Cyberattacks, Media Coverage and Municipal Finance

L. Andreadis*, E. Kalotychou*, C. Louca*, C. Lundblad[§], and C. Makridis[¶*1]

First Draft: 14 Oct 2022

This version: 06 Jun 2023

Abstract

We investigate the role of information dissemination about cyberattacks through major newswires on municipal finance. Employing a difference-in-differences approach to identify causal effects, we find that county-level cyberattacks covered by the media cause increases in new offer yields and reduce bond issuance. Heterogeneous effects related to investor clientele suggest a capital supply channel. Municipalities respond to financing shortages by drawing their cash holdings and reducing their more elastic investments. Overall, awareness of cybersecurity risk hinders municipalities' access to capital and restricts their ability to provide public services and infrastructure.

Keywords: Cyberattack, Media, Municipal Bonds, Public Finance, Public attention

JEL code: G12, G14, H74

---

[*]Cyprus University of Technology (ek.andreadis@edu.cut.ac.cy, eleni.kalotychou@cut.ac.cy, christodoulos.louca@cut.ac.cy)

[§] University of North Carolina, Chapel Hill (christian_lundblad@kenan-flagler.unc.edu)

[¶] Stanford University (cmakridi@stanford.edu).

---

[1] We would like to thank Cláudia Custódio, Chris Florackis, Ioannis (Yianni) Floros, Dennis Philip as well as conference and seminar participants at Financial Engineering & Banking Society 2022, Hellenic Finance and Accounting Association 2022, Financial Management & Accounting Research 2022. Special thanks to Bledi Taska at Lightcast and Sebastian Steffen for sharing the cybersecurity job posting data and to John Hund for guidance on municipal finance issuance data. The authors thank MSRB for providing the official statements of municipal bonds issuances. Thanos Pafitis and Charis Pezeridis provided excellent research assistance. All opinions reflect those of the authors and not those of any affiliated institutions.

1. Introduction

The role of media coverage in capital markets has been extensively studied in the field of finance and economics (e.g., Beaudry and Portier, 2014; Tetlock, 2015). While prior literature has focused on understanding how the media acts as an amplification and propagation mechanism in *private* markets, the impact of media coverage on public finance remains largely unexplored.[2] Media coverage can have significant effects on public finance by altering the marginal cost of financing public debt, resulting in negative externalities (e.g., Gao, Lee and Murphy, 2020). This study aims to explore the impact of news dissemination, specifically related to publicly reported data breaches, on municipalities' access to finance.

Cyberattacks have become increasingly severe and widespread, posing a significant concern for market participants (World Economic Forum, 2021). If media coverage of a data breach, which is clear, sharp, and specific, increases awareness of cybersecurity risk and reinforces investors' *broader* perception of its prevalence, then investors will demand a higher reward to compensate for bearing the risk. Conversely, if public news on cyberattacks is not acknowledged by markets and investors, it should not significantly impact the local financial market. Understanding the scale of the effects, if any, is, therefore important for influencing technology policy and regulation.

To investigate the impact of information dissemination about cyberattacks through major news sources on municipalities' access to finance, we focus on the

[2] Media attention can causally influence private markets (Dyck and Zingales, 2003; Tetlock, 2007; Dougal et al., 2012), by affecting investors' information processing and beliefs, trading behavior and ultimately equilibrium asset prices (Engelberg and Parsons, 2011; Solomon, Soltes and Sosyura, 2014; Ahern and Sosyura, 2015). In addition, it has the potential to tighten corporate governance (Dyck et al., 2008; Dyck et al., 2010), but can also amplify behavioural biases and overreaction (Shue and Townsend, 2021; Jiang, Liu, Peng and Wang, 2022).

municipal bond market. This market provides an ideal setting due to its retail investor dominance, establishing a more direct link between media coverage and security prices (Schultz, 2013). As proxies for information dissemination, we use the cumulative number of cyberattacks covered by major newswires and the corresponding number of cyberattack-related news articles. Considering (i) that the impact of cyberattacks and pertinent news is stronger for investors closer to the incident's location (Kang and Kim, 2008; Kedia and Rajgopal, 2009) and (ii) the significant within-state dispersion in the frequency of cyberattacks, we measure information dissemination at the county level, allowing us to compare similar areas that happen to be subject to different cyberattacks.

