types of collateral. To the extent that government have the ability to raise taxes when facing shocks to operating costs, GO and double-barreled bonds may be better insulated from cyberattacks than revenue bonds. For example, Auh et al. (2022) provide evidence supporting this idea in the case natural disasters. Governments, however, may not be able to easily raise taxes when faced with financial difficulty. Consistent with this idea, Butler and Yi (2022) find evidence that bonds backed by specific revenue streams such as revenue bonds are more insulated from adverse state-level trends such as population aging.

Finally, senior bonds have higher contractual priority than subordinated bonds, which implies the magnitude of negative returns is likely to be decreasing in seniority.

4.2 Primary market outcomes

We study the effect of external data breaches on governments' primary market outcomes using the following dynamic difference-in-differences specification:

$$y_{it} = \alpha_i + \alpha_{mt} + \sum_{j=-2}^{j\geq+3} \beta_j \mathbb{1}\{J_{it} = j\} + \delta \mathbf{X} + \epsilon_{it} \tag{2}$$

where i, t, and j denote governments, years, and years relative to external data breach date. $j < 0$, $j \geq 0$, and $j \geq +3$ represent years prior to the data breach year, years after the event year, and three or more years after the breach year. $\mathbb{1}\{J_{it} = j\}$ are indicator variables for data breaches j years relative to the current year so β_j are estimates of pre-trends and dynamic treatment effects. y_{it} is the outcome of interest for government i in year t. α_i and α_{mt} are government and government type by year fixed effects, and X is a set of control variables including governments' size and, in some specifications, state by year fixed effects and government size by government type fixed effects. We include size controls and type by year fixed effects because the incidence of data breaches

is higher among larger municipalities and varies across government entity types, as shown in Figure 1. We double cluster the standard errors at the state and government type-year level.

Recent applied econometrics literature shows that the coefficients in conventional two-way fixed effects (TWFE) models with staggered treatment may be biased whenever observations treated earlier are used as controls for observations treated later in event time (De Chaisemartin and D'Haultfoeuille, 2022; Baker, Larcker and Wang, 2022). In our setting, the number of municipalities that face an external data breach, or "treated" municipalities is small relative to the set of "non-treated" entities, which mostly comprises of never-treated municipalities. Consequently, potential bias in the TWFE coefficients is less likely to be a problem.

We examine five major municipal bond issuance outcomes that are tightly linked to governments' borrowing costs and access to funding: bond issuance amount, offering yield, as well as the share of issuance that is negotiated, senior, or in the form of GO bonds. *Negotiated* is the share of negotiated offerings—where issuers retain the underwriter earlier in the process than in municipal bond auction so as to buffer market or issue uncertainty (Smith, 1987; Sorensen, 1979; Garrett and Ivanov, 2023). *GO Share* in these specifications is defined as the share of unlimited GO bonds, which are backed by the full taxing authority of a given government. *Senior Share* is defined as the share of bonds that have the highest contractual priority in default. We aggregate all outcomes to the government-year level because issuance is infrequent and few governments issue bonds at higher frequencies. Specifically, for each government-year we calculate the total municipal bond issuance and the share of such issuance that is negotiated, GO, or senior as well as the offering amount-weighted average offering yields.

4.3 Cyberattacks and cybersecurity laws

Finally, we assess the impact of data breach notification laws on the incidence of future cyberattacks and government spending using the following dynamic difference-in-differences specification:

$$y_{it} = \alpha_i + \alpha_{mt} + \sum_{j=-4}^{j=+4} \beta_j \mathbb{1}\{J_{it} = j\} + \epsilon_{it} \tag{3}$$

where i, t, and j denote governments, years, and years relative to the enactment of a data breach notification law. $j < 0$ and $j \geq 0$ represent years prior or after the enactment of breach notification laws. $\mathbb{1}\{J_{it} = j\}$ represent indicator variables for the enactment of breach notification laws j years relative to the current year so β_j are estimates of pre-trends and dynamic treatment effects. y_{it} is the outcome of interest for government i in year t. α_i and α_{mt} are government and government type by year fixed effects. We double cluster the standard errors at the state and government type-year level.

As most states enact data breach notification laws by the end of our sample period and many of these laws include violation penalties (see Figures 2 and C.2), most governments eventually receive "treatment." Conventional two-way fixed effects estimates are likely to be biased as observations treated in the early years of our sample period enter the control group in later years. To alleviate this problem, we use the imputation procedure of Borusyak, Jaravel and Spiess (2021). The estimator tailors the control group so as to avoid such "bad" comparisons. Specifically, the procedure excludes already-treated units from the control group and compares outcomes of local governments "treated" with notification laws to the predicted outcomes of governments in "untreated" or "yet to be treated" states.

Governments may have greater incentives to improve cybersecurity infrastructure if data breach notification laws require or allow for monetary penalties in the event of noncompliance. In our preferred specification we define "treatment" whenever the data breach notification laws have associated penalties, while the control group includes observations in state-years with notification laws that do not allow for monetary penalties and in state-years without notification laws.

In our base specifications, we require that the law applies to local governments and not just to states and state agencies. We also use a less stringent definition of treatment where we consider any laws, whether or not they allow for penalties, including laws that only apply to states and state agencies. We focus on the subset of general-purpose local governments and exclude states, authorities, and special districts from our analysis. General-purpose governments represents a natural empirical setting to test for the effects of cyberattacks on public entities because they provide a wide array of services to citizens and are more attractive cyberattack targets. We exclude state entities because they face high probability of cyberattacks and the state-level cybersecurity regulation may be

endogenously tailored to these entities. We use a similar approach when we analyze the effect of data security laws.

5 Cyberattacks and financing costs

5.1 Secondary market prices

We fist examine whether municipal bond prices in the secondary market are adversely affected by external data breaches (see Equation 1). Panel A of Table 2 shows that duration-adjusted municipal bond returns from thirty days before to thirty days after data breach notifications are negative and approximately 16 bps in magnitude. This implies substantial bond valuation losses as a result of cyberattacks, especially given the low municipal bond yields during most of our sample period. Further adjusting bond returns for credit ratings and maturity leads to very similar negative abnormal returns of roughly 18 bps. The latter estimate is equivalent to a negative 10-day return of roughly 5 bps. Panel B shows that the abnormal return estimates are stable across government type. Abnormal returns are slightly larger in magnitude for county and state governments than for cities and districts, but these differences are not statistically significant.

We next use the abnormal returns to provide a direct estimate of the monetary costs of cyberattacks under the assumption that the abnormal returns lead to permanent bond price adjustment. To do so, we re-estimate the regression specification from column 2 of Panel A, weighting each observation by the outstanding dollar amount of each bond. Weighting by outstanding amount allows us to compute the total dollar losses to all holders of the bonds that traded around the cyberattack. We estimate a negative abnormal bond return of roughly 20 bps, which is larger than the estimate in Panel A of Table 2. This suggests that larger governments that typically have have larger municipal bond issues experience larger adverse effects of cyberattacks. The 20 bps estimate translates to a total \$1.77 billion ($\approx 20\ bps * \$870\ billion$) in mark-to-market losses to investors on the \$870 billion in outstanding bonds affected by external data breaches between 2010 and 2019. This estimate is likely a lower bound of the true costs to investors because many bonds affected by cyberattacks may be illiquid and may not trade in the sixty-day window required to compute abnormal returns.

In Panel C of Table 2 we examine heterogeneity in abnormal bond returns along bond

collateral and seniority categories. Specifically, in columns 1-3 we split the sample into revenue, GO, and double-barreled bonds and show that abnormal returns do not vary significantly across these collateral categories. In other words, external data breaches appear to pose substantial risk to future revenue streams of state and local governments, irrespective of collateral type. Columns 4 and 5 show that senior bonds experience smaller losses than subordinated issues, in line with the idea that higher-priority debt holders are more insulated from risk. Yet, even among senior bonds cyberattacks are associated with negative abnormal returns of 15 bps. Overall, these results highlight the potential for cybersecurity incidents to cause significant bond price declines across a wide range of municipal bonds, ultimately inflicting losses on the investors holding these bonds.

5.2 External breaches and primary market activity

We next examine how external data breaches are related to governments' primary market outcomes such as municipal bond issuance, offering yields, issue uncertainty, as well as collateral and seniority. We corroborate our issuance estimates by examining the time series evolution of outstanding debt around external data breaches.

In Table 3 shows how cyberattacks are related to primary market outcomes in event time. Columns 1 and 2 show that cyberattacks are generally not correlated with the ability of governments to raise financing in the municipal bond market as the estimates in the bond issuance amount specifications are statistically insignificant. Column 2 shows an increase in municipal bond offering amount of roughly 5% in the cyberattack year but this increase is only marginally significant. In other words, there appears to be limited evidence that governments raise additional financing in response to cyberattacks.

While cyberattacks do not appear to impair the ability of governments to tap the municipal bond market, entities hit by a data breach face greater financing costs. Columns 3 and 4 show a significant increase in offering yields for governments facing an external data breach of between 11 and 13bps. The increase in yields is not only statistically significant, but also economically so, representing about 5 percent of the average offering yield during our sample period. These effect are also permanent and persist for over three years after the cyberattack, suggesting that government may do little to alleviate investor concerns about cybersecurity risks in the intermediate and long-run. Overall, investors require additional compensation for bearing cyber risk.

It is important to note that the response of offering yields to cyberattacks is slightly smaller than the secondary market effect, likely due to the low frequency of primary market issuance activity for most issuers. Additionally, issuers most affected by cyberattacks may postpone municipal bond offerings if the potential issuance costs are prohibitively expensive. This will result in only the least affected issuers going to market, thereby attenuating the estimated effects of cyberattacks on offering yields and amounts. Such attenuation is less likely to occur in the secondary bond market, where some investor are likely to trade after the realization of negative news and incorporate such information in bond prices.

