Municipal Cyber Risk

Jonathan Jensen Fiona Paine

June 9, 2023

Abstract

Cyber attacks are estimated to cost billions of dollars per year. However, cyber risk is hard to study since companies rarely disclose hacks and don't share information on cyber security investment. This paper takes a novel approach by looking at municipal hacking. We use a dataset of municipal ransomware attacks merged with hand collected IT investment data and municipal bond data. We find that lower IT investment predicts hacking. Furthermore, following a ransomware attack, municipal bond yields fall by 13 basis points and IT investment as a share of total town expenditure increases by 23 basis points. We investigate potential channels leading to decreased yields post hacking. We find evidence that being hacked reduces cyber risk by disciplining municipalities to move closer to the optimal level of IT spending.

1 Introduction

In a 2022 speech, SEC Chair Gary Gensler estimated that the total economic cost of cyber attacks "is at least in the billions, and possibly in the trillions, of dollars" [1]. Not only are they costly, but cyber attacks are increasingly common[2]. However, cyber risk is hard to study because companies don't share information on cyber security investment and until recently companies rarely disclosed hacks. The result is that very little is known about how cyber risks are captured in financial markets.

The goal of this paper is to investigate movements in bond spreads and municipal investment decisions around ransomware attacks. We study municipalities because data on hacking events, as well as municipal investment decisions are publicly available. Merging municipal data on bond yields, ransomware, and IT investment gives novel insights into how cyber risk impacts local governments and, more generally, firms.

Our key finding is that cyber risk is priced in municipal bond spreads. We find that lack of IT spending is predictive of municipal hacking. Moreover, after a hack, towns react by increasing IT spending. We find that yields do not react in the short term (up to 6 months) to a town disclosing a ransomware event. This is suggestive of investors already having the impact of the type of ransomware attack in our sample priced into bonds. There is also no increase in trading volume around a town ransomware attack suggesting that the bond yields aren't driven by new information, liquidity, or attention effects.

However, in the 24 months following a ransomware attack, towns see a gradual decline in bond yields. This decline in bond yields isn't driven by changes in the town's economic fundamentals. The number of firms, employment, and average annual payroll are unchanged following cyber attacks, ruling out firm behavior changes as a factor driving the effect on municipal yields. We argue that the declining bond yields is driven by decreased cyber risk of the town thanks to increased in IT spending.

[1] https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124

[2] https://www.verizon.com/business/resources/reports/dbir/

We next use the disclosure of a company being hacked in a given county as a shock to municipal cyber security spending. The intuition is that a corporate hack increases the salience of cyber risk for the stakeholder in the town while not impacting any of the town's other fundamentals. We find that IT spending in a county increases following a corporate hack and bond yields decline. This result is consistent with salience being important for cyber security investment.

A critical question is: Why do towns change IT investment after a hack? This has important implications for policies aimed at improving cyber security in both the public and private sectors. We hypothesize that town reactions are driven by a systematic underinvestment in cyber security by municipalities. Following a hacking event, municipalities are disciplined and increase IT spending, reducing the risk of future cyber events.

We show evidence for two mechanisms leading to an ex ante underinvestment in cyber security and IT infrastructure. First, municipal stakeholders may be short-termist. We find that in towns with higher resident turnover (our proxy for short-termism), the reaction in yield spreads to ransomware attacks is larger, meaning that there is more underinvestment. Second, for cyber risk, newspapers serve to increase ex-post disclosure of ransomware attacks instead of acting as monitoring devices as in Gao et al. (2020). We find that towns with more local newspapers react more to ransomware attacks, suggesting that there is a lack of awareness about cyber risk until a town is hacked, but following the hack, stakeholders learn and update preferences.

The paper proceeds as follows: First, we provide an overview of the literature on cyber security risk and municipal finances. Second, we discuss the institutional details of municipal cyber attacks. Next, we describe the data used in our analysis and document the effect of cyber attacks on municipal bond yields and IT investment. We then discuss potential mechanisms driving our result. Finally, we conclude.

2 Literature

Our paper contributes to the burgeoning literature in finance and economics on cyber security risk as well as the literature on the determinants of muni bond yields.

First, Florackis et al. (2023) and Jamilov et al. (2021) use textual analysis of 10K filings and earnings calls respectively to create a measure of cyber security risk. Florackis et al. (2023) find that their measure of cyber security risk is predictive of a firm being hacked and is a priced factor in the cross section of stock returns. By contrast, our paper is able to directly measure IT spending and thus does not need rely on a proxy of cyber risk. Lattanzio and Taillard (2023) use the measure of cyber security risk developed by Florackis et al. (2023) to study the impact of cyber security risk on mergers.

Kamiya et al. (2021) develop a model of optimal firm exposure to cyber risk. The implication is that rational agents with full information should not react to a cyber attack. However, they find a negative stock price reaction which spills over into other firms in the same industry. Their analyses suggest that data breaches are negative signals about the cyber risk of a hacked firm. Our results are a slightly different setting, since we are looking at ransomware attacks of municipalities as opposed to firm data breaches. We find that there is no negative bond price reaction to municipal ransomware attacks. Instead, ransomware attacks have a longterm effect of decreasing a town's risk by increasing IT spending. It's important to note that our measured effect is on the monthly scale, while Kamiya et al. (2021) find a negative reaction in the 3 day window around the event. Moreover, while Kamiya et al. (2021) find a decline in sales growth in the three years post data breach, we do not find any negative effect in tax revenue, business starts, or employment in towns post hacking.

Bana et al. (2022) studies the response of firm hiring to a data breach. They find that firms increase cyber security hiring after a hack. In addition, the magnitude of this effect is relatively small, but larger with more media and attention. We find similar reaction among towns, who tend to increase IT spending after a ransomware attack. A drawback of their approach is that cyber security hiring is an imperfect proxy for cyber risk for two reasons. First, cyber security is often outsourced and, due to labor shortages, companies that can hire in cyber security tend to be bigger and able to pay higher salaries. Thus there is a selection problem in the effect they measure. Secondly, improved cyber security comes largely through hardware improvements, software updates, and training programs for all company employees. These aren't captured in hiring.

In contrast to the common data breach setting, and this paper's ransomware setting, Crosignani et al. (2023) study a cyber attack (NotPetya) that propagated across companies through network ties, becoming one of the most damaging cyber attacks to date. Eight very large public firms were simultaneously directly impacted with another 233 customers and 320 suppliers indirectly affected. A key finding is that customers of suppliers directly hit by the cyber attack were more likely to end their trading relationship with the affected supplier. They are further able to draw a contrast with both natural disasters disruptions and credit supply shocks. In particular, the unpredictable nature, the speed of transmission, and the potential magnitude of reach of cyber attacks.

We contribute to the literature on factors that impact municipal borrowing costs. Schwert (2017) finds that the majority of bond spreads are accounted for by default risk. Gao et al. (2020) show that local newspaper closures (a shock to monitoring costs) increase municipal bond spreads. Jerch et al. (2020) find that natural disasters make municipal debt more risky. Chava et al. (2022) find that winning the bid to offer new corporate subsidies to a potential new firm leads to an increase in bond spreads. Painter (2020) finds that counties more exposed to climate risk pay more underwriting fees and have higher initial yields.

We also contribute to the literature studying the interaction of municipal borrowing costs and public investment. Adelino et al. (2017) find that decreases in municipal credit supply adversely affect the provision of local public goods and services. Similarly, Agrawal and Kim (2022) find that frictions in the bond market lead to higher levels of drinking water pollution. Amornsiripanitch (2022), show similar results. While these papers all show the effect of borrowing costs on investment, we find some evidence that public investment in IT infrastructure impacts borrowing costs.