To establish the causal effect of information dissemination about cyberattacks on municipalities' access to finance, we employ a difference-in-differences framework. This framework accounts for multiple treatment and control groups (Bertrand and Mullainathan, 2003), making it suitable for analyzing cyberattacks that occur at different times and in different counties. Our main finding is that both the cumulative number of cyberattacks covered by major newswires (henceforth major attacks) and the corresponding number of cyberattack news articles (henceforth major attack news) have a significant adverse effect on municipal bond yields. Interestingly, this effect becomes stronger for counties exposed to a greater number of major attacks and major attack news. In economic terms, a 1% increase in the number of major attacks (major attack news) leads to an increase in offering yields ranging from 3.7 (1.6) to 5.9 (2.7) bp, depending on the level of attack exposure.

To address methodological and endogeneity concerns, we conduct a variety of robustness tests. Recognizing the growing concerns about staggered two-way fixed effects difference-in-differences models, (Goodman-Bacon, 2021; Sun and Abraham,

2021), we follow Cengiz, Dube, Lindner and Zipperer (2019) and employ a "stacked regression" model, which combines event-specific datasets comprised of the treated cohort (i.e., the attacked county) and all the other "clean" control observations within the treatment window (i.e., counties that have not experienced a cyberattack by the end of our sample period). This approach along with stacked-by-time fixed effects addresses a "bad comparison" problem, which may bias the estimates. (e.g., Baker, Larcker and Wang, 2022). The results become stronger, indicating that the "bad comparison" problem undermines the significance of the results. Furthermore, we find no pre-trend – bond yields of treated and control counties are statistically indistinguishable before the cyberattacks, affirming a causal relationship.

Furthermore, we address concerns that both cyberattacks and bond yields may be driven by underlying local economic conditions. A coarsened exact matching, however, indicates that the results are robust to selection effects arising from county characteristics that may make attacks in certain counties more, or less plausible. In addition, by exploiting variation within-county clusters that exhibit similar economic conditions, and within-adjacent counties, we continue to find a significant positive effect on bond yields indicating that the effect is causal and not driven by deteriorating local economic conditions coinciding with major attacks and major attack news.

Next, we investigate the role of both issuer and investor awareness about cybersecurity risk following major attacks and news as a potential mechanism behind these results. Specifically, we find positive correlations between major attacks and major attack news with (i) explicit textual warnings about cybersecurity risk that issuers provide to investors through the bonds' official statements, and (ii) a notable surge (abnormal) in investor attention towards cybersecurity risk, as evident by state-level

monthly search volume index (SVI) data from Google Trends. Crucially, both explicit warnings and heightened investor attention about cybersecurity risk moderate the relationship between major attacks and major attack news with bond yields. We also conduct a placebo test that considers attacks whose information *ex-ante* is less likely to reach investors. Interestingly, we find no relation between these attacks with bond yields, something that reinforces the role of information transmission from press coverage for our results. Finally, we also find that our main results become stronger with time, implying a gradual increase in market participants' awareness of cybersecurity risk.

These findings support the view that the publicity of cyberattacks, the corresponding information dissemination through major newswires, and the increased issuer and investor awareness about cybersecurity risk are crucial drivers of our results. Essential for such an interpretation, however, is also the prevalence of cybersecurity risk. In the presence of such risk, rational entities are expected to proactively implement security measures to safeguard against cybersecurity threats. One such measure is investment in human capital to improve cybersecurity expertise. Accordingly, we explore the impact of such investment on the relationship between major attacks and major attack news with bond yields. Using job postings data aggregated at the county-level and cumulated over time, as a proxy for human capital investment, we find that both the number of cyber job postings and the job posting cyber skills strengthen the relationship between major attacks and major attack news with bond yields.