Columns 5 and 6 of Table 3 indicate that issuers are more likely to choose negotiated instead of competitive offering after a data breach. Issuers opt into negotiated offerings when faced with high issue or market uncertainty. Negotiating pricing allows issuers to better tailor the bond characteristics to investor preferences in light of the higher uncertainty. Consequently, an increase in negotiated offerings after data breaches is suggestive of greater uncertainty in raising capital through the municipal bond market. Albeit the estimates are statistically noisy, there is a marked increase in the likelihood of a negotiated offering of up to 5 percentage points after the data breach with no evidence of pre-trends. Finally, although the dynamic effects three or more years after a cyber attack are insignificant, they remain large and comparable to the earlier event estimates. This suggests the increase in primary market uncertainty may be permanent.

It is possible that issuers may try to buffer primary market uncertainty in other ways such as changing bond collateral type or debt seniority. In Table 4 we show that issuers do not significantly change the type of debt issued following a data breach. Columns 1 and 2 display the effect of data breaches on the share of issuance consisting of general obligation debt, while columns 3 and 4 focus on the share of issuance consisting of senior debt. In both cases, all event study estimates are small and statistically insignificant.

Finally, it is possible that issuers faced with high uncertainty following cyber attacks choose to raise financing through private debt. Ivanov and Zimmermann (2023); Ivanov, Zimmermann and Heinrich (2022) show that governments have substantially increased their reliance on bank loans since Great Recession. To assess this possibility we examine the evolution of total balance sheet debt from the Census around cyberattacks. Total outstanding debt incorporates debt from all sources such as municipal bonds, private

placements, bank loans, or leases. Table 5 shows the effect of external data breaches on the ratio of government debt to revenues using the difference-in-difference specification from Equation (2). Across all specifications, there appears to be no effect of external data breaches on outstanding debt. On average, municipalities do not seem to increase external borrowing in response to an external data breach.

5.3 Ransomware attacks

In addition to data breaches, governments may also become targets to ransomware attacks. Instead of monetizing cyber vulnerabilities by selling PII as in the case of data breaches, ransomware criminals encrypt the IT systems of target entities and demand a ransom payment in exchange for providing a decryption key. Some victims pay the ransom and regain access to their IT systems, while others choose to restore operations using back-ups. Therefore, ransomware attacks may cause significant interruptions to the provision of public services if they affect critical infrastructure or healthcare facilities.

We are unable to fully explore the effect of ransomware attacks on governments' financing costs because of the limited number of such attacks in our sample (only 235 events) . The infrequent nature of debt issuance activity and the low number of ransomware incidents precludes an event study analysis of primary market outcomes around ransomware attacks. Consequently, it is only feasible to evaluate the effect of ransomware attacks on bond prices in the secondary market.

Table 6 presents event study estimates of abnormal bond returns from thirty days before to thirty days after ransomware notifications. Panel A shows that, on average, municipal bonds experience a negative abnormal return of roughly 13 bps following ransomware attacks, with a stronger average effect for county governments. Panel B shows similar effects for general obligation and revenue bonds, and an effect twice as large in magnitude for subordinated than for senior bonds. Overall, the magnitude of abnormal bond returns is slightly larger for data breaches than ransomware attacks. This is consistent with prior research documenting that few ransomware attacks are truly disruptive (Crosignani, Macchiavelli and Silva, 2023). For example, many ransomware attacks may be resolved by either paying ransom or utilizing properly segmented back-ups.

5.4 External breaches and government spending

What is the channel through which data breaches lead to higher financing costs? Data breaches are likely to lead to substantial litigation costs and remediation costs associated with securing the information technology (IT) infrastructure compromised by cyberattacks. Importantly, these costs may be persistent and remain elevated for years. Indeed, in a survey of global enterprises, Kaspersky (2018) finds that expenditures following data breaches include legal costs and remediation costs—hiring external professionals, training existing staff, and improving IT systems, as well insurance costs. Since we are unable to observe expenditures at such granular level, we examine the time series evolution of total expenditures around cyberattacks. Total expenditures should increase with cyberattacks to the extent that cyberattacks lead to increases in legal and remediation costs, and governments do not simultaneously cut other spending. Such spending cuts, however, are only likely to bias against detecting any effects of cyberattacks on total expenditures.

The results in Table 7 show that total expenditures scaled by total revenue increase significantly starting one year after cyberattacks. Furthermore these effects are permanent and persist three and more years following cyberattacks. The expenditure increases are also significant, ranging from 3 to 5% relative to expenditure-revenue ratios three or more years prior to a cyberattack.

The lack of significant pre-trends also suggests that external data breaches are not predominantly targeted to entities with large prior expenditures relative to revenues. It is important to note that we control for combinations of entity type interacted with year, size, and size interacted with entity type as data breaches vary by government type and size (see Figure 1). Overall, the higher expenditures in the aftermath of cyberattacks may put pressure on government budgets and lead to the previously documented increase in financing costs.

6 Cybersecurity regulation and cyber risk

Given the large financing costs of cyberattacks documented so far, regulation may incentivize governments to improve cybersecurity infrastructure and become less susceptible to cyberattacks. We investigate this question in the context of two sets of

state-level regulations, namely data breach notification laws and data security laws.

First, we explore the effect of data breach notification laws, requiring governments affected by a data breach to notify the public of external data breaches in a timely manner. Some laws apply only to states while others to both states and local governments. A moderate increase in litigation risk and monetary penalties arising from data breach notification laws may incentivize municipalities to invest in cybersecurity, thus reducing the future incidence of cyberattacks. At a minimum, notifying citizens of data breach requires at least a basic level of cybersecurity so that governments detect breaches.

Figure 3 shows the dynamic effects of data breach notification laws on expenditures and the probability of future data breaches. Panels A and C use the preferred definition of treatment, limiting the treatment sample to governments in state-years that allow penalties for local governments. Panels B and D use the less stringent definition of treatment, which also includes laws without penalties or laws that only apply to states and state agencies. Panels A and B of Figure 3 show the dynamic effects of data breach notification laws on the ratio of total expenditures to revenues. The parallel trends assumption appears to be satisfied in the data, as there are no significant trends prior to treatment. We estimate a short-lived increase in expenditures in the enactment year, which is consistent with a temporary increase in compliance costs. While the magnitude of the effect in the enactment year is similar in Panels A and B, it is only statistically significant in Panel B. The short-lived increase in expenditures after the enactment of data breach notification laws suggests that municipalities may spend some resources on improving cybersecurity and compliance following the passage of the law. Data breach notifications requirements necessitate a minimum level of cybersecurity awareness or being able to detect an external breach. Such level of cybersecurity awareness may, however, be insufficient to stave off cyberattacks.

Panel C of Figure 3 shows the dynamic effects of notification laws on the probability of future external data breaches, using our preferred definition of treatment. The lack of pre-trends suggests that the introduction of notification laws is not motivated by a recent increase in cyberattacks. Moreover, the lack of any significant reduction in the probability of a cyberattack following the introduction of notification laws suggests that these laws may not reduce the incidence of future cyberattacks. Using the less stringent definition of treatment, Panel D similarly shows no significant decline in the incidence of

data breaches following the enactment of data breach notification laws.

Next, we explore the effect of data security laws, which introduce more explicit requirements for municipalities to strengthen cybersecurity. In the past two decades, many states have implemented data security laws which provide guidelines to state and local government entities on how to secure information systems against data breaches. These laws typically establish a state oversight body tasked with setting security standards and with conducting security audits and employee training.

Figure 4 presents the dynamic effects of data security laws on total expenditures and the probability of external data breaches. The coefficients in Panel A indicate that expenditures are lower in the year prior to enactment and temporarily increase in the two years following enactment. The anticipation effect is consistent with a wait-and-see approach by municipalities which may prefer to reduce spending until the details of the regulation are fully revealed and clarified by regulators. The presence of anticipation effects around regulations is not uncommon in the corporate finance literature (e.g., Ivanov, Pettit and Whited, 2020). The expenditures pattern post-enactment indicates that some spending is undertaken to comply with data security laws. However, as displayed in Panel B, it appears that data security laws do not reduce the incidence of future cyberattacks, despite the potential compliance expenditures. Overall, both data breach notification and data security laws appear to induce some compliance expenditures but no observable decline in the incidence of future cyberattacks. In other words, such laws appear ineffective at reducing cyber vulnerabilities at the municipal level.

7 Policy implications

Investment in cybersecurity infrastructure reduces ex-post remediation and litigation costs to the extent that such investment reduces the probability or the severity of future cyberattacks. Consequently, regulation requiring cybersecurity infrastructure investment may be beneficial if it requires industry-recognized cybersecurity programs that are considered best practice. Such programs may decrease the incidence and severity of data breaches, thus mitigating ex-post litigation and financing costs, as well as the loss of privacy that accompanies data breaches. However, municipalities may not have enough incentives to front-load these cybersecurity investment costs, especially if they do not

perfectly shield them from attacks. Indeed, the worst case scenario for municipalities would be to pay the ex-ante investment costs as well as the ex-post litigation and remediation costs. Incentives should be provided to entice municipalities to invest in cybersecurity ex-ante, instead of only in the aftermath of a successful attack. Recent laws that incorporate incentives to make ex-ante cybersecurity investments have been passed in a few states (McGladrey, 2021). These laws give companies a safe harbor against data breach lawsuits if they comply with industry-recognized cybersecurity programs.

Additionally, the U.S. Securities and Exchange Commission adopted a new rule in 2023, requiring public corporations to timely disclosure material cybersecurity events and provide annual updates on cybersecurity risk management and governance (SEC, 2023). Currently, there is no such guidance or requirement for state and local governments to timely disclose cybersecurity incidents that represent material adverse information for municipal bond holders. Our findings suggest that municipal bond investors quickly incorporate at least some of the news about cyberattacks in bond prices. Requiring more transparency could provide additional pricing-relevant information to investors and possibly incentivize issuers to improve cybersecurity. However, providing granular details on cybersecurity may also be detrimental to governments. In particular, disclosure of specificities of cybersecurity defenses and related insurance coverage may facilitate cybercrime by highlighting vulnerabilities in their cybersecurity posture.