3 Cyber Security Background

Cyber security is broadly the ability of an organization or individual to keep malicious actors from impacting or infiltrating their network. The actors of concern can be an individual, an organized criminal group, or a nation state. These actors vary in sophistication and motivation. For the purpose of this paper we will ignore nation states who tend to perpetrate targeted highly sophisticated attacks and have motivations that go beyond monetary interests. Instead, hacking is taken to be a random crime of opportunity where the hackers are hoping to make money. According to the 2023 Verizon Data Breach Investigations Report, 95% of hacking incidents are financially motivated[3]. Hacking can be profitable in two main ways. First, in a data breach scenario, a hacker gains access to an organization's network and is able to steal valuable data including: trade secrets, credit card numbers, or PPI (private personal information). This data is then sold on the dark web. The second method of monetizing hacking is using ransomware. In a ransomware attack an organization is locked out of their computer system and network until a ransom is paid (usually in bitcoin). There is often nothing stopping the hackers from also copying any sensitive data and selling it on the dark web in addition. One contrast to the data breach setting is that there can be negotiations between the hackers and the hacked organization over the size of the ransom.

While there have been numerous famous data breaches, for example Equifax in 2017, ransomware has been growing in prevalence. According to reports, over half of all malware attacks are ransomware and local governments are a major target[4]. Thus this paper focuses on ransomware attacks. Our main scenario is: a criminal organization sends phishing emails with malicious code embedded in them to all the towns in the US. An employee in some town

[3] https://www.verizon.com/business/resources/reports/dbir/

[4] https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020-q3/#id4

clicks on the phishing link, causing the malicious code to run on the town's network. The malicious code takes advantage of an unpatched vulnerability in the network and is able to cascade, causing all the employees to be locked out of their computers. In this scenario there are multiple cyber security failures in the town. First, the employee didn't have sufficient cyber security training to recognize the signs of a phishing email. Second, the town wasn't updating their software and keeping up to date with patches. Third, the unusual activity on the network from the malicious code wasn't identified and blocked by their security system. It's critical to note that in most local governments, the IT department is responsible for all of these safety controls.

Municipal IT departments who face budget constraints and an inability to hire, won't have sufficient resources to either maintain or outsource the appropriate cyber security controls. According to a 2019 NLC Cyber Security Report *"When asked if the local government's budget was adequate, 67% of respondents said it wasn't high enough to secure the network properly"*. Moreover *"Over half of those who answered the survey said that elected officials tended not to prioritize cybersecurity budgets and policy"* and *"Only 17% of respondents say their local elected officials are very engaged in cybersecurity efforts."* When asked to what extent various factors were acting as barriers to local government achieving the highest possible level of cybersecurity "inability to pay competitive salaries for cybersecurity personnel, insufficient number of cybersecurity staff, and lack of funds" all had greater than 50% of respondents deem them either a "severe barrier" or "somewhat severe barrier". Thus increasing IT spending can increase security and decrease probability of a town getting hacked.

To illustrate the consequences of a municipal ransomware attack, Baltimore serves as a good case study. On May 7, 2019 all of Baltimore's servers except for essential services were taken offline by a ransomware attack. This impacted applications for building permits and business licenses, city worker's access to email, and property transfers necessary for real estate sales. Furthermore, citizens were unable to pay water bills, property taxes, and parking tickets. Hackers demanded $76,000 worth of Bitcoin for access to systems to be restored, but the city government refused to pay. In all, recovering from the ransomware attack lasted until September and Baltimore spent $10 million purely on IT recovery[5][6]. It's important to note that while the ransom demanded wasn't large and even the spending on IT recovery wasn't large compared to Baltimore's budget, the consequences to Baltimore's future ability to produce cash flows are much more significant. As the NLC 2019 Cyber Security Report worries "Trust in government is eroding, and security breaches may further reduce faith in government".

The sample of ransomware attacks will be detailed in the next section. However, while the ransomware attacks in our sample aren't catastrophic, hacking has the potential to be wide reaching and extremely damaging. An example of this is the NotPetya attack, which spread across numerous companies and caused supply chain disruptions which are studied in Crosignani et al. (2023). We assume in this paper, that if one town improves IT, it does not mean that it's neighbor is more (or less) likely to be hacked. An important part of our "scattershot" assumption is that a town's probability of being hacked in any given quarter depends only on it's own IT spending. This assumption holds in part because the ransomware attacks in our sample don't experience any network contagion like that seen in the NotPetya attack. The reason is that municipalities don't have supplier relationships with each other. Furthermore, news reports indicate that the hacks in our sample aren't targeted.

Given this background, it shouldn't be too surprising that, anecdotally, municipal bond investors care about cyber risk. This can be seen in a survey of municipal bond analysts by Hilltop Securities from Nov/Dec 2021. When asked *"What is your opinion of how prepared state and local governments and other municipal market participants are currently for cyber attacks?"* 63% of respondents chose "Hardly prepared" and another 30% chose "Somewhat prepared". In addition when asked *"What do you think are the 5 most important issues/trends influencing the municipal bond market today?"* Cyber security was the sixth

[5] Sources: Vox News Article

[6] Sources: https://statescoop.com/baltimore-cio-frank-johnson-no-longer-with-city-ransomware/

most popular choice (with 29% of resondents) tied with Climate change and ahead of ESG and U.S.federal government relief (2020 CARES Act, 2021 Rescue Plan Act). This is also consistent with results in the literature[7] that suggest that cyber risk is a priced factor in the cross section of stock returns for publicly traded companies.

More directly, cyber risk is a factor that bond rating agencies consider. The Moody's rating methodology for US cities and counties states that *"event risks — which are varied and can include natural disasters, sudden changes in state law or regulation, material litigation, pandemics or* cyber crime events — *can have a material credit impact on even a stable city or county."*[8][9]

4 Data

Ransomware Attacks

Our dataset of ransomware attacks is from Rege (2023) and covers the near universe of municipal hacks based on publicly disclosed events and media articles. The sample of hacks we use are those we are able to match to municipalities with bond data. In all we have 153 ransomware attacks between 2013 and 2020. Figure 1 shows the geographic distribution of counties where ransomware attacks occurred in our sample. There is a lack of any geographic clustering as one would expect for cyber attacks. Figure 2 shows the distribution of hacks over time. The number of attacks is increasing over time.

Our dataset has some shortcomings. First, it focuses only on ransomware attacks. Other types of adverse cyber events, for example data breaches, can be costly for municipalities and firms. Because we only observe ransomware attacks, it is possible that some of our control group has been exposed to treatment through other types of cyber attacks. In this case, our estimates serve as a lower bound for the true values. Another concern is that only

[7] Sources: Florackis et al. (2023); Jamilov et al. (2021)

[8] Moody's rating methodology

[9] https://www.bankinfosecurity.com/moodys-warns-cyber-risks-could-impact-credit-ratings-a-8702

large noteworthy ransomware attacks show up in our sample. Our data contains both large and small attacks on large and small municipalities, and appears to be widely distributed geographically. However, if there is selection in the types of municipalities that show up in the ransomware database, our results might not apply to the entire universe of US municipalities.

IT Spending Data

IT spending data is an important measure of how exposed to cyber risk a town is ex-ante. A contribution of this paper is that we use an actual measure of IT spending, not just a proxy. For the hacked towns and their matched pairs (described in Section 5) we manually visit each town website and find their publicly posted annual budget. A large number of towns breakout IT spending as a separate budget item, which we record for the years that it's available. If the reported value for IT is zero or the value is not reported we mark it as missing and it gets dropped from the analysis. Florida, Georgia, Arizona, and Iowa have comprehensive databases of town IT spending for the entire state which we combine and then use in some of our additional analyses.