Beyond establishing the causal effect of major attacks on yields, and understanding the driving mechanism, we also examine which type of bonds are mostly affected.. Anecdotal evidence suggests that the actual cost of a cyberattack

encompasses financial loss from service disruption, recovery expenses, and the challenge of allocating capital to prevent future attacks.[3] Accordingly, cyberattacks represent an emerging risk and can have significant fiscal costs leading potentially to disruption of the local economy and increase in default risk.[4] As default risk is a major determinant of bond yields (Wang, Wu, Zhang, 2008; Schwert, 2017) we investigate its role in the association between cybersecurity risk awareness and yields. We find that the impact of cybersecurity risk awareness on yields concentrates among riskier bonds – that is, the uninsured bonds (whose cash flows are not backed by a third party) and long-maturity bonds (whose cash flows are more sensitive to cyberattack implications) are the ones more affected.

Furthermore, we investigate the financing and investing implications for municipalities. Municipalities facing higher cybersecurity risk may encounter challenges in raising capital. We find a negative relationship between cybersecurity risk awareness and both the probability and the amount of county-level municipal debt issuance. This finding suggests that as capital becomes costlier, municipalities face difficulties in securing funds through bond issuance. We also consider investor clientele and their incentives to invest locally (Babina et al., 2021; Bergstresser and Cohen, 2018) and find evidence supporting a capital supply channel. In particular, the effect of cybersecurity risk awareness on the amount and probability of county-level bond issuance is more prevalent in counties with lower levels of investor home bias and no

[3] For example, in 2020 alone, ransomware attacks against U.S. government organizations impacted 71 million people and carried an estimated price tag of $18.88 billion in downtime and recovery costs (See: The Economic Impact of Cyber Attacks on Municipalities, white paper, KnowBe4.com)

[4] See: "Cyber Attacks Present Credit Risk to Muni Issuers, S&P Says", Bloomberg (https://news.bloomberglaw.com/privacy-and-data-security/cyber-attacks-present-credit-risk-to-muni-issuers-s-p-says)

tax privilege legislation. This indicates that stronger incentives to supply capital to the local bond market mitigate the cyberattack risk awareness effect, perhaps due to closer ties within the area or tax-induced benefits.

Moreover, as awareness of cybersecurity risk impedes municipalities' access to capital, they are compelled to rely more on internal financing. In this vein, we find a negative relationship between cybersecurity risk awareness and cash holdings. If cash holdings, however, are insufficient to support financing needs, municipalities may also reduce total expenditures. Supporting this notion, we observe a negative relationship between cybersecurity risk awareness and total capital outlays, driven by declines in more elastic capital outlays.

In conclusion, our results indicate that markets respond to data breaches: awareness of cybersecurity risk negatively impacts municipalities through increased financing costs and reduced ability to access capital. Municipalities respond by utilizing cash reserves to support their activities, but this is not always sufficient, leading to reductions in total capital outlays, particularly more elastic capital outlays.

2. Related literature and contribution

This study contributes to several strands of the literature. First, it relates to the literature on the role of information asymmetry in the municipal bond market. This opaque market is largely dominated by retail investors, who underreact to information (Da, Engelberg, and Gao, 2011; Ben-Raphael, Da, and Israelson, 2017) because they lack the ability and resources to attend to and digest information promptly (Barber and Odean, 2008), resulting in inefficiencies (Harris and Piwowar, 2006; Cornaggia, Cornaggia, and Israelsen, 2020). Our results highlight the role of media in alleviating

information asymmetry by helping diffuse information about an emerging risk, such as cybersecurity risk. Specifically, placing a cyberattack in the forefront of public discourse lowers the cost of information acquisition (Grossman and Stiglitz, 1980), and increases investors' attention (Merton, 1987; Solomon, Soltes and Soysyura, 2014), something that could alter investors' perceptions about cybersecurity risk.[5]

Second, we contribute to the growing literature that explores the role of media in capital markets.[6] Many studies document an association between media coverage and stock market activity (Tetlock, 2007; Fang and Peress, 2009). Other studies establish causality effects of media coverage. For instance, Engelberg and Parsons (2011) use extreme weather events that disrupt or delay the delivery of daily newspapers, as exogenous shocks to identify the causal impact of media coverage on investor trading. Peress (2014) uses newspaper strikes as shocks to information dissemination by the media to demonstrate that media improve stock price efficiency. We add to this literature in several ways: First, instead of broad media news, we focus on information dissemination related to specific exogenous shocks, caused by cyberattacks covered by major newswires. Most importantly, motivated by the psychology literature which demonstrates that exposure to extreme negative events induces feelings that may affect investors' risk perceptions in other unrelated domains (e.g., Lerner and Keltner, 2001), we are interested in potential spillover effects of the information dissemination about cyberattacks in the municipal bond market, rather than

[5] In particular, Maschmeyer, Makridis, and Smeets (2023) compile data on media reporting attached to data breaches and find that zero-day exploits are especially associated with greater coverage, as well as those that target the military or financial sector. These results are consistent with the role of new information in public markets.