8 Conclusion

State and local governments are attractive targets for cybercriminals because they collect large amounts of sensitive personal information. We show that external data breaches impose significant costs to governments. Following a data breach, governments' bonds experience large negative abnormal returns in the secondary market. In addition, governments face significantly higher financing costs and issue uncertainty in the primary municipal bond market following cyberattacks. Governments also increase spending following cyberattacks, consistent with higher remediation and litigation costs.

We also examine the effectiveness of data breach notification and data security laws and show that they do not reduce the likelihood of future cyberattacks. In other words, these laws may fail to provide meaningful incentives for governments to

improve cybersecurity. While governments' spending increases temporarily in response to these laws, suggestive of higher cyber infrastructure investment, such spending appears insufficient to reduce the incidence of future data breaches.

References

Adelino, Manuel, Chiyoung Cheong, Jaewon Choi, and Ji Yeol Jimmy Oh. 2021. "Mutual fund flows and capital supply in municipal financing." Working Paper, available on SSRN at `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3966774`.

Ahnert, Toni, Michael Brolley, David A Cimon, and Ryan Riordan. 2022. "Cyber Risk and Security Investment." *Available at SSRN 4057505*.

Akey, Pat, Stefan Lewellen, and Inessa Liskovich. 2021. "Hacking corporate reputations." *Rotman School of Management Working Paper No. 3143740*.

Aldasoro, Iñaki, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach. 2020. "The drivers of cyber risk." *BIS Working Paper*.

Amir, Eli, Shai Levi, and Tsafrir Livne. 2018. "Do firms underreport information on cyber-attacks? Evidence from capital markets." *Review of Accounting Studies*, 23(3): 1177–1206.

Auh, Jun Kyung, Jaewon Choi, Tatyana Deryugina, and Tim Park. 2022. "Natural Disasters and Municipal Bonds." *Available at SSRN: https://ssrn.com/abstract=3996208*.

Babina, Tania, Chotibhak Jotikasthira, Christian Lundblad, and Tarun Ramadorai. 2021. "Heterogeneous taxes and limited risk sharing: Evidence from municipal bonds." *Review of Financial Studies*, 34(1): 509–568.

Bagley, John, Stefan Gissler, Kent Hiteshew, and Ivan Ivanov. 2023. "Pushing Bonds Over the Edge: Investor Demand and Municipal Bond Liquidity." *Available at: https://www.brookings.edu/wp-content/uploads/2023/05/muni_liquidity_july_updated.pdf*.

Baker, Andrew C, David F Larcker, and Charles CY Wang. 2022. "How much should we trust staggered difference-in-differences estimates?" *Journal of Financial Economics*, 144(2): 370–395.

Ben-Rephael, Azi, Jaewon Choi, and Itay Goldstein. 2021. "Mutual Fund Flows and Fluctuation in Credit and Business Cycles." *Journal of Financial Economics*, 139(1): 84–108.

Borusyak, Kirill, Xavier Jaravel, and Jann Spiess. 2021. "Revisiting event study designs: Robust and efficient estimation." *arXiv preprint arXiv:2108.12419*.

Brooks, Chuck. 2023. "A Risk Management Cybersecurity Imperative For State, Local Tribal Governments." Available at: Forbes (Data Accessed: February 24, 2023).

Butler, Alexander, and Hanyi Yi. 2022. "Aging and public financing costs: Evidence from U.S. municipal bond markets." *Journal of Public Economics*, 211: 1–18.

CBO. 2018. "Public Spending on Transportation and Water Infrastructure, 1956 to 2017." Available at: `https://www.cbo.gov/publication/54539` (Accessed: February 26, 2023).

Chernenko, Sergey, and Viet-Dung Doan. 2022. "Mutual fund liquidity creation." Working Paper, available on SSRN at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4019567.

Cornaggia, Jess, Kimberly J. Cornaggia, and Ryan D. Israelsen. 2017. "Credit Ratings and the Cost of Municipal Financing." *Review of Financial Studies*, 31(6): 2038–2079.

Cornaggia, Jess, Kimberly J. Cornaggia, and Ryan D. Israelsen. 2020. "Where the Heart Is: Information Production and the Home Bias." *Management Science*, 66(12): 5485–6064.

Cornaggia, Kimberly, John Hund, and Giang Nguyen. 2022. "Investor attention and municipal bond returns." *Journal of Financial Markets*, 100738.

Crosignani, Matteo, Marco Macchiavelli, and André F Silva. 2023. "Pirates without borders: The propagation of cyberattacks through firmsâ supply chains." *Journal of Financial Economics*, 147(2): 432–448.

De Chaisemartin, Clément, and Xavier D'Haultfoeuille. 2022. "Two-way fixed effects and differences-in-differences with heterogeneous treatment effects: a survey." *Econometrics Journal*.

DiMaggio, Jon. 2022. *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime.* No Starch Press.

Duffie, Darrell, and Joshua Younger. 2019. "Cyber runs." *Hutchins Center Working Paper*.

Eisenbach, Thomas M, Anna Kovner, and Michael Junho Lee. 2021. "Cyber risk and the US financial system: A pre-mortem analysis." *Journal of Financial Economics, forthcoming*.

Falato, Antonio, Ali Hortacsu, Dan Li, and Chaehee Shin. 2021. "Fire-Sale Spillovers in Debt Markets." *Journal of Finance*, 76(6): 3055–3102.

Farrell, Michael, Dermot Murphy, Marcus Painter, and Guangli Zhang. 2023. "The Complexity Yield Puzzle: A Textual Analysis of Municipal Bond Disclosures." *Available at: https://www.brookings.edu/wp-content/uploads/2023/05/ComplexityYieldPuzzleBrookings.pdf*.

FBI. 2021. "Internet crime report." *Internet Crime Complaint Center*.

FitchRatings. 2022. "State, Local Govts' Cybersecurity Staffing Challenges Raise Risks." Available at: https://www.fitchratings.com/research/us-public-finance/state-local-govts-cybersecurity-staffing-challenges-raise-risks-12-12-2022 (Accessed: February 26, 2023).

Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michael Weber. 2023. "Cybersecurity risk." *Review of Financial Studies*, 36(1): 351–407.

Gao, Pengjie, Chang Lee, and Dermot Murphy. 2020. "Financing dies in darkness? The impact of newspaper closures on public finance." *Journal of Financial Economics*, 135(2): 445–467.

Garrett, Daniel, and Ivan Ivanov. 2023. "Gas, Guns, and Governments: Financial Costs of Anti-ESG Policies." *Available at SSRN: https://ssrn.com/abstract=4123366*.

Giannetti, Mariassunta, and Chotibhak Jotikasthira. 2022. "Bond Price Fragility and the Structure of the Mutual Fund Industry." *Available at SSRN: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3963161*.

Goetzmann, William N, and Matthew Spiegel. 1995. "Non-Temporal Components of Residential Real Estate Appreciation." *Review of Economics and Statistics*, 77(1): 199–206.

Goldsmith-Pinkham, Paul, Matthew Gustafson, Ryan Lewis, and Michael Schwert. 2019. "Sea level rise and municipal bond yields." *Rodney L. White Center for Financial Research*.

Green, Richard C, Dan Li, and Norman Schürhoff. 2010. "Price discovery in illiquid markets: Do financial asset prices rise faster than they fall?" *Journal of Finance*, 65(5): 1669–1702.

Ivanov, Ivan, and Tom Zimmermann. 2023. "The "Privatization"' of Municipal Debt." FRB of Chicago Working Paper No. 2023-30 available at `https://www.chicagofed.org/publications/working-papers/2023/2023-30`.

Ivanov, Ivan, Luke Pettit, and Toni M Whited. 2020. "Taxes depress corporate borrowing: Evidence from private firms." *Available at SSRN 3694869*.

Ivanov, Ivan, Tom Zimmermann, and Nathan Heinrich. 2022. "Limits of disclosure regulation in the municipal bond market." *Available at SSRN 4022819*.

Jamilov, Rustam, Helene Rey, and Ahmed Tahoun. 2021. "The anatomy of cyber risk." *Working Paper*.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz. 2021. "Risk management, firm reputation, and the impact of successful cyberattacks on target firms." *Journal of Financial Economics*, 139(3): 719–749.

Kashyap, Anil K, and Anne Wetherilt. 2019. "Some principles for regulating cyber risk." *AEA Papers and Proceedings*, 109: 482–87.

Kaspersky. 2018. "On the money: Growing IT security budgets to protect digital transformation initiatives." *Kaspersky Lab*.

Kavanagh, Shayne, Rob Roque, and Teri Takai. 2022. "Cyber risk savvy: How to be a smart customer of cyber insurance." Available at: `https://gfoaorg.cdn.prismic.io/gfoaorg/3d840f3b-4ce1-4a06-aa65-a29b2cec8216_Cyber+Risk+Savvy_R1.pdf` (Accessed: November 16, 2022).

Kotidis, Antonis, and Stacey L Schreft. 2022. "Cyberattacks and Financial Stability: Evidence from a Natural Experiment." *FEDS Working Paper No. 2022-025.*

Li, Yi, Maureen O'Hara, and Xing (Alex) Zhou. 2022. "Mutual Fund Fragility, Dealer Liquidity Provision, and the Pricing of Municipal Bonds." Working Paper.

McGladrey, Kayne. 2021. "Three US state laws are providing safe harbor against breaches." Available at: `https://www.cshub.com/security-strategy/articles/three-us-state-laws-are-providing-safe-harbor-against-breaches` (Accessed: April 10, 2024).