Municipal Bonds

Data on municipal bond characteristics comes from FTSE Russell (formerly Mergent). We obtain bond characteristics including CUSIP, dated date, issuance amount, issuer name, initial offering yield, tax exempt status, insurance status, coupon rate, maturity date, and bond type. Municipal bond secondary market transaction data comes from the Municipal Securities Rulemaking Board (MSRB). Bond characteristics are merged into secondary market transactions using the bond CUSIP.

Matching bond CUSIPs to the correct issuing government can be challenging, because there is no issuer ID that can be easily mapped to the census of governments GOVSID. We extract the first 6-digits of each CUSIP (unique to each issuer). We then use Bloomberg to map each CUSIP to the county of issuance. We then use name matching within each county to map municipal bond CUSIPs to census of governments GOVSID.

We follow Gao et al. (2020) and Chava et al. (2022) in aggregating municipal bond yields to the monthly frequency. First, following Downing and Zhang (2004), we restrict our sample to only customer purchase trades. We do this to eliminate possible bid-ask bounce effects. Next, we drop CUSIPs with remaining days to maturity greater than 36,000, less than 0, or missing. Then we drop bonds with missing coupon data. We also restrict the sample to bonds with a USD price of between \$50 and \$150 (eliminating extreme outliers in price). We focus only on secondary market trades and exclude primary market trades, and trades within 15 days of initial issuance. We also drop trades within a year of maturity, and observations for which the yield is negative or greater than 50%. Finally we drop bonds for which we observe fewer than 10 transactions within the sample. We then aggregate the bond yields to the monthly level by taking a par-traded weighted average of all customer purchase trades within a given month.

To construct yield spreads, we follow Gao et al. (2020) and Longstaff et al. (2005). We first calculate the risk free price of coupon payments as well as the face value of the municipal bond using the US treasury yield curve for zero-coupon yields (Gurkaynak et al. (2006)). We then calculate the implied risk free yield using the risk price, bond coupon payments, and final face value payment. The yield spread is then calculated as the difference between the yield we observe in the trading data and the calculated risk-free yield.

We use both general obligation (GO) and revenue bonds. There are two reasons that we include both types of bonds in our analysis. First, due to our limited sample size and limited transactions in the municipal bond market, restricting our analysis by bond type would significantly reduce the power of our analysis. Second, both types of bonds can plausibly be impacted by cyber security risk. Revenue bonds that are secured by a specific type of revenue, like utility payments, would be affected by ransomware attacks that disrupt payment systems and service provision. GO bonds might be impacted by any cyber attack that imposes significant costs on the municipality and impacts default risk.

We also use data on the number of establishments, payroll, and employment of firms at the county level from County Business Patterns (CBP) data, provided by the Census. Information on population turnover comes from the IRS Statistics of Income (SOI) Migration data. Data on the number of newspapers in a given county is taken from “US News Deserts” data from the UNC Hussman School of Journalism and Media.

5 Results

Matching

We use nearest neighbor matching on several criteria to create a reasonable control group for the municipalities who are subject to a ransomware attack. We match on population, total revenue, total tax revenue, and total expenditures to match municipalities to others of similar size. We match based on the fraction of expenditures and the fraction of revenue from government transfers to account for potential differences in reliance on state governments and the types of public goods provided between municipalities in different states. We include total debt outstanding to account for the municipal debt burden, and together with tax revenues, the potential default risk. We also match exactly on the type of government as defined by the census of governments (township, municipality, county, or school district). Equation 1 shows the calculation of similarity scores between municipalities.

$$s_{ij} = \sqrt{(x_{i1} - x_{j1})^2 + ... + (x_{ik} - x_{jk})^2} \tag{1}$$

Where i and j are municipalities either within the same state, or explicitly in different states, but of the same type of government. For each municipality i, we match with a single municipality j, based on the minimum value of s_{ij}.

We perform matching both within the same state, and restricting to outside of the state. In-state matching allows us to get a more comparable control group because cities, counties, townships, or municipalities in one state might have different obligations than in other states. For example, in Massachusetts, municipal governments general fund both education as well as local infrastructure projects (like highways). In other states, county governments might fund infrastructure projects and school districts might directly raise taxes and fund education. Within the same state, the role of different types of local governments should be very similar.

There are two drawbacks to restricting matching to in-state. First, this limits the pool of potential controls. For example, in our sample we observe ransomware attacks in large cities like Baltimore or Detroit. Finding other cities of similar size in the same states is a challenge in both cases. Second, there may be spillovers in the response to ransomware attacks throughout a state. For example, if Baltimore is hacked and all neighboring cities increase cyber security infrastructure, we would underestimate our effect. We show results for both in state and out of state matching. The difference in these estimates captures (in part) the spillovers within the same state of cyber attack response.

Matching is necessary in our setting because municipal IT spending data is not widely available. We must hand collect IT data for each government. With a limited number of hacked municipalities (153), the matched sample greatly reduces the number of municipalities for which we need IT spending data.

Factors that Predict Town Hacking

We start by investigating which town characteristics predict (in sample) town hacking. Of particular interest is how town IT expenditures impact the probability of a town getting hacked. We regress a binary indicator for whether a town has been hacked on various town pre-hacking characteristics including: population, education spending, government transfers, total revenue, total tax revenue, total debt, total expenditures, and IT expenditures. We also include a state fixed effect and government type fixed effect.

We estimate the regression on two samples. First, using the universe of local governments reporting in the Census of Governments data. Using both state fixed effects and government type fixed effects, population is the only significant characteristic and is weakly positively correlated with hacking (Table 6, Column 2). This shows the randomness of hacking and the difficulty in predicting which towns are risky. A major challenge is that most of the town characteristics are correlated with each other so it's impossible to disentangle their effects on the probability of hacking.

Next, we restrict the sample to the towns for which we have IT spending data. In other words, we utilize the hacked towns and the matched sample only. In Table 6, Columns 4-6 show that towns with higher IT spending have a lower probability of being hacked despite controlling for a wide array of other potential predictors.

Ransomware Attacks and IT Spending

We next look at how towns react to a successful ransomware attack. We use the matched sample of hacked towns and control towns to estimate the regression

$$y_{it\tau} = \beta Hack_{it} + \delta X_{it\tau} + \alpha_\tau + \nu_i + \varepsilon_{it\tau} \tag{2}$$

where $y_{it\tau}$ is log of IT spending or the ratio of IT spending to total town expenditures. In different specifications we include $X_{it\tau}$ which are town characteristic controls, α_τ is a hack year fixed effect, and ν_i which is a town fixed effect.

Table 4 shows the results for the change in IT investment following a ransomware attack. The sample size is limited because IT spending data must be hand collected for each treated municipality and the matched sample. We see a significant increase in IT spending following the ransomware event. In particular, IT spending as a share of total expenditures increases by 23 basis points. Most towns have IT spending that is 1-4% of their budget so our measured magnitude is economically meaningful. Moreover, we look at the differential impact of hacking on IT spending by a town's leverage which is a proxy for how financially constrained a town is. The main effect is a 43 basis point increase in IT spending as a share of total expenditures after a hack, however, the more constrained a town is, the less the IT spending increases as a share of total expenditures. This is result is consistent with the literature on financing constraints and investment.

A reasonable hypothesis is, that increasing IT spending decreases cyber risk. This directly follows from IT spending predicting hacking as shown in the previous section. Thus, as long as cyber risk is priced in municipal bonds then we would expect the increase in IT spending after a town is hacked to correspond to a decline in bond yields. The next section test this hypothesis.