[6] Tetlock (2014, 2015) and Ahern and Peress (2022) provide excellent reviews of the relevant theoretical framework and causal effects of media in finance.

the attacked firms. Second, we posit that information dissemination does not affect all investors equally. Building on prior literature, which suggests that the impact of extreme negative events is stronger for investors closer to the incident's location (Kang and Kim, 2008; Kedia and Rajgopal, 2009), we assume that the information dissemination effect is stronger for investors closer to the cyberattack incidence; in fact, we use this idea to identify causal effects. We nonetheless recognize that there is media bias and, therefore, news stories are themselves noisy signals, as Makridis, Maschmeyer and Smeets (2022) point out by showing that not all cybersecurity incidents receive equal attention – "zero-day" exploits and cyber operations on the military and finance sector receive more coverage.

Finally, the study also relates to the literature that explores the direct implications of cyberattacks. Many studies focus on the impact of cyberattacks on the valuations of the attacked firms (Hilary, Segal and Zhang, 2016; Amir, Levi and Livne, 2018; Makridis and Dean, 2018; Tosun, 2021) and how these firms adjust their investment, financial, governance, and risk management policies (Kamiya, Kang, Kim, Milidonis and Stulz, 2021; Ashraf, 2022; Akey, Lewellen, Liskovich and Schiller, 2021; Binfarè, 2020). Other studies, examine the systematic nature of cyberattacks (Crosignani, Macchiavelli, and Silva, 2023) and pricing implications in the stock market (Florackis, Louca, Michaely and Weber, 2023; Jiang, Khanna, and Yang, 2020; Jamilov, Rey, and Tahoun, 2021). Makridis (2021) also found that some data breaches may have positive effects on firm reputation by generating increased publicity, although the most severe breaches were linked with declines. We add to the prior literature that focuses on firm-level and stock market implications, by demonstrating the

repercussions of cyberattacks in the municipal bond market, which allow us to exploit spatial variation in the breach.

3. Data

We combine information from various databases to construct our sample. We use the Privacy Rights Clearing (PRC) house data and Factiva to obtain information about cyberattacks and to verify the data,[7] the U.S. Census of Governments surveys, the U.S. Bureau of Economic Analysis (BEA), the U.S. Bureau of Labor and Statistics (LBS), and the Lightcast to gather county-level data on finances, demographics, economics and job postings, the U.S. Department of the Treasury to get the risk free rate, and the FTSE Russell (formerly known as Mergent Municipal Bond Securities Database) and Thomson Reuters to gather municipal bond data. The Appendix provides a complete list of the variables used in the study and their corresponding data sources.

3.1 Cyberattack data

We use PRC to obtain information about entities that were subject to a data breach, along with a short description of the incident, the date the event was made public, the type of breach, the type of organization, and, if available, the number of records affected. We only analyze data breaches that involve lost personal information by hacking or malware-electronic entry by an outside party. We then use Factiva to manually cross-reference the information from PRC, and to identify cyberattacks that attracted the attention of main global news outlets (e.g., CNBC, Financial Times, Wall

[7] The PRC is a non-profit organization that aims to increase consumers' awareness of privacy protection (for more details, see https://privacyrights.org/).

Street Journal) or are covered in major newswires (e.g., AP, Bloomberg, Reuters). We call such data breaches "major" attacks and use them for our main analyses because information about these attacks was widely disseminated and became available to investors through media channels. Importantly, for most data breaches, PRC provides the coordinates of the location where the attack took place. Using these coordinates and a web-crawling algorithm, we geolocate each data breach to its county. When coordinates are missing, or refer to a dummy location, we manually search and allocate the breach to the county where the headquarters of the entity subject to the attack is located. Our final sample covers the period 2005-2019 and includes 2,493 cyberattacks out of which 293 were categorised as "major" attacks.