MSRB. 2022. "Trends in Municipal Bond Ownership." *MSRB*, Available at: `https://www.msrb.org/sites/default/files/Trends-in-Municipal-Securities-Ownership.pdf` (Data Accessed: February 27, 2023).

NASCIO. 2021. "The 2021 State CIO Survey." Available at: `https://www.nascio.org/resource-center/resources/the-2021-state-cio-survey/` (Accessed: February 24, 2023).

NFMA. 2020. "Best Practices in Cybersecurity Risk Disclosure for State & Local Governments in Municipal Offerings." Available at: `https://www.nfma.org/assets/documents/position.stmt/wp_cybersecurityfinal_nov2020.pdf` (Accessed: November 16, 2022).

Norris, Donald F, Laura Mateczun, Anupam Joshi, and Tim Finin. 2018. "Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity." *Public Administration Review*, 79(6): 895–904.

Norris, Donald F, Laura Mateczun, Anupam Joshi, and Tim Finin. 2021. "Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity." *Journal of Urban Affairs*, 43(8): 1173–1195.

Painter, Marcus. 2020. "An inconvenient cost: The effects of climate change on municipal bonds." *Journal of Financial Economics*, 135(2): 468–482.

Scherbina, Anna, and Bernd Schlusche. 2023. "The Effect of Malicious Cyber Activity on the US Corporate Sector." *Working Paper, Available at SSRN: 4400066.*

SEC. 2023. "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." Available at: `https://www.sec.gov/files/rules/final/2023/33-11216.pdf` (Accessed: April 10, 2024).

SecurityScorecard. 2018. "Government cybersecurity report." *SecurityScorecard.*

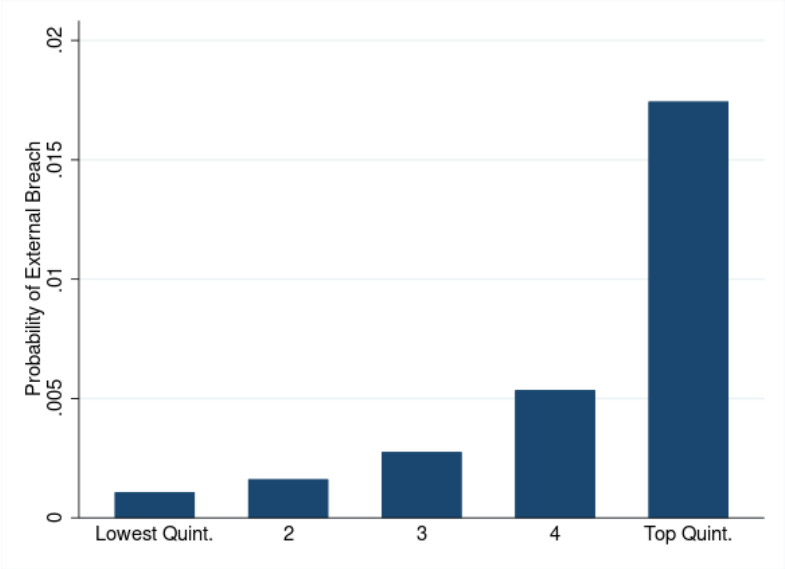
Smith, Richard L. 1987. "The Choice of Issuance Procedure and the Cost of Competitive and Negotiated Underwriting: an Examination of the Impact of Rule 50." *Journal of Finance*, 42(3): 703–720.

Sorensen, Eric H. 1979. "A Note on: Negotiated Municipal Bond Underwritings: Implications for Efficiency." *Journal of Money, Credit and Banking*, 11(3): 366–370.

Figures

Figure 1: External breaches across government size and type. Figure 1 shows the annual probability of an external data breach across government size and type categories. We compute the government size quintiles in Panel A based on the annual distribution of total government revenues within each type of government. The government type categories in Panel B exclude state governments because the annual probability of an attack among states exceeds 40%.

A. Government Size



B. Government Type

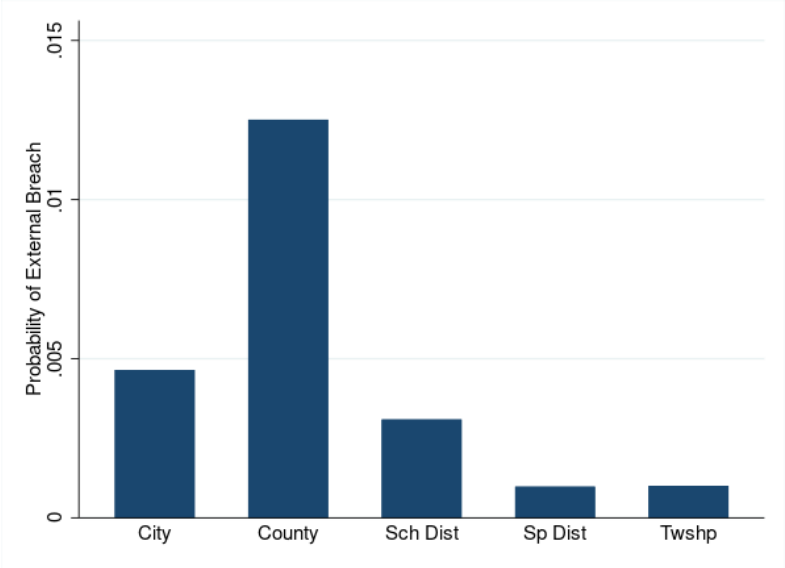


Figure 2: Data breach notification laws. This figure shows the timing of enactment (in grey) and effective dates (in black) for the first data breach notification law in each state that applies to state or local governments. We exclude states that do not have any breach notification laws or those where such laws only apply to corporations—Connecticut, DC, Mississippi, New Mexico, North Carolina, South Dakota, Utah, Wyoming.

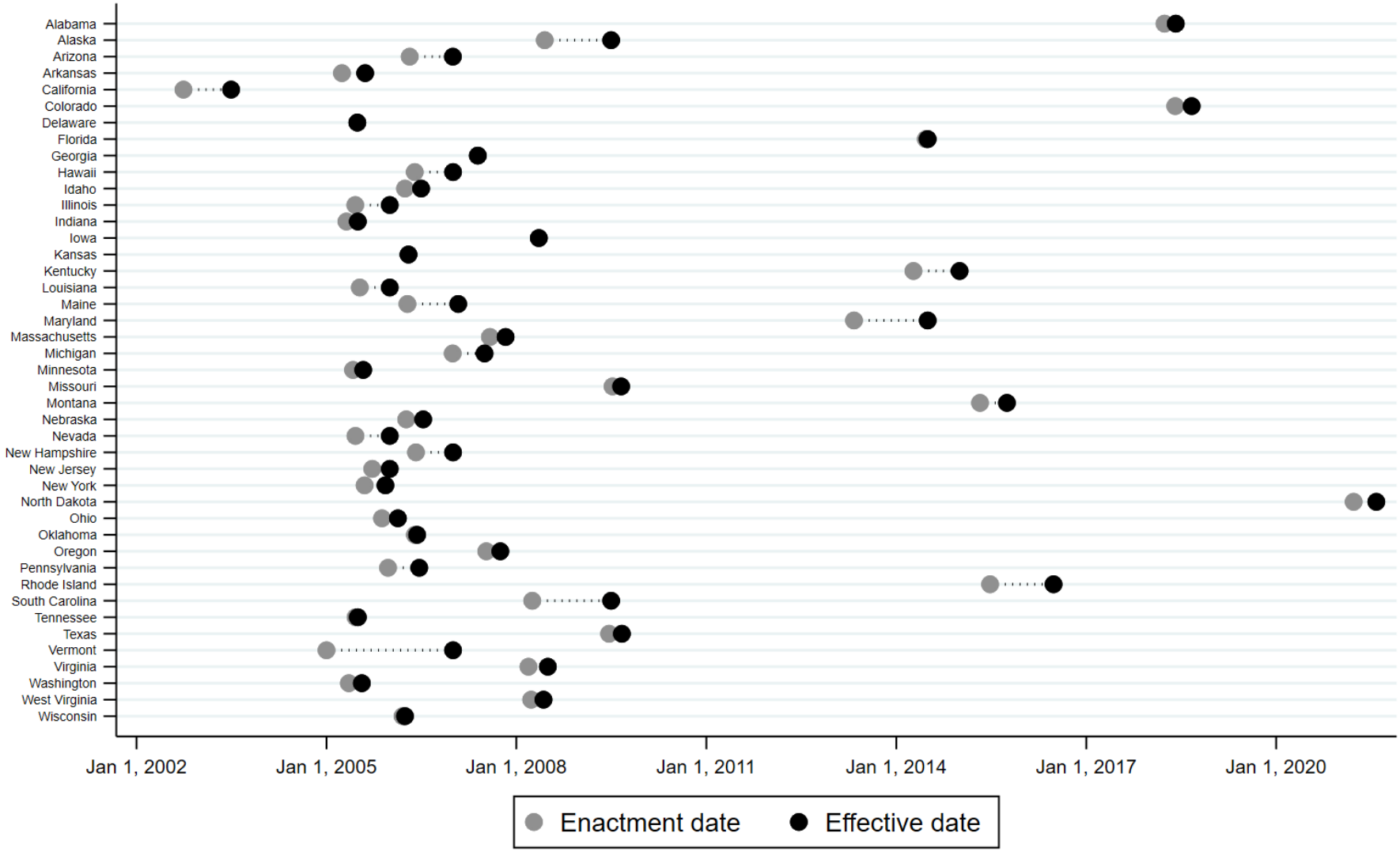


Figure 3: Breach notification laws and cyber risk. We use the estimator of Borusyak, Jaravel and Spiess (2021) to estimate the effect of data breach notification laws on governments total expenditures and the probability of cyber attacks in event time. Panels A and B show event study estimates for governments' total expenditures, while Panels C and D show estimates for the probability of cyberattacks. In Panels A and C we examine the effect of the first data breach notification law in each state that applies to local governments and has associated penalties, damages, or permits the state's attorney general (AG) to impose penalties or damages in case of violation. In Panels B and D we consider the first breach notification law in each state that applies to state agencies or local governments, irrespective of whether it allows for penalties or AG actions. The event time in each figure corresponds to years relative to the enactment year of breach notification laws. All specifications include government and government type×year fixed effects. We cluster the standard errors at the government level.