Ransomware Attacks and Bond Yields

We first look at the realization of cyber risk on financial markets. We follow Gao et al. (2020) and estimate the following regression specification

$$y_{it\tau} = \beta_\tau Hack_{it} + \delta X_{it\tau} + \alpha_\tau + \nu_i + \gamma_t + \varepsilon_{it\tau} \tag{3}$$

where $y_{it\tau}$ is the bond yield measure discussed in Section 4. As before, in different specifications we include $X_{it\tau}$ which are town characteristic controls, α_τ is a hack date fixed effect, ν_i which is a town fixed effect, and γ_t which is a year-month fixed effect.

Figure 3 shows the effect of ransomware attacks on municipal bond spreads. Interestingly, there is very little immediate impact of the ransomware attack on bond yields, but over 24 months the yields fall. The lack of response in the short term is consistent with investors already having the impact of the type of ransomware attack in our sample priced into bonds. Moreover, seeing a response over 24 months is consistent with bond yields falling due to actions taken by the town since allocating money and following through on investment takes time, especially in a government setting.

Figure 4 examines the effect on bond yields in a 30-day window around the hack. We see that there is almost no immediate effect on hacked towns relative to the matched sample.

The longer horizon decline in bond yields suggests that towns become less risky after a hack. We show in later sections that this is due to towns reacting to hacking by increasing IT spending and decreasing cyber risk and not due to alternative explanations.

Table 1 show coefficients from a differences in differences estimation of bond yields and yield spreads within 2 years of a ransomware attack. We see that the aggregate effect is roughly 12 to 17 bps in affected municipalities relative to a matched sample. Table 2 shows the same results for the out of state matched sample. The out of state match would exclude any in-state spillovers that would lead to treatment of the control group. For example, if a municipality suffering a ransomware attack lead to some kind of state wide intervention impacting the IT spending and cyber security of other municipalities. We see similar results in the out of state matched sample, indicating that there are minimal spillovers within state.

Table 3 suggests that the decline in bond yields isn't due to a liquidity channel where hacking increases the trading volume and so prices more accurately reflect fundamentals. In fact as seen in Table 3 trading volumes decline between 12% and 8%. Volume is the total bond value traded in a given month (as opposed to number of trades executed). The window we use is 24-months before to 24-months after a hack occurs.

This evidence is suggestive of a negative relationship between IT investment and bond spreads through decreased cyber risk. However, it could be the case that ransomware events lead to some other intermediate outcome that is correlated with bond spreads and IT spending separately. In other words, the decline in bond yields may be caused by an omitted variable: for example, improved business conditions due to the increase in IT spending. This would be a threat to bond yield changes after a hack capturing cyber risk.

We use several approaches in order to test the relationship between cyber risk and bond yields. First, we look at the impact of a town hack on other outcome variables that may cause bond yields to decrease. In particular we look at: number of firms, firm size, and annual payroll. We find no reaction to a hack in these other town fundamentals. Second, we use a company data breach in a given county as an exogenous shock to that county's cyber security spending and find results consistent with our main analysis.

Firm Behavior

We test whether firm behavior (measured by the number of firms, firm size, and annual payroll) changes following a ransomware attack. A potential concern would be that municipal bond yields fall not due to changes in cyber security risk, but rather because increased municipal IT investment has an effect on firm behavior. Chava et al. (2022) document a relationship between corporate subsidies and municipal bond yields. The channel here would be similar. Certain municipal investments might attract more or larger firms leading to an increase in the local tax base and ultimately a decrease in municipal bond yields. In order to rule this out, we look for changes in firm behavior before and after a cyber attack. Table 7 shows the effect of a municipal cyber attack on firm employment, annual payroll, and total number of establishments 5 years around the event. We see that there is no measurable difference in firm behavior in counties with and without a cyber attack, suggesting that increased firm investment is not driving the reduction in bond yields.

Firm Hack as Shock

Since the municipal ransomware sample size is small, we repeat our analysis looking at every county in Arizona, Florida, Georgia, and Iowa. This analysis provides further evidence that yield declines associated with increased town IT spending are capturing decreased cyber risk and not an omitted factor.

Now, instead of looking at hacks of the counties themselves, we use a company in a given county being hacked as a shock to the municipal IT spending in that county. The intuition is that company hacks don't have long term negative financial consequences as shown by Kamiya et al. (2021) where there are only negative cumulative abnormal returns in the 3 days around the announcement of a corporate data breach. Thus a corporate data breach shouldn't affect any of the underlying fundamentals of a county. Instead, a corporate data breach impacts a county by increasing the awareness and salience of cyber risk which may result in increased municipal IT investment. Moreover, the IT investment that is prompted by a corporate data breach is more likely to be targeted towards mitigating cyber risk as opposed to general computing services.

We use county IT spending data between 2008 and 2021 for counties in Arizona, Georgia, Florida, and Iowa. These states are chosen because they have centralized county data sets which include IT expenditures. Since IT data is at the county-year level, we use volume weighting to aggregate bond yields to the same level. Company hacking data comes from the PRC Data Breach database. We assign a hack to a county if either the company being hacked is headquartered in that county or, for single store / limited scope hacks, the effected part of the organization was in the county. We avoid using geographically widely reported and national level hacks because there is no clear control group in that setting. Any town reaction to a national level shock has many potential confounders.

The first question is whether county IT spending is impacted by a company hack in the county. The regression of interest is

$$\text{IT Ratio}_{i,t} = \beta \times \text{Hack Count}_{i,t} + X_{i,t} + e_{i,t} \tag{4}$$

where *IT Ratio* is the percentage (out of 100) of total expenditures that are IT spending. *Hack Count* is a time series of the number of disclosed company hacks in a county. The intuition is that with each additional company hack in a county there is additional attention and salience. $X_{i,t}$ captures the controls. We control for the state and include different combinations of year and county fixed effects. By controlling for the state we mitigate the concern that different states might take varied approaches in oversight and regulations for IT and cyber security of municipalities.

The results are shown in Table 8, Columns 1-3. While all the specifications are positive and similar in magnitude only the county fixed effect specification is statistically significant.

We find that the average extra company hack in a county increases the level of the IT ratio in that county by 8.5 bps. This is reasonable compared to the magnitudes of IT spending in our sample where the mean IT ratio is 1.2%.

Next we look at whether municipal yields decline as IT spending increases around a firm hack. Table 8, Columns 4-6 show that yield spreads decline between 3.5 and 7.7 bps. This provides further evidence that cyber risk is priced in municipal bond yields.

However, in order to directly link IT spending and cyber risk and make a causal statement we would need to go a step further. We try using firm hacking as an instrument for IT Ratio in the endogenous regression:

$$\text{Spread}_{i,t} = \beta \times \text{IT Ratio}_{i,t} + X_{i,t} + e_{i,t} \tag{5}$$

Unfortunately, as Table 9 shows our IV regression is under powered due to the limited sample size. Despite this, the results in Table 9 find that increasing IT spending decreases bond yields. This is consistent with the story of ransomware attacks disciplining governments to decrease cyber security risk in the long run. While the magnitudes of the measured effects are unrealistic, the consistency in sign of the estimated coefficients is encouraging evidence.

6 Why Does Town IT Spending React to Hacking?

There are two possible explanations for why stakeholders in a town react to being hacked. The first is that before the hack they are at the optimal level of IT investment, and the hack reveals new information which changes their optimal level of investment. This is highly implausible since bond investors aren't learning new information. The second is that towns weren't at their optimal level of IT investment and being hacked forces towns to adjust their IT. In other words, there is underinvestment in IT by towns and the hacks in our sample act as disciplining devices. Of course underinvestment can be driven by a number of economic mechanisms including agency problems, myopia, and salience. We use heterogeneity exercises to tease out evidence for underinvestment due to myopia and salience.