Figure 1 presents a heat map of the cumulative number of cyberattacks across counties in 2019. Panel A shows all the cyberattacks, whereas panel B focuses only on major attacks. Areas with dark red color exhibit a greater number of cyberattacks. The map shows that both cyberattacks and major attacks concentrate in parts of the West (e.g., California) and Northeast (e.g., Massachusetts). Interestingly, there is substantial geographic heterogeneity in cyberattacks within states, highlighting the importance of a county-level analysis that preserves the granularity of cyberattack locations. In addition, cyberattacks concentrate in certain counties, which may exhibit different characteristics. Accordingly, to mitigate concerns over a potential selection bias, we perform several robustness tests that consider variability in economic conditions and demographics and show that our results remain qualitatively similar.

Figure 2 presents the frequency of cyberattacks by year. Panel A uses all cyberattacks whereas panel B focuses only on major attacks. The data demonstrate an

upward trend, especially after 2011, consistent with media and policy institute claims that cybersecurity risk has been increasing over time (World Economic Forum, 2021).

3.2 Municipal bond data

We use the Municipal Bonds dataset by FTSE Russell to gather primary market issuance data and municipal bond characteristics. All municipal bonds in FTSE Russell are 4,465,887 issued by 67,408 municipal issuers across different local government units (e.g., counties, cities, school districts etc.). We restrict the sample to bonds issued between January 2012 and December 2021 to respectively mark the beginning of SEC concerns about the digitalization era and its corresponding risks associated with cybersecurity, and the end date for our access to FTSE Russell.[8] We also exclude bonds issued for refunding purposes and hence focus only on new borrowing. Finally, we exclude all bonds issued through unconventional channels such as the U.S. government or under certain schemes, such as the tobacco and tuition agreements, Build America bonds, notes, certificates and taxable bonds. For this sample, we retrieve the key bond characteristics such as 9- and 6- digit issuance and issuer CUSIP, respectively, settlement date, the amount issued, state of the issuing authority, name of the issuer, yield to maturity, tax status, insurance status, call status, credit ratings, coupon rate and maturity date.[9] Bonds with missing information are excluded. Then, using the issuer 6-

[8] In October 2011, the Division of Corporation Finance's provided guidelines regarding disclosure obligations aiming at increasing awareness about timely, comprehensive, and accurate information regarding cybersecurity risk. See https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm for details.

[9] The individual bond-level credit ratings are derived from FTSE Russell database or, replaced by issuer ratings if issuance-level ratings are unavailable. In the case of multiple ratings from S&P, Fitch and Moody's we opt for the lowest. We encode reported ratings into numerically equivalent values ranging from 1 for the lowest to 21 for the highest quality. In the bond-level analysis, we use insured ratings for the insured bonds and underlying ratings for the uninsured bonds.

digit CUSIP and information from Thomson Reuters we locate each bond to the county where is issued and we get the Federal Information Processing Standard (FIPS) codes. Finally, we match the bonds with the PRC data, giving us 313,567 bonds.

Using this sample, we conduct two types of analyses, namely a bond-level analysis and a county-level analysis. Regarding the bond-level analysis, like Cornaggia et al. (2022), we focus only on general obligation (GO) bonds because we lack data on project-specific characteristics that relate to the credit risk of revenue bonds. The sample for this analysis includes 229,628 GO bond issues. Concerning the county-level analysis, we aggregate all the bonds at the county-year-semester level.[10] The sample for this analysis includes 42,360 observations. Panels A and B in Table 1 illustrate our sample construction process whereas Table 2 presents descriptive statistics.