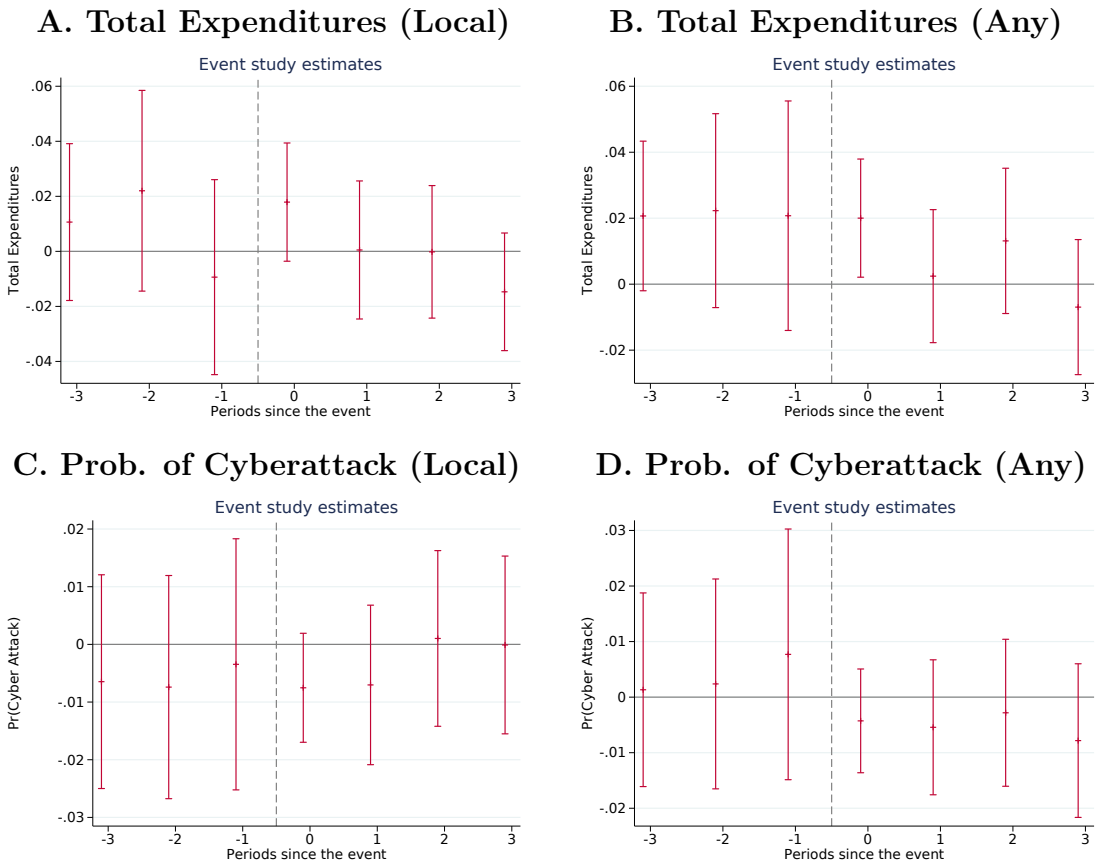
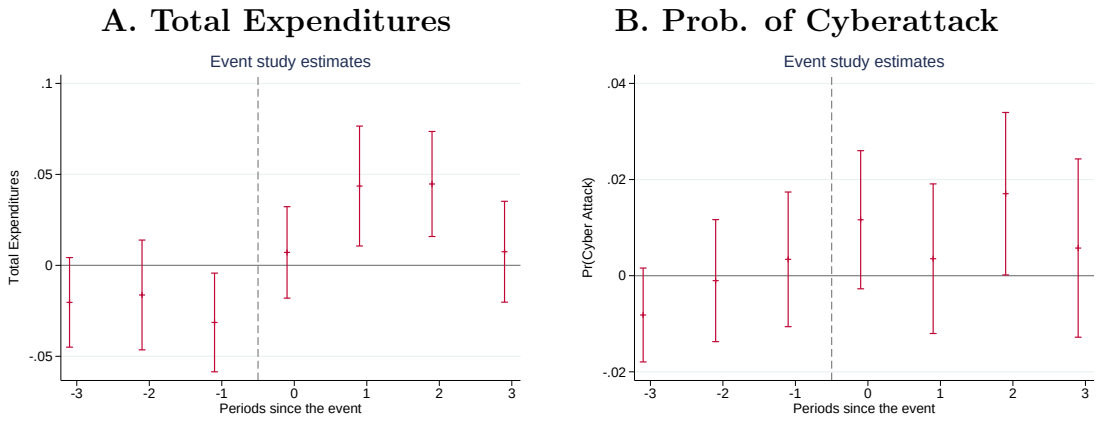


Figure 4: Data security laws and cyber risk. We use the estimator of Borusyak, Jaravel and Spiess (2021) to estimate the effect of data security laws on governments total expenditures and the probability of cyber attacks in event time. Panel A shows event study estimates for governments' total expenditures, while Panel B shows estimates for the probability of cyberattacks. We examine the effect of the first data security law in each state that applies to governments. The event time in each figure corresponds to years relative to the enactment year of data security laws. All specifications include government and government type×year fixed effects. We cluster the standard errors at the government level.



Tables

Table 1: Government characteristics and cyberattacks. Table 1 presents summary statistics for governments' financial characteristics based on whether they experience a cyberattack in the current year.

	Mean	SD	Obs	25^{th}	50^{th}	75^{th}
Balance Sheet Characteristics						
Total Revenues,$m	154	2,688	281,113	5	15	42
Attacked	10,678	29,523	1,683	81	358	4493
Not Attacked	90	1,162	279,430	5	14	41
Expenditures-to-Revenues	1.00	0.22	281,113	0.92	0.97	1.04
Attacked	1.18	0.62	1,683	0.92	0.99	1.13
Not Attacked	1.00	0.22	279,430	0.92	0.97	1.04
Debt-to-Revenues	0.68	1.24	281,113	0.02	0.37	0.86
Attacked	0.72	0.79	1,683	0.20	0.53	1.03
Not Attacked	0.68	1.24	279,430	0.02	0.37	0.86
Bond Market Characteristics						
Bond Issuance,$m	28	146	77,761	2	7	17
Attacked	363	921	640	17	61	236
Not Attacked	25	116	77,121	2	7	17
Yield	2.62	1.36	77,671	1.64	2.61	3.68
Attacked	2.37	1.18	640	1.72	2.30	3.08
Not Attacked	2.63	1.36	77,031	1.64	2.61	3.68
Negotiated	0.35	0.46	77,671	0.00	0.00	1.00
Attacked	0.39	0.44	640	0.00	0.07	1.00
Not Attacked	0.35	0.46	77,031	0.00	0.00	1.00

Table 2: Abnormal bond returns around cyberattack notices. This table presents average abnormal returns (in basis points) for bonds affected by cyberattack notices. We compute abnormal returns from thirty days before to thirty days after cyberattack notices. In Panel A, we adjust returns for bond duration in column 1 and also for the average average returns of sub-indexes based on credit rating and maturity in columns 2 and 3. For the sake of comparison, we convert abnormal returns in column 3 to 10-day returns. In Panels B and C, we adjust all bond returns for bond duration, credit rating, and maturity. Panel B shows sample splits based on government type: city/township, county, district, and state, while Panel C partitions the sample based on bond collateral (GO, revenue, and double-barreled) and seniority (senior and subordinated), respectively. The standard errors are double clustered by trade date and issuer CUSIP.

Panel A: Abnormal bond returns

Duration Adjustment	Yes	Yes	Yes
Risk/Maturity Adjustment	No	Yes	Yes
10-day Return	No	No	Yes
Bond Return	-16.112***	-17.744***	-5.301***
	(2.433)	(1.295)	(1.516)
Observations	36,179	35,679	35,677
Number of Events	2,582	2,573	2,573

Panel B: Abnormal bond returns and government type

Govt Type	City/Twp	County	District	State
Bond Return	-16.976***	-21.722***	-15.215***	-19.235***
	(1.509)	(3.241)	(5.613)	(4.997)
Observations	26,036	5,210	1,439	2,940
Number of Events	1,372	609	213	378

Panel C: Abnormal bond returns and bond heterogeneity

	Collateral			Priority	
	Rev	GO	Double	Senior	Subordinated
Bond Return	-17.808***	-18.233***	-17.518***	-15.154***	-18.891***
	(1.987)	(1.727)	(6.267)	(2.025)	(1.786)
Observations	14,844	18,960	522	10,947	24,732
Number of Events	1,674	810	117	1,533	2,221

Table 3: External data breaches and primary market outcomes. This table presents event study estimates of the evolution of primary bond market outcomes in response to cyberattacks (see Equation 2). The primary market outcomes of interest are aggregated to the government-year level and include the total dollar amount of municipal bonds issuance, the weighted average offering yield to maturity, and the share of the offering amounts that is negotiated. The municipal bond data come from Mergent Municipal Securities Database and the Annual Survey of State and Local Government Finances of the U.S. Census Bureau and runs from 2004 through 2018. We restrict the sample to government-years with at least four consecutive years of data. All specifications include government and government maturity×year fixed effects; in columns 2, 4, and 6 we also add government type×year fixed effects and government types×size interactions. All variables are defined in Appendix A. We double cluster the standard errors at the state and government type×year level. *** p<0.01, ** p<0.05, * p<0.1.