Potential Mechanisms

We divide the sample into multiple subsamples to understand heterogeneous effects that are informative of the underlying economic channel behind underinvestment in IT.

If ransomware attacks act as a governance mechanism, we would expect a stronger effect when ex ante governance is relatively weak. In order to test for this we construct a measure for citizen inattention in local government policy. We do this by measuring population turnover by county. Turnover is defined by the sum of in-migration and out-migration divided by total population. We measure turnover for 2015, and then characterize each county as high or low turnover based on whether it is above or below the median turnover value.

Table 10 shows that the effect of ransomware events on bond yields is concentrated in municipalities in high turnover counties. Similarly, in Table 11 we see that the positive effect in IT spending is also concentrated in high turnover municipalities. Together these results suggest that under investment in IT may be driven by inattention on the part of local residents. When a ransomware attack creates public scrutiny around municipal IT practices, these high inattention and low IT investment counties increase investment leading to the long-run reduction in cyber risk.

In addition to looking at ex-ante measures of resident attention, we can also look at how easily news of the ransomware event would disseminate to local residents. To do this, we can follow Gao et al. (2020) and look at local newspapers. While Gao et al. (2020) find that newspapers serve an ex-ante monitoring role, our results are more consistent with an ex-post information role similar to what is found by Bana et al. (2022). Table 12 shows that bond yields decline more in counties with more newspapers. Moreover, Table 13 shows that IT spending increases by more in towns with more newspapers. If newspapers were serving as monitoring devices then we would expect that towns with more newspapers would react less to being hacked because they would already be closer to the optimal level of IT investment. Instead, in our setting, newspapers complement the disciplining of towns.

7 Conclusion

Cyber risk is an important issue for both firms and municipalities that is both understudied and receiving increasing policy attention. We show evidence that IT investment is under provided by municipalities and following cyber events, IT spending increases and municipal borrowing costs fall. We find that both resident inattention and newspaper monitoring play a role in this response.

Following a cyber attack, we see very little short term effect (less than 12 months) on municipal bond yields. We see a significant negative effect on yields in a 24 month window following ransomware attacks. We also find that municipalities victimized by cyber attacks increase IT investment in the following years. Taken together, these results suggest that cyber attacks lead to an increased provision of efficient IT investment, reducing the risk of cyber attacks and decreasing municipal bond yields in the long run.

We investigate several channels leading to the potential under provision of IT investment at the municipal level. First we show that underinvestment may be driven by resident inattention and short-termism. We show that counties with high resident turnover experience the largest decrease in bond yields following ransomware attacks. We also show that monitoring and local news coverage can play a role in mitigating the underinvestment. In municipalities with local newspapers, bond yields fall the most. We separately use firm hacking in a given county as an exogenous shock to county IT spending and show IT spending rises while bond yields fall.

These results show important differences between cyber security risk and other potential risks faced by municipalities such as climate risk. Similarly to adverse climate events, ransomware attacks signal specific vulnerabilities and suggest that future cyber events are increasingly likely in the future. However, to a much larger extent than climate risk, municipalities are able to invest to mitigate the risk of future cyber attacks. While cyber attacks don't appear to change municipal bond yields, the following investment in IT infrastructure appears to decrease municipal risk.

One potential channel that we don't investigate in this paper is whether IT investment is only useful in decreasing cyber security risk when other municipalities remain vulnerable. If every other municipality became more secure, would that increase the probability of being targeted for a cyber attack? This has clear policy implications for how to reduce aggregate cyber risk for municipalities and even corporations. Further work is needed to understand the spillovers in cyber security between municipalities and firms.

Another key question that is beyond the scope of this paper is why towns do not appear to be at the optimal level of IT investment. A change in IT investment after a hack suggests that the hack is acting as a disciplining device of some sort. This could be due to incompetent or wasteful municipal governance, or because governments are maximizing some private benefit instead of making efficient investments, as suggested in Diamond (2017). It could also be a product of a benevolent and rational government that is maximizing benefit to taxpayers and taxpayer demand for IT investment changes following ransomware attacks.

More work is needed to understand the impact of cyber security risk on both firm and municipal investment behavior.

References

Adelino, M., Cunha, I., and Ferreira, M. A. (2017). The economic effects of public financing: Evidence from municipal bond ratings recalibration. *Review of Financial Studies*, 30:3223–3268.

Agrawal, A. and Kim, D. (2022). Municipal bond insurance and public infrastructure: Evidence from drinking water.

Amornsiripanitch, N. (2022). The real effects of municipal bond insurance market disruptions. *Journal of Corporate Finance*, 75:102240.

Bana, S., Brynjolfsson, E., Jin, W., Steffen, S., and Wang, X. (2022). Cybersecurity Hiring in Response to Data Breaches . *WP*.

Chava, S., Malakar, B., and Singh, M. (2022). Impact of corporate subsidies on borrowing costs of local governments: Evidence from municipal bonds.

Crosignani, M., Macchiavelli, M., and Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains . *Journal of Financial Economics*.

Diamond, R. (2017). Housing supply elasticity and rent extraction by state and local governments. *American Economic Journal: Economic Policy*, 9(1):74–111.

Downing, C. and Zhang, F. (2004). Trading activity and price volatility in the municipal bond market. *Journal of Finance*, 59:899–931.

Florackis, C., Louca, C., Michaely, R., and Weber, M. (2023). Cybersecurity Risk . *Review of Financial Studies*.

Gao, P., Lee, C., and Murphy, D. (2020). Finance dies in darkness? The impact of newspaper closures on public finance . *Journal of Financial Economics*.

Gurkaynak, R. S., Sack, B., and Wright, J. H. (2006). The u.s. treasury yield curve: 1961 to the present. *Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board, Washington, D.C.*

Jamilov, R., Rey, H., and Tahoun, A. (2021). The Anatomy of Cyber Risk . *NBER Working Paper*.

Jerch, R., Kahn, M. E., and Lin, G. C. (2020). Local public finance dynamics and hurricane shocks.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., and Stulz, R. M. (2021). Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms . *Journal of Financial Economics*.

Lattanzio, G. and Taillard, J. P. (2023). M&A and Cybersecurity Risk: Empirical Evidence

. *WP*.

Longstaff, F. A., Mithal, S., and Neis, E. (2005). Corporate yield spreads: Default risk or liquidity? new evidence from the credit default swap market. *Journal of Finance*, 60:2213–2253.

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

Rege, A. (2023). Critical Infrastructure Ransomware Attacks (CIRA) Dataset . *Temple University*, Version 11.9. Online at `https://sites.temple.edu/care/ci-rw-attacks/`. Funded by National Science Foundation CAREER Award #453040. ORCID: 0000-0002-6396-1066.

Schwert, M. (2017). Municipal bond liquidity and default risk. *The Journal of Finance*, 72:1683–1722.

A Additional Tests

Table 14 shows the effect of ransomware attacks on bond yield spreads. We see a similar effect as with bond yields. In general, spreads fall between 13 and 20 bps in the 24-months following a ransomware attack.

We also divide the sample in half by the hacking date. Table 15 shows the effect of the hack on bond yields for each subsample. We see that all of the effect is concentrated in the early portion of the sample. The reasons for this are a little unclear. This result could be evidence that IT underinvestment is decreasing overtime, or that the disciplining effect of ransomware attacks on IT investment is being increasingly priced in by the market.

Table 16 shows the effect of ransomware attacks on bond yields comparing the in-state and out-of-state matched sample, neither of which were actually victims of the attack. This allows us to quantify potential in-state spillovers. For example, if another municipality within the same state were the victim of a ransomware attack, and this prompted additional IT investment by all municipalities within the state. We see that there are no significant effects, suggesting that there are not significant spillovers within state.