3.3 County financial and demographic data

We compile a database of county finances using the U.S. Census of Governments surveys from legacy files provided by the U.S. Census from 1972-2019. Note that the quinquennial Census surveys include all local government units (e.g., cities, states, counties etc.) whereas the intercensal years include only the larger municipalities. To avoid sampling and selection biases, we linearly interpolate values for all cities, townships and counties between the 5-year census survey years, preserving the data when intercensal years data exist. Interpolation, however, is problematic when entities with missing data are exposed to different economic environments relative to entities

[10] Aggregating bonds at a more granular level reduces the variability of our main variables of interest. Nevertheless, aggregating at the county-year-quarter level our results remain qualitatively similar.

with full data. To alleviate this problem, we require that at least one entity within a county have full data over the period 1972-2019. We then use this entity to interpolate the remaining entities with missing data *within* that county.[11] Our final sample consists of 758 counties and includes 5,956 county-year observations.

We also gather additional county-level moderating and control variables. Specifically, we obtain the number of cyber-related job postings and associated cyber-skill job postings from Lightcast, an organization that scrapes the universe of online job postings and mines the text of the postings.[12] We also use information about owner-occupied housing units and occupied housing units from the Census Bureau, to measure home bias.[13] Finally, from the BEA, we gather the per capita personal income as well as the population, and from the LBS we get the percentage change of employed persons.

4. Empirical results

Our aim is to investigate the impact of information dissemination about cyberattacks on municipalities' access to finance. Specifically, using a bond-level analysis, we inquire whether municipal investors incorporate cybersecurity risk into offer yields. Using a county-level analysis, we further inquire whether the economic costs of cybersecurity risk affect (i) a county's ability to raise capital from the municipal bond market and (ii) a county's activities.

---

[11] Our premise is that entities within a county are affected by more homogeneous economic forces.

[12] Of note, see a closely related article by Bana et al. (2023) who show that data breaches for a given firm are linked with cybersecurity job postings for that firm. We also thank the authors for sharing their data so that we could estimate comparable models at the county-level.

[13] The data are collected in the American Community Survey conducted every year by the Census Bureau. These surveys are sampling over 3.5 million housing units. In our study, we use the average number of owner-occupied housing units and occupied housing units for the 5-year period starting in 2012.

4.1 Cyberattacks and bond yields

Identifying a causal impact of information dissemination about cyberattacks on bond yields is challenging since we cannot observe the counterfactual, namely what would have happened to the municipalities' access to finance if their county had not experienced a cyberattack. To address concerns about omitted variables that affect whether a municipality experiences a data breach, we use a difference-in-differences regression approach. Specifically, we estimate the following model:

$$Y_{i,c,t} = a + \beta \text{ x } ID_{c,t} + X_{i,t} + Z_{c,t-1} + \gamma_{i,t} + \delta_c + \eta_t + \varepsilon_{i,c,t} \qquad (1)$$

where, $Y_{i,c,t}$ is the offer yield of bond *i* in county *c* in month *t*. The county-level variable $ID_{c,t}$ measures information dissemination about cyberattacks. We construct two independent measures which rely on cyberattacks that received public attention in major news outlets and newswires (e.g., major attacks): (*i*) the cumulative number of county-level major attacks (*Major_Attacks*) and (*ii*) the cumulative number of news articles related to the specific county-level major attack (*Major_Attack_News*). Because (i) the media cover high-value news that emphasizes criminality (Smith, McCarthy, McPahil and Augusting, 2001), (ii) the impact of cyberattacks and related news is stronger for investors closer to the incident's location (Kang and Kim, 2008; Kedia and Rajgopal, 2009) and (iii) the municipal bond market is dominated by retail investors, we tentatively expect that increased awareness regarding the emerging risk of cyberattacks has repercussions for the capital market; that is, investors require a reward for bearing cybersecurity risk. $X_{i,t}$ is a vector of bond-level controls whereas $Z_{c,t-1}$ is a vector of lagged county-level characteristics. We include issuer fixed effects ($\gamma_{i,t}$) to

account for unobserved variations across bond issuers and state-year fixed effects (δ_c) to absorb variations across states in a given year and year-month fixed effects (η_t) to control for time effects. Standard errors are clustered at the county level to match the level of aggregation of the main independent variable. Our approach allows for a comparison of the direct cost effect of the information dissemination about cyberattacks on offer yields (β) along two dimensions: over time within the same issuer and across counties with investors exposed to different levels of cyberattack awareness.