	(1)	(2)	(3)	(4)	(5)	(6)
Outcome variable:	Log(Issuance)		Offering Yield		Negotiated	
Breach Year= −2	0.010	-0.005	0.057	0.064	0.010	0.009
	(0.038)	(0.036)	(0.041)	(0.043)	(0.017)	(0.015)
Breach Year= −1	0.019	0.000	0.034	0.029	0.006	0.002
	(0.032)	(0.034)	(0.036)	(0.039)	(0.025)	(0.026)
Breach Year= 0	-0.030	-0.043	0.107**	0.113***	0.039*	0.028
	(0.044)	(0.045)	(0.040)	(0.039)	(0.023)	(0.025)
Breach Year= +1	0.027	0.047*	0.102**	0.116**	0.034	0.039
	(0.028)	(0.026)	(0.045)	(0.044)	(0.027)	(0.028)
Breach Year= +2	-0.019	-0.028	0.056	0.046	0.056**	0.047*
	(0.034)	(0.037)	(0.047)	(0.051)	(0.026)	(0.025)
Breach Year≥ +3	0.000	0.010	0.129***	0.104**	0.048	0.036
	(0.028)	(0.027)	(0.046)	(0.047)	(0.035)	(0.033)
R^2	0.721	0.719	0.721	0.726	0.487	0.505
N	48,206	42,777	48,206	42,777	33,360	29,887
Government FE	Yes	Yes	Yes	Yes	Yes	Yes
MatMonths×Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Type×Year FE	No	Yes	No	Yes	No	Yes
Type×Size	No	Yes	No	Yes	No	Yes

Table 4: External data breaches and issuance characteristics. This table presents event study estimates of the evolution of primary bond market outcomes in response to cyberattacks (see Equation 2). The primary market outcomes of interest are aggregated to the government-year level and include the share of unlimited general obligation (GO) bonds (columns 1 and 2) or senior bonds (columns 3 and 4). The municipal bond data come from Mergent Municipal Securities Database and the Annual Survey of State and Local Government Finances of the U.S. Census Bureau and runs from 2004 through 2018. We restrict the sample to government-years with at least four consecutive years of data. All specifications include government and government maturity×year fixed effects; in columns 2 and 4 we also add government type×year fixed effects and government type×size interactions. All variables are defined in Appendix A. We double cluster the standard errors at the state and government type×year level. *** p<0.01, ** p<0.05, * p<0.1.

	(1)	(2)	(3)	(4)
Outcome variable:	GO Share		Senior Share	
Breach Year= −2	0.001	-0.004	-0.007	-0.009
	(0.011)	(0.011)	(0.010)	(0.010)
Breach Year= −1	0.001	-0.004	0.003	-0.000
	(0.014)	(0.014)	(0.010)	(0.009)
Breach Year= 0	-0.012	-0.018	0.012	0.012
	(0.011)	(0.011)	(0.011)	(0.009)
Breach Year= +1	0.009	0.001	-0.002	-0.008
	(0.016)	(0.015)	(0.010)	(0.010)
Breach Year= +2	0.004	-0.001	-0.002	-0.001
	(0.013)	(0.012)	(0.011)	(0.009)
Breach Year≥ +3	-0.002	-0.012	-0.015	-0.013
	(0.020)	(0.015)	(0.012)	(0.011)
R^2	0.63	0.645	0.756	0.753
N	48206	42777	48206	42777
Government FE	Yes	Yes	Yes	Yes
MatMonths×Year FE	Yes	Yes	Yes	Yes
Type×Year	No	Yes	No	Yes
Type×Size	No	Yes	No	Yes

Table 5: External data breaches and total debt. This table presents event study estimates of the evolution of total outstanding debt scaled by total revenue in response to cyberattacks (see Equation 2). The governments' balance sheet data come from the the Annual Survey of State and Local Government Finances of the U.S. Census Bureau and runs from 2004 through 2018. We restrict the sample to government-years with at least four consecutive years of data. *Total Debt*, is defined as the total outstanding debt as of year-end divided by the total annual revenues of each government-year. All specifications include government and government type×year fixed effects. The specifications in columns 2, 3, and 4 also include a control for government size—the lagged natural logarithm of government revenues, government type fixed effects interacted with government size, state×year fixed effects. We double cluster the standard errors at the state and government type×year level. *** p<0.01, ** p<0.05, * p<0.1.

	(1)	(2)	(3)	(4)
Outcome variable:	Total Debt			
Breach Year= -2	-0.004	-0.003	-0.003	-0.003
	(0.019)	(0.018)	(0.018)	(0.018)
Breach Year= -1	-0.022	-0.024	-0.024	-0.018
	(0.018)	(0.018)	(0.018)	(0.017)
Breach Year= 0	-0.011	-0.012	-0.012	-0.011
	(0.019)	(0.019)	(0.019)	(0.017)
Breach Year= $+1$	-0.015	-0.017	-0.017	-0.022
	(0.020)	(0.019)	(0.019)	(0.020)
Breach Year= $+2$	-0.031	-0.033	-0.034	-0.040
	(0.022)	(0.022)	(0.022)	(0.025)
Breach Year$\geq +3$	-0.029	-0.033	-0.034	-0.039
	(0.035)	(0.036)	(0.035)	(0.036)
R^2	0.838	0.838	0.838	0.844
N	279,752	279,458	279,458	279,458
Government FE	Yes	Yes	Yes	Yes
Type×Year FE	Yes	Yes	Yes	Yes
Size Control	No	Yes	No	No
Size Control×Type	No	No	Yes	Yes
State×Year	No	No	No	Yes

Table 6: Abnormal bond returns around ransomware attack notices. This table presents average abnormal returns (in basis points) for bonds affected by cyberattack notices. We compute abnormal bond returns from thirty days before to thirty days after cyberattack notices. We adjust returns for bond duration and for the average average returns of municipal bond indexes based on credit rating and maturity. In Panel A, we present abnormal bond returns for the full sample, city and township, and county governments in columns 1-3, respectively. In Panel B we examine heterogeneity in abnormal returns according to whether bonds are general obligation or senior. In columns 1 and 2 we restrict the sample to general obligation (GO) bonds and revenue bonds, respectively. In columns 3 and 4 we restrict the sample to senior and subordinated bonds, respectively. The standard errors are double clustered by trade date and issuer CUSIP.

Panel A: Abnormal Bond Returns and Government Type

Govt Type	All	City/Twp	County
Bond Return	-12.950***	-9.320***	-25.119***
	(3.575)	(3.444)	(7.418)
Observations	2,237	1,587	577
Number of Events	235	132	76

Panel B: Abnormal Bond Returns Heterogeneity

	Collateral		Priority	
	Rev	GO	Senior	Subordinated
Bond Return	-19.011***	-11.502**	-9.718***	-18.556***
	(6.048)	(4.294)	(3.706)	(5.331)
Observations	753	1,386	1,419	818
Number of Events	117	91	182	155

Table 7: External data breaches and government expenditures. This table presents event study estimates of the evolution of governments' total expenditures scaled by total revenues in response to cyberattacks (see Equation 2). The governments' balance sheet data come from the the Annual Survey of State and Local Government Finances of the U.S. Census Bureau and runs from 2004 through 2018. We restrict the sample to government-years with at least four consecutive year of data. *Total Expenditures* is the total expenditures divided by the total revenues of each government-year. All specifications include government and government type-by-year fixed effects. The specifications in column 2, 3, and 4 also include a control for government size—the lagged natural logarithm of government revenues, government type fixed effects interacted with government size, state×year fixed effects, respectively. We double cluster the standard errors at the state and government type×year level. *** p<0.01, ** p<0.05, * p<0.1.

	(1)	(2)	(3)	(4)
Outcome variable:	Total Expenditures			
Breach Year= −2	0.012	0.012	0.012	0.010
	(0.008)	(0.008)	(0.009)	(0.008)
Breach Year= −1	0.009	0.009	0.009	0.009
	(0.012)	(0.012)	(0.012)	(0.012)
Breach Year= 0	0.005	0.005	0.005	0.011
	(0.019)	(0.019)	(0.019)	(0.014)
Breach Year= +1	0.028**	0.027**	0.027*	0.025*
	(0.014)	(0.013)	(0.013)	(0.013)
Breach Year= +2	0.038***	0.038***	0.038**	0.036***
	(0.014)	(0.014)	(0.014)	(0.013)
Breach Year≥ +3	0.050**	0.051**	0.049**	0.047**
	(0.022)	(0.022)	(0.022)	(0.019)
R^2	0.263	0.262	0.263	0.331
N	279,752	279,458	279,458	279,458
Government FE	Yes	Yes	Yes	Yes
Type×Year FE	Yes	Yes	Yes	Yes
Size Control	No	Yes	No	No
Size Control×Type	No	No	Yes	Yes
State×Year	No	No	No	Yes

Online Appendix: Not For Publication

This appendix includes several sections of supplemental information. Appendix A contains definitions for all the variables used in the paper, Appendix B the name matching algorithm, and Appendix C additional figures and tables.