Table 17 examines the 30-day yield response to ransomware events relative to the out-of-state matched sample. We see, consistent with 4 that there are no significant effects. If anything, we see a small significant positive effect one specification, suggesting that markets view the hack as bad news. This is consistent with the story that the hack itself is not good for bond yields, but rather the increased IT investment over the following 24 months leads to decreased yields.

Tables

Table 1: Yield Response to Hack
Effect of ransomware attacks on bond yields. Comparing hacked municipalities with in-state matched municipalities. Observations are at the bond-month level.

	(1)	(2)	(3)	(4)	(5)
Hack X Post	-0.33	-0.19	-0.17**	-0.12**	-0.13**
	(-1.25)	(-1.65)	(-2.40)	(-2.08)	(-2.14)
Controls	No	No	No	No	Yes
Year-Month FE	No	Yes	Yes	Yes	Yes
Muni FE	No	No	No	Yes	Yes
Hack Date FE	No	No	Yes	No	No
Observations	54082	54082	54082	54081	53293
R$\hat{2}$	0.05	0.31	0.39	0.50	0.57

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 2: Yield Response to Hack Out-of-State Match
Effect of ransomware attacks on bond yields. Comparing hacked municipalities with out-of-state matched municipalities. Observations are at the bond-month level.

	(1)	(2)	(3)	(4)	(5)
Hack X Post	-0.20	-0.28*	-0.29**	-0.13***	-0.14**
	(-0.74)	(-1.95)	(-2.17)	(-2.60)	(-2.54)
Controls	No	No	No	No	Yes
Year-Month FE	No	Yes	Yes	Yes	Yes
Muni FE	No	No	No	Yes	Yes
Hack Date FE	No	No	Yes	No	No
Observations	61791	61791	61791	61787	60848
R^2	0.05	0.27	0.29	0.48	0.54

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 3: Trading Volume Response to Hack

	(1)	(2)	(3)	(4)	(5)
Hack X Post	-0.12**	-0.10**	-0.09**	-0.09**	-0.08**
	(-2.48)	(-2.28)	(-2.12)	(-2.16)	(-2.38)
Controls	No	No	No	No	Yes
Year-Month FE	No	Yes	Yes	Yes	Yes
Muni FE	No	No	No	Yes	Yes
Hack Date FE	No	No	Yes	No	No
Observations	52974	52974	52974	52973	52208
R^2	0.00	0.01	0.04	0.06	0.11

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 4: IT Response to Hack

	(1)	(2)	(3)	(4)	(5)	(6)
	log_IT	IT_share	IT_share	IT_share	IT_share	IT_share
	b/t	b/t	b/t	b/t	b/t	b/t
treat_post	0.10	0.23**	0.23**	1.04	0.43***	-0.81
	(0.87)	(2.18)	(2.18)	(1.19)	(3.46)	(-0.72)
treat_post × log_population				-0.06		
				(-0.87)		
treat_post × leverage					-0.08*	
					(-1.95)	
treat_post × constraint						1.12
						(1.09)
govsid FE	No	No	No	Yes	Yes	Yes
match_id FE	Yes	Yes	Yes	No	No	No
hack_year FE	No	No	Yes	Yes	No	Yes
Observations	637	637	637	637	637	637
R^2	0.870	0.642	0.642	0.899	0.899	0.899

* $p < .10$, ** $p < .05$, *** $p < .01$

Table 5: Treatment on Treated: log(IT) around hacking
Effect of ransomware attacks on municipal IT spending. Dependent variable is either log(IT spending) or the share of IT spending in total government expenditures.

	(1)	(2)	(3)	(4)	(5)	(6)
	log_IT	IT_share	IT_g	IT_share	IT_share	IT_share
	b/t	b/t	b/t	b/t	b/t	b/t
post	0.12	0.17**	0.08	0.25***	-0.95	0.88
	(0.93)	(2.42)	(0.36)	(3.28)	(-0.89)	(1.11)
post × leverage				-0.09*		
				(-2.18)		
post × constraint					1.08	
					(1.04)	
post × log_population						-0.06
						(-0.95)
Constant	13.74***	1.11***	0.30***	1.10***	1.10***	1.11***
	(306.27)	(55.85)	(9.59)	(59.47)	(58.50)	(54.75)
govsid FE	Yes	Yes	Yes	Yes	Yes	Yes
year FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	316	316	316	316	316	316
R^2	0.909	0.829	0.408	0.832	0.832	0.831

* $p < .10$, ** $p < .05$, *** $p < .01$

Table 6: Determinants of Being Hacked
Results of a simple linear regression whether a municipality is the victim of a ransomware attack and several municipal characteristics.

	(1)	(2)	(3)	(4)	(5)	(6)
Log(Population)	0.00***	0.00*	-0.11**	-0.10**	-0.11**	-0.11**
	(4.53)	(1.80)	(-2.36)	(-2.24)	(-2.41)	(-2.36)
Education Spending / Total Revenue	-0.01***	-0.00	0.18	0.15	0.19	0.23
	(-3.31)	(-0.24)	(0.50)	(0.43)	(0.54)	(0.66)
Government Transfers / Total Revenue	-0.00	-0.00	0.30*	0.31*	0.38**	0.36**
	(-0.23)	(-0.37)	(1.78)	(1.85)	(2.22)	(2.14)
Log(Total Revenue)	0.00	0.00	-0.05	-0.08	-0.13	-0.15
	(1.16)	(1.33)	(-0.39)	(-0.57)	(-0.93)	(-1.08)
Log(Total Tax Revenue)	-0.00	-0.00	0.11**	0.15***	0.18***	0.15***
	(-0.57)	(-0.39)	(2.24)	(3.03)	(3.44)	(3.13)
Log(Total Debt)	-0.00**	-0.00	-0.01	-0.01	-0.01	-0.01
	(-2.27)	(-0.27)	(-0.49)	(-0.43)	(-0.33)	(-0.90)
Log(Total Expenditures)	0.00	-0.00	0.08	0.09	0.14	0.15
	(0.35)	(-0.25)	(0.61)	(0.64)	(1.00)	(1.09)
log(IT Exp.)				-0.03**	-0.04***	
				(-2.51)	(-2.84)	
IT/Total Expenditures						-0.00***
						(-2.76)
State FE	No	Yes	No	No	Yes	Yes
Government Type FE	No	Yes	Yes	Yes	Yes	Yes
Observations	30,990	30,989	254	254	254	254
Adj. R^2	0.01	0.02	0.04	0.06	0.07	0.07

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 7: Firm Response to Municipal Cyber Events

	(1) Establishments	(2) Establishments	(3) Establishments	(4) Employees	(5) Payroll
Hack X Post	-1236.49	24.92	24.00	1948.55	608997.51*
	(-0.45)	(0.30)	(0.29)	(0.91)	(1.81)
Year FE	No	No	Yes	Yes	Yes
Muni FE	No	Yes	Yes	Yes	Yes
Observations	1378	1378	1378	1378	1378
R^2	0.02	1.00	1.00	1.00	0.99

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 8: How Private Company Hacks co-move with both Muni IT Spending and Muni Bond Spreads

	(1)	(2)	(3)	(4)	(5)	(6)
	IT Ratio	IT Ratio	IT Ratio	spread	spread	spread
	b/t	b/t	b/t	b/t	b/t	b/t
Hack Count	0.002	0.085***	-0.009	-0.035*	-0.077**	-0.020
	(0.09)	(3.18)	(-0.30)	(-1.81)	(-2.23)	(-0.59)
County FE	No	Yes	Yes	No	Yes	Yes
State FE	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	No	Yes	Yes	No	Yes
Observations	1146	1146	1146	1146	1146	1146
R^2	0.223	0.017	0.223	0.321	0.008	0.323

* $p < .10$, ** $p < .05$, *** $p < .01$

Table 9: IV Approach

	(1)	(2)	(3)
	spread	spread	spread
	b/t	b/t	b/t
IT Ratio	-0.557**	-0.905**	2.296
	(-2.21)	(-2.14)	(0.25)
Constant	3.065***	6.345***	-9.692
	(3.50)	(2.72)	(-0.21)
County FE	No	Yes	Yes
State FE	Yes	Yes	Yes
Year FE	Yes	No	Yes
Observations	1146	1146	1146
R^2	0.227	0.000	0.041
F	24.096	4.497	60764682.103

* $p < .10$, ** $p < .05$, *** $p < .01$

Table 10: Yield Spread in High and Low Turnover Counties
Differential effects of ransomware attacks on municipal bond yields in high and low population turnover counties. Population turnover is defined as the total migration inflows plus outflows divided by total population. High turnover counties are above the median value and low turnover are below. Observations are at the bond month level.