Like Cornaggia et al. (2022), bond market control variables, $X_{i,t}$, include the credit rating, coupon rate, bond maturity and its inverse, log bond size, risk-free rate proxied by the corresponding maturity-matched treasury yield, indicator variables for whether the bond is callable and insured. In addition, following Gao, Lee and Murphy (2020), $Z_{c,t-1}$ includes per capita income, county population level and one-year employment growth as controls for location-specific productivity shocks. We also note that the exact timing of public reporting on data breaches is somewhat idiosyncratic since hackers often sit on vulnerabilities and decide to exploit them for reasons that are not necessarily correlated with firm productivity, which is consistent with the evidence on parallel trends that we present later.

Table 3 reports the results. Columns (1) and (2) show positive and significant loadings on the measures of information dissemination about cyberattacks, consistent with a causal effect of cybersecurity risk on municipal offer yields. The coefficient estimates of major attacks imply that a 1% increase leads to an increase in the offering yield of 5.5 bp (p = 0.032). For the average annual issuance amount of $235 million per county, this higher yield translates to $13 million in additional annual interest cost per county. The results for major attack news are qualitatively similar, albeit the economic

effect is smaller. Specifically, a 1% increase leads to an increase in offering yield of 2.3 bp, which translates to $ 5.5 million additional annual interest cost (p=0.040).

Next, we divide our key independent variables into high and low major attack or major attack news percentiles, based on the top 10% of their corresponding distribution. Columns (4) and (5) show that the coefficient estimates monotonically increase from low to high percentiles, and the impact concentrates within the high percentile groups (p=0.030 and p=0.027, respectively). This result is consistent with recent evidence from Makridis (2021) who exploited within-firm variation to assess the impact of data breaches on reputation and brand power. Although the average-sized publicly reported data breach had a positive effect on brand power, the largest and most severe data breaches had a negative effect.

Turning to the control variables, the results are consistent with prior literature. For instance, bonds with a higher rating, with a greater maturity inverse, with a greater issuance amount, insured bonds, and bonds issued in counties with larger populations exhibit, on average, lower yields. In contrast, bonds with a higher coupon, a longer maturity, with a call provision and bonds issued in counties with greater per capita income exhibit, on average, higher yields.

Overall, the results support the view that information dissemination about cyberattacks affects municipal investors who in turn demand compensation for bearing cybersecurity risk. In this sense, the public sector responds to information similarly to the private sector; simply that a municipality, rather than private entity, that suffers a breach does not dull the real economic consequences.

4.2 Robustness tests

In this section, we perform additional tests to ensure our results are robust to methodological issues and endogeneity concerns.

4.2.1 Methodological issues

Recent literature has raised concerns about the validity of estimates relying on standard difference-in-differences models, particularly when the timing of the treatment varies across different groups (e.g., Baker, Larcker and Wang, 2022; Goodman-Bacon, 2021; Sun and Abraham, 2021). In our setting, problem arises as the treatment effects could vary with respect to the time since the first cyberattack in a county. This could induce a "bad comparison" problem, which could potentially bias the estimates. Multiple approaches have been recently proposed for dealing with such a problem with different assumptions in regards to the consideration of the comparison groups, and restrictions about accommodating time-varying covariates, some of which may be critical to control for in our analysis.

Accordingly, as in Cengiz et al., (2019) we examine the robustness of our estimates using a "stacked regression" model. This model combines event-specific datasets comprising of the treated cohort (i.e., the attacked county) and all the other "clean" control observations within the treatment window (i.e., counties have not experienced a cyberattack by the end of our sample period). This approach along with stacked-by-time fixed effects addresses the "bad comparison" problem. Panel A of Table 4 reports the results. Columns (1) and (2) continue to show positive and significant coefficient estimates on our measures of information dissemination about

cyberattacks. Remarkably, the results become stronger, indicating that the bias arising from the "bad comparison" problem undermines the significance of the results.