A Variable Definitions

Variable Name	Description
Type	The type of each government entity. Our data cover state, county, city, township, school district, and special district governments. *Source:* Annual Survey of State and Local Government Finances from the U.S. Census Bureau.
Log(Issuance)	The natural logarithm of the total municipal bonds issuance amount raised by a each government in a given year. To the extent that a government has multiple bond offerings in a given year issuances in a given year, this variable is the sum of the issuance amounts across offerings. *Source:* Mergent Municipal Securities Database.
Offering Yield	The average offering yield across different bond series issued by a given government-year, weighted by the dollar amount of each bond series. The offering yield for a given bond series is the original yield at which the series is first made available to investors. *Source:* Mergent Municipal Securities Database.
Negotiated	The share of the total dollar amount of municipal bond issuance of a given government-year that is in the form of negotiated offerings. In a negotiated offering, a government entity retains the underwriter early in the issuance process to help structure the offering before marketing it to potential investors. *Source:* Mergent Municipal Securities Database.
GO	The share of the total dollar amount of municipal bond issuance of a given government-year that is in the form of unlimited general obligation bond offerings. In an unlimited general obligation bond offering, the municipality pledges its tax revenues unconditionally to pay back the obligation. *Source:* Mergent Municipal Securities Database.
Rev	The share of the total dollar amount of municipal bond issuance of a given government-year that is in the form of revenue bond offerings. A revenue bond is backed by a specific stream of revenues of the municipality. *Source:* Mergent Municipal Securities Database.

Continued on next page

Table A.1 – *Continued from previous page*

Variable	**Description**
Double	A double-barreled bond is secured by both a specific source of revenues (as in revenue bonds) and the taxing power of a given government (as in GO bonds). *Source:* Mergent Municipal Securities Database.
Senior	Senior debt has a higher repayment priority than subordinated debt. *Source:* Mergent Municipal Securities Database.
Total Debt	The total outstanding debt divided by the total revenues of a given government as of the end of a given year. *Source:* Annual Survey of State and Local Governments.
Total Expenditures	The total annual general expenditures divided by the total revenues of a given government in a given year. *Source:* Annual Survey of State and Local Government Finances from the U.S. Census Bureau.
Breach Year = X	An indicator variable that takes the value of one whenever a government faces an external data breach X years relative to the observation year, and zero otherwise. Positive values of X indicate that the attack happens X years prior to the observation year, while negative values indicate that the attack happens X years after the observation year. *Source:* Advisen Limited.

B Name Matching Algorithm

Since state and local governments in the Census and Advisen do not share a common identifier, we rely on a name matching algorithm to identify entities across datasets. We match Advisen to the Census of Governments which provides a near-complete universe of state and local governments. Our matching strategy proceeds in a series of steps, outlined below for each of the two datasets.

We match governments in Advisen to all governments that appear in the 2002, 2007, 2012, and 2017 Censuses, primarily through fuzzy matching. We rely on the Levenshtein, Jaro-Winkler, and Cosine Similarity algorithms from the Python Record Linkage Toolkit.[9] Within each state and county cell, we select the highest-score match of a given entity in Advisen to the Census according to each of the three algorithms.[10] Out of the three potential matches, we select the match with the highest score, using a cutoff of 0.85. Whenever scores are tied, Levenshtein takes precedence, followed by Jaro-Winkler, and Cosine. We then manually check the resulting matches. We then manually match incorrect Advisen-Census matches and entities in Advisen that had no Census match above the 0.85 cutoff.

Our algorithm includes additional iterations when it comes to matching special district governments. We first attempt to match special districts to specific entities in the Census, wherever possible. For example, we match the "BI-STATE DEVELOPMENT AGENCY OF THE MISSOURI-ILLINOIS METROPOLITAN DISTRICT (INC)" to Missouri's "BI-STATE DEVELOPMENT AGENCY" from the Census. Whenever such direct matches are not available, we use government websites to determine whether to roll up special districts to the township, city, county, or state level. For example, using such roll-ups we match the "ALABAMA DEPARTMENT OF FINANCE" in Advisen to the state of Alabama in the Census. The government entities that we roll up to general governments are typically departments, offices, and divisions of a larger governing body. Examples of entities that we do not roll up are authorities, councils, agencies, commissions, boards, public universities, hospitals that are part of state universities, and libraries in light of the complexity in determining their governance. We drop prisons, where the level of governmental control is unclear. Finally, we drop hospital auxiliaries and charitable foundations in Advisen that we match to the Census as these are non-profits instead of government entities.

To ensure the accuracy of public school district matches, we first verify that each potential school district in Advisen appears in the Institute of Education Services' National Center for Education Statistics online database, as well as on school webpages. We then match the entities we are able to verify to the Census. Whenever public school districts in Advisen that do not match to a district in the Census (189 cases), we attempt to determine whether they are controlled by general-purpose governments such as states, cities, or counties by reading through government websites. For example, a county government lists its public schools as departments on its website, with the corresponding Advisen entities as "X COUNTY SCHOOLS" or "X COUNTY SCHOOL DISTRICT." In these cases, we match schools/school districts/school boards to general

[9] For additional detail see `https://recordlinkage.readthedocs.io/en/latest/about.html`.

[10] 249 out of the 6,516 entities in Advisen have missing values in the state or county fields. We match those instances to the Census manually, wherever possible, identifying 67 out of the 249 entities. For example, the "FLORIDA DEPARTMENT OF EDUCATION" (missing county information) is matched to "FLORIDA." Similarly, the "STATE OF NORTH CAROLINA" (missing both state and county information) is matched to "NORTH CAROLINA" in the Census.

purpose governments such as city, county, or town governments. These instances also tend to cluster in Maryland, Virginia, and North Carolina. Finally, we exclude charter schools because they are directly affiliated with general government entities.

Similarly, to ensure the accuracy of hospital district/health agency matches, we first manually match hospitals to their controlling body using the public American Hospital Directory database, hospital websites, and news articles.

C Additional Analyses

Figure C.1: Data breach notification laws: local governments. This figure shows the timing of enactment (in grey) and effective dates (in black) for the first data breach notification law in each state that applies to local governments. We exclude from the figure states that do not have any breach notification laws or those where such laws only apply to corporations or state entities.

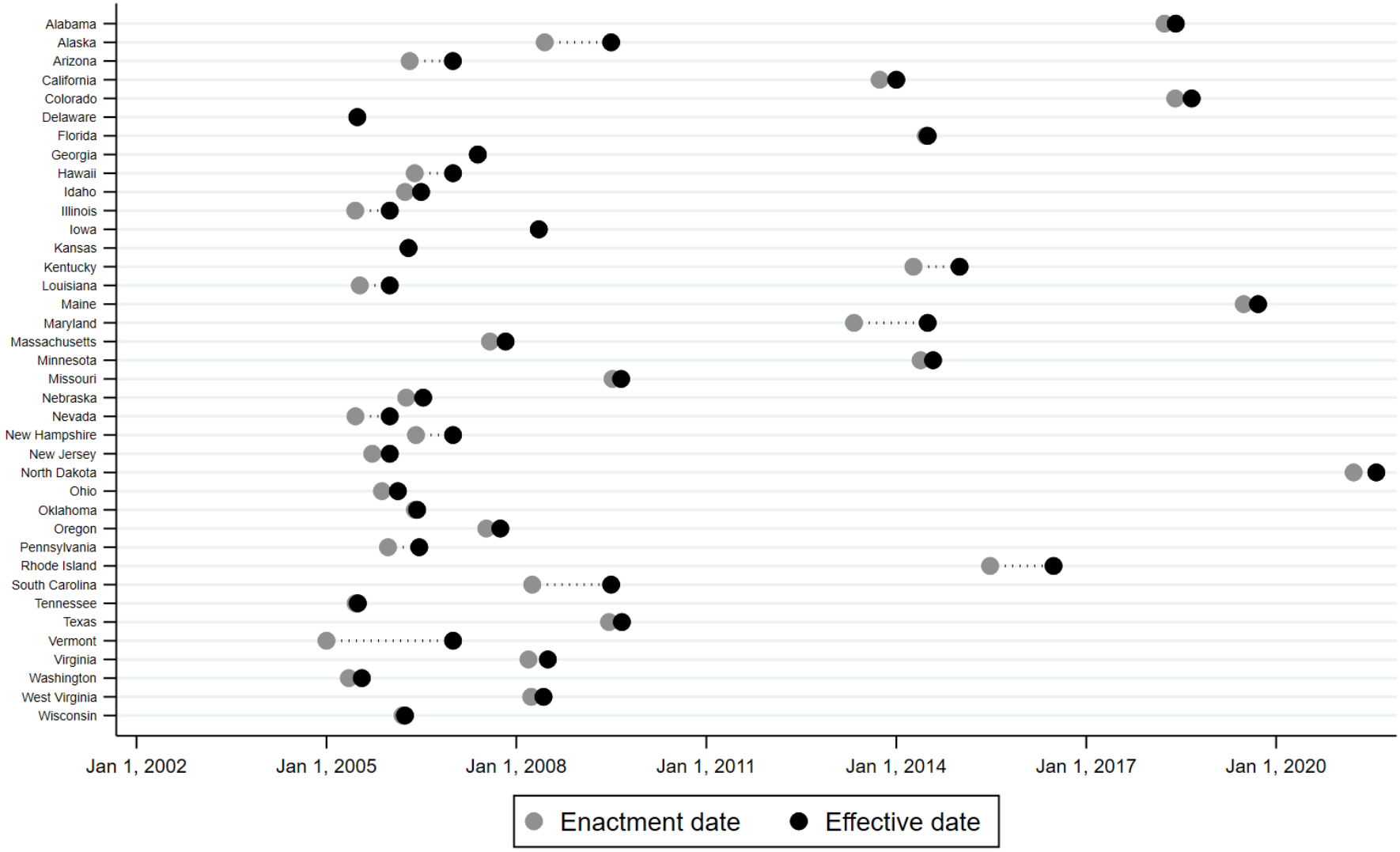


Figure C.2: Data breach notification laws: penalties. This figure shows the timing of enactment (in grey) and effective dates (in black) for the first data breach notification law in each state that applies to state or local governments and has associated penalties, damages, or permits the state's attorney general (AG) to impose penalties or damages in case of violation. We exclude from the figure states that do not have any breach notification laws, where such laws only apply to corporations, or do not impose penalties, damages or permit AG actions.