	(1)	(2)
	High Turnover	Low Turnover
Hack X Post	-0.20***	-0.07
	(-2.94)	(-0.71)
Controls	Yes	Yes
Year-Month FE	Yes	Yes
Muni FE	Yes	Yes
Hack Date FE	No	No
Observations	21267	32027
R^2	0.41	0.53

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 11: Hack interacted with county turnover
Differential effects of ransomware attacks on IT investment in high and low population turnover counties.

	(1)	(2)	(3)	(4)
	log_IT	log_IT	IT_share	IT_share
	b/t	b/t	b/t	b/t
treat_post	-0.07	-0.21	0.05	-0.20
	(-0.27)	(-0.76)	(0.40)	(-1.80)
treat_post × high_turnover	0.89*	0.89*	0.68*	0.66
	(1.98)	(2.04)	(1.67)	(1.80)
County FE	Yes	Yes	Yes	Yes
year FE	No	Yes	No	Yes
Observations	637	637	637	637
R^2	0.543	0.549	0.726	0.745

* $p < .10$, ** $p < .05$, *** $p < .01$

Table 12: Hack interacted with county newspaper count
Differential effects of ransomware attacks on municipalities based on the number of local newspapers

	(1) yield b/t	(2) yield b/t
treat_post	-0.125**	-0.108**
	(-2.24)	(-2.06)
News Paper	0.000	0.000
	(.)	(.)
treat_post × News Paper	-0.003***	-0.003***
	(-4.68)	(-5.35)
govsid FE	Yes	No
cusip FE	No	Yes
year FE	Yes	Yes
Observations	53390	52881
R^2	0.476	0.842

* $p < .10$, ** $p < .05$, *** $p < .01$

Table 13: Hack interacted with county newspaper count

	(1) log_IT b/t	(2) log_IT b/t	(3) IT_share b/t	(4) IT_share b/t
treat_post	0.063	-0.147	0.355***	0.061
	(0.56)	(-1.10)	(2.76)	(0.55)
treat_post × News Paper	0.007***	0.007***	-0.001	-0.002
	(5.27)	(4.11)	(-0.65)	(-1.20)
govsid FE	Yes	Yes	Yes	Yes
year FE	No	Yes	No	Yes
Observations	637	637	637	637
R^2	0.939	0.944	0.898	0.912

* $p < .10$, ** $p < .05$, *** $p < .01$

Table 14: Yield Spread Response to Hack
Effect of ransomware attacks on bond yield spreads. Comparing hacked municipalities with in-state matched municipalities. Observations are at the bond-month level.

	(1)	(2)	(3)	(4)	(5)
Hack X Post	-0.18	-0.23	-0.20*	-0.14**	-0.13*
	(-0.60)	(-1.56)	(-1.96)	(-2.07)	(-1.77)
Controls	No	No	No	No	Yes
Year-Month FE	No	Yes	Yes	Yes	Yes
Muni FE	No	No	No	Yes	Yes
Hack Date FE	No	No	Yes	No	No
Observations	54082	54082	54082	54081	53293
R^2	0.02	0.22	0.32	0.43	0.49

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 15: Early and Late Sample Yield Response
The effect of ransomware attacks on bond yields of hacked municipalities relative to a matched sample, split by year.

	(1)	(2)
	Prior to 2018	Post 2018
Hack X Post	-0.24*	-0.01
	(-1.88)	(-0.13)
Controls	Yes	Yes
Year-Month FE	Yes	Yes
Muni FE	Yes	Yes
Hack Date FE	No	No
Observations	26123	27170
R^2	0.53	0.44

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 16: In-State vs Out-of-State Match
The effect of ransomware attacks on bond yields, comparing the in-state and out-of-state matched sample, neither of which were the victim of ransomware attacks. For example, suppose that city A was the victim of a ransomware attack at time T, and that city A is matched to city B (in-state) and city C (out-of-state). This shows the effect of the hack at time T on yields in city B relative to city C, in order to quantify potential spillovers of government response within state.

	(1)	(2)	(3)	(4)	(5)
In-State X Post	0.14	-0.03	-0.05	-0.02	-0.02
	(0.62)	(-0.80)	(-1.29)	(-0.59)	(-0.63)
Controls	No	No	No	No	Yes
Year-Month FE	No	Yes	Yes	Yes	Yes
Muni FE	No	No	No	Yes	Yes
Hack Date FE	No	No	Yes	No	No
Observations	53785	53785	53785	53780	53168
R^2	0.02	0.23	0.27	0.35	0.44

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 17: Short-term Yield Response to Hack
The response of bond yields to ransomware attacks in a hacked municipality relative to an out-of-state matched municipality within 30-days of the ransomware attack

	(1)	(2)	(3)	(4)
Hack x Post	0.00	-0.05	-0.03	0.04**
	(0.02)	(-0.83)	(-0.67)	(2.22)
Constant	2.01***	0.70	0.41	2.32***
	(20.78)	(0.66)	(0.36)	(67.63)
Controls	No	Yes	Yes	No
Date FE	No	No	Yes	Yes
Muni FE	No	Yes	Yes	No
CUSIP FE	No	No	No	Yes
Observations	3752	3643	3384	2463
R^2	0.02	0.70	0.77	0.99