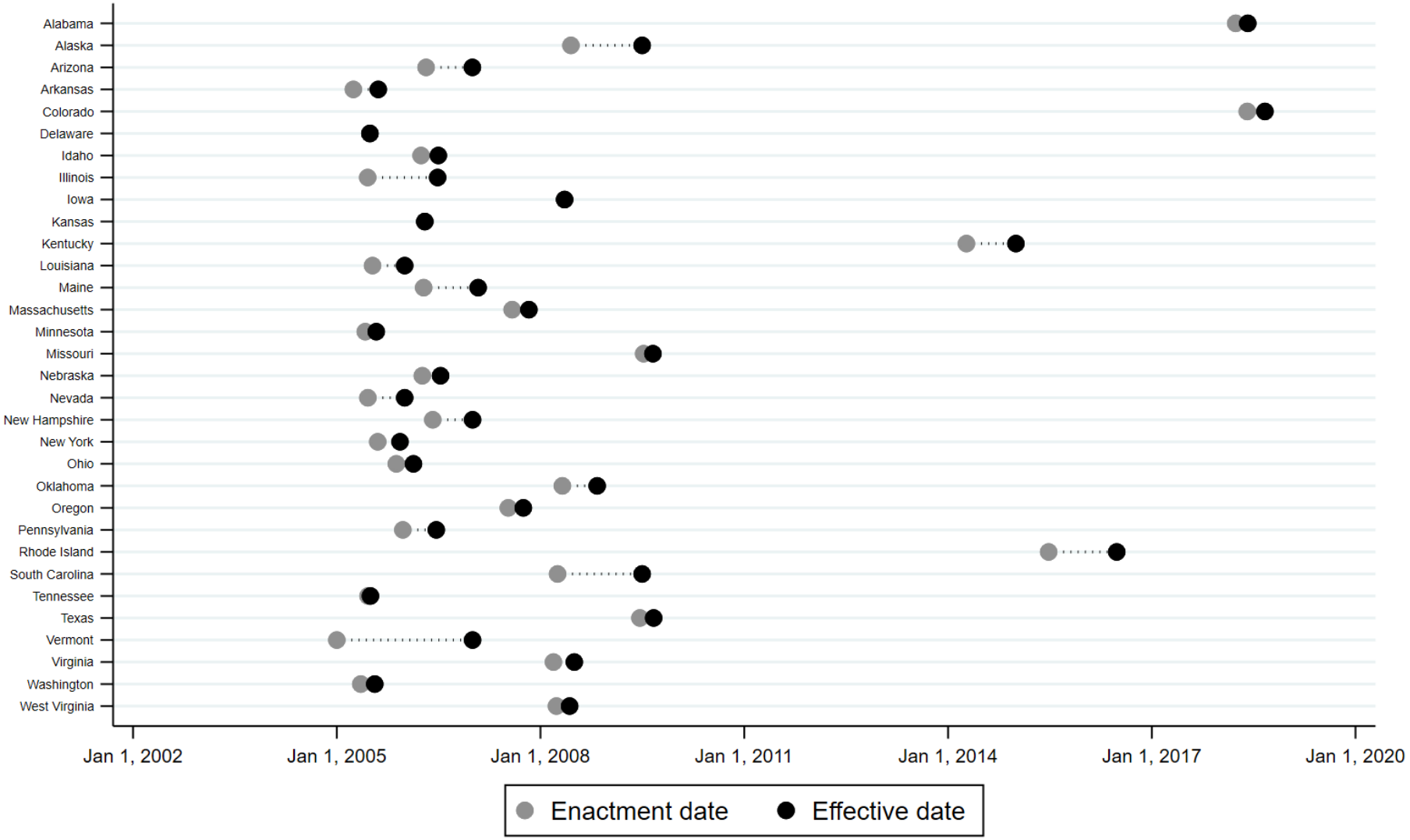


Figure C.3: Data breach notification laws: local governments & penalties. This figure shows the timing of enactment (in grey) and effective dates (in black) for the first data breach notification law in each state that applies to local governments and has associated penalties, damages, or permits the state's attorney general (AG) to impose penalties or damages in case of violation. We exclude from the figure states that do not have any breach notification laws, where such laws only apply to corporations, state entities, or where the laws do not prescribe penalties, damages, or AG actions.

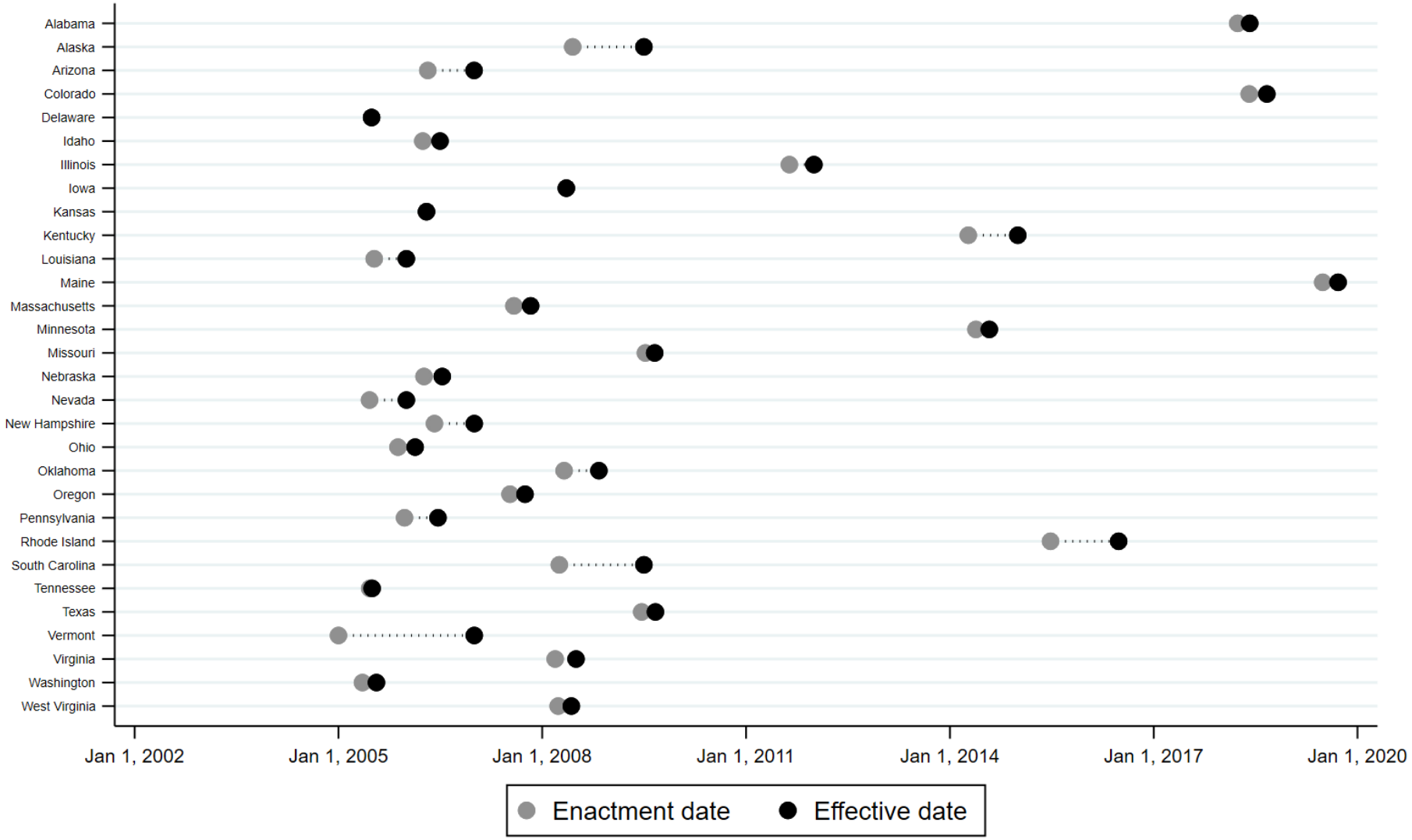


Table C.1: Abnormal bond returns around cyberattack notices: tax-exempt bonds. This table presents average abnormal returns (in basis points) for tax-exempt bonds affected by cyberattack notices. We compute abnormal returns from thirty days before to thirty days after cyberattack notices. In Panel A, we adjust returns for bond duration in column 1 and also for the average average returns of sub-indexes based on credit rating and maturity in columns 2 and 3. For the sake of comparison, we convert abnormal returns in column 3 to 10-day returns. In Panels B and C, we adjust all bond returns for bond duration, credit rating, and maturity. Panel B shows sample splits based on government type: city/township, county, district, and state, while Panel C partitions the sample based on bond collateral (GO, revenue, and double-barreled) and seniority (senior and subordinated), respectively. The standard errors are double clustered by trade date and issuer CUSIP.

Panel A: Abnormal bond returns

Duration Adjustment	Yes	Yes	Yes
Risk/Maturity Adjustment	No	Yes	Yes
10-day Return	No	No	Yes
Bond Return	-16.459***	-18.035***	-5.542***
	(2.495)	(1.381)	(1.584)
Observations	33,021	32,569	32,568
Number of Events	2,430	2,422	2,422

Panel B: Abnormal bond returns and government type

Govt Type	City/Twp	County	District	State
Bond Return	-17.474***	-20.429***	-16.080***	-20.184***
	(1.615)	(3.303)	(5.565)	(5.401)
Observations	23,744	4,759	1,380	2,636
Number of Events	1,296	574	204	347

Panel C: Abnormal bond returns and bond heterogeneity

	Collateral			Priority	
	Rev	GO	Double	Senior	Subordinated
Bond Return	-18.374***	-18.546***	-15.417**	-15.698***	-19.010***
	(2.071)	(1.871)	(5.931)	(2.305)	(1.896)
Observations	13,187	17,631	494	9,582	22,987
Number of Events	1,554	776	111	1,347	2,112