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Figures

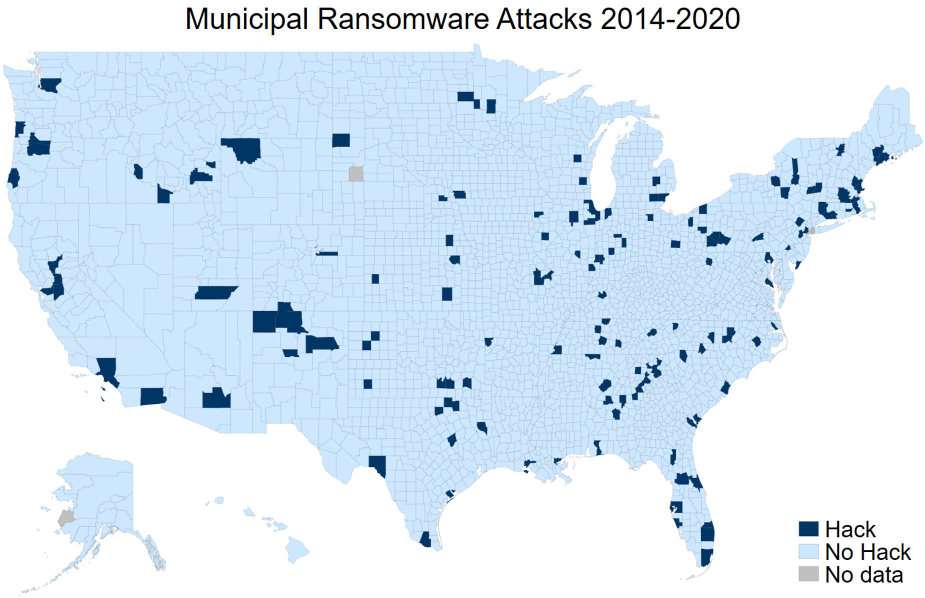

Figure 1: Map of Municipal Ransomware Attacks

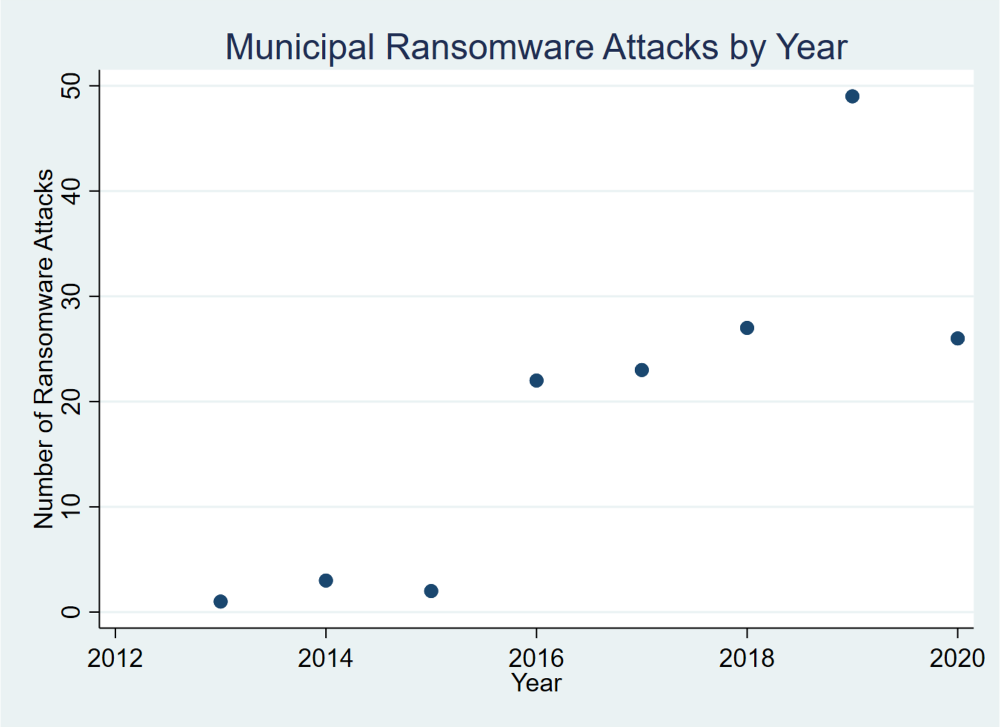

Figure 2: The Number of Municipal Ransomware Events by Year

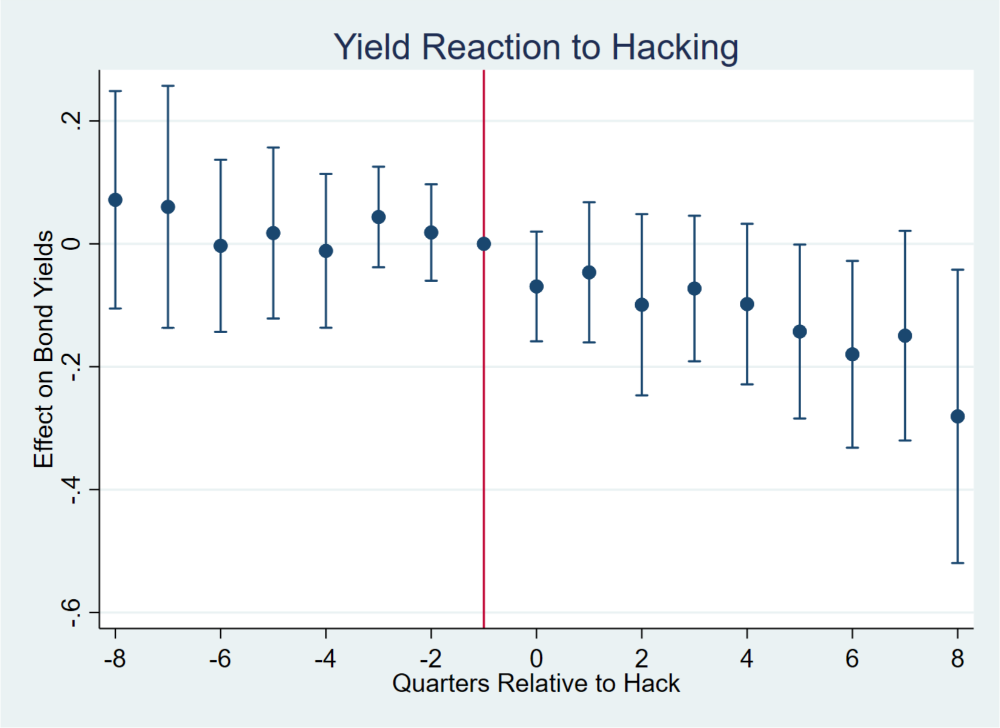

Figure 3: Event study of municipal bond yields following ransomware attacks

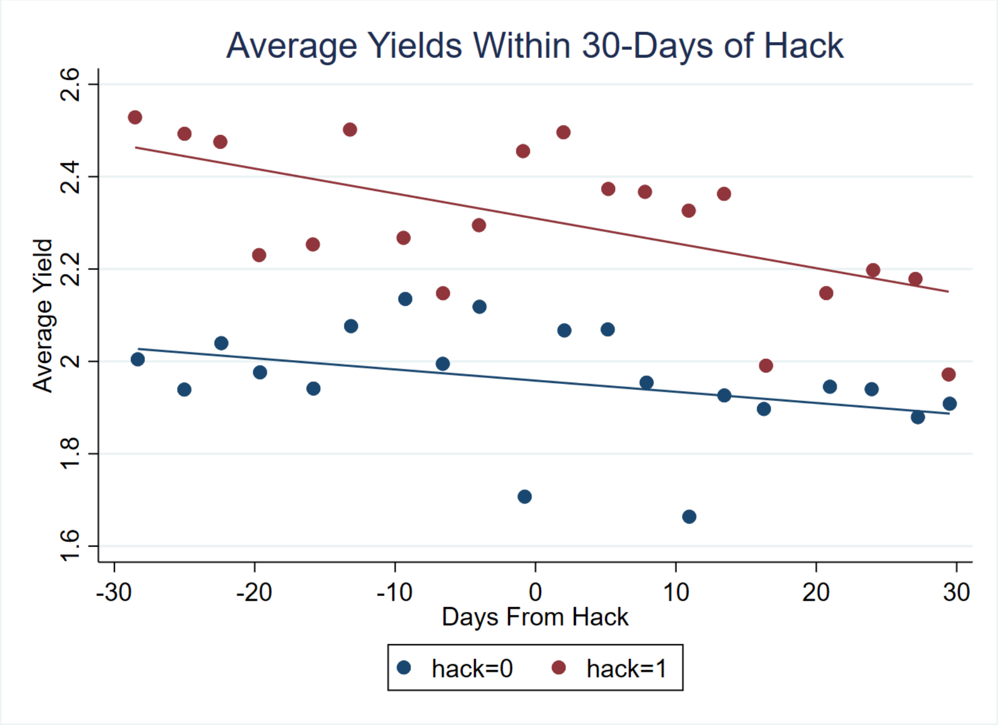

Figure 4: Bond yields in hacked and control municipalities within 30-days of the hack event