In addition, we also test the parallel trend assumption which states that in the absence of treatment, the average change in the dependent variable would have been the same for the treatment and control groups. Violation of the parallel trend assumption could potentially indicate endogeneity stemming from reverse causality; in our context, reflected in an increasing trend in offer yields of the attacked counties before the attack. To assess the validity of the parallel trend assumption underlying our difference-in-differences design, we conduct a placebo test using pseudo-cyberattack years during the period preceding the first cyberattack in each county and assess the bond offer yield differential for the treatment and control groups against that in the post-attack period. Like Cengiz et al., (2019) and Mathur et al., (2023), we construct indicators for whether a year $\tau = t \; for \; t \in \{-3, -2, -1, 0, +1, +2, +3, +4\}$ years from the first cyberattack where *t = 0* refers to the year of the attack event. As the timing of the first attack differs across counties the indicator is county-specific and equals 1 if $\tau = t$ periods from the first major cyberattack on any entity headquartered in the county. The pre-and post-first attack indicator variables are then included in the model as the main variables of interest.

Figure 3 presents the coefficient estimates of the main independent variables, namely, the pseudo-attack year indicator dummies over the pre-attack period and the post-attack interaction dummies. We express the estimates as changes relative to year -1 (i.e., the year prior to the treatment), the estimates for which are normalized to 0. The results show no statistically significant pre-trend – that is, the treatment effect is statistically insignificant during the period leading up to the first cyberattack, but

statistically significant and positive in the years after the first cyberattack. These results are consistent with the view that municipal bonds that experienced a data breach in their county would have trended similarly as others in the same state and year that did not.

4.2.2 Other endogeneity concerns

If the characteristics of counties hit by cyberattacks are different relative to counties with no attacks, then the estimated cyberattack effect on bond yields might be biased due to the inability of the model to capture the non-linear effects of the county control variables on bond yields. To mitigate such functional form misspecification biases arising from the non-random selection of the location of the cyberattacks and reduce the impact of confounding in the estimation of causal effects of cyberattacks on bond yields, we use the non-parametric Coarsened Exact Matching (CEM) approach of Iacus, King and Porro (2012). The CEM approach enables us to control for some or all of the potentially confounding influence of county control variables by reducing the imbalance between the treated and control groups. To operationalize the approach, we define counties with cyberattacks as our treated group and counties with no cyberattacks as our control group. We match each treated county to counties with the same characteristics (level of per capita income, population or employment growth) in the control group.

Controlling for and matching on all the county control variables simultaneously is impractical; we would lose approximately 90% of our sample. A closer inspection of the data reveals that the problem is with the population variable, which is intuitive since data breaches are more likely to receive coverage in a larger area with more press. Thus, we binarize population into an indicator for above and below the median population for

a county; this, allows us to include all the county control variables.[14] Panel B of Table 4 reports the results. Columns (1) and (2) show that the results remain qualitatively similar attesting that functional form misspecification bias does not drive our findings.

Next, we investigate whether the positive relation between major attacks and major attack news with bond yields, could endogenously be explained by omitted variables that simultaneously drive major attacks, major attack news and bond yields. One such variable which warrants further attention is the local economic environment, even though our model includes county characteristics as controls. If cyberattacks are more likely to hit counties when economic conditions are deteriorating, then our results could be an artifact of the underlying local economic conditions. In this section, we entertain this alternative explanation as follows: First, we replicate our main analysis after including county characteristic deciles. Hence, the identification of the cyberattacks effect derives from the differences-in-differences framework exploiting *within* county cluster variation based on county characteristics deciles (average per capita income, population and employment growth); this approach provides a high hurdle for identifying the impact of cyberattacks on bond yields. Panel A of Table 5 reports the results. Columns (1) and (2) show that the cyberattack effect remains quantitatively similar and continues to appear positive and statistically significant. Second, we use adjacent counties to identify the effect by exploiting variation within bordering counties. The rationale of this approach is based on the notion that economically comparable counties are geographically close to each other. Consistent with this view, there is a plethora of evidence that emphasize the role of geography in

[14] Note that the results remain qualitatively similar when using CEM for each county characteristic independently, instead of considering simultaneously all the county characteristics.

economic development (e.g., Belenzon and Schankerman, 2013). Panel B of Table 5 reports the results. Like the previous results, Columns (1) and (2) show a positive and statistically significant relation between major attacks and major attack news with bond yields. Overall, the local economic environment is unlikely to explain our results.

4.4 Mechanism: Cybersecurity risk awareness

In this section, we investigate a potential mechanism through which the press coverage of cyberattacks impacts municipal bond yields. In particular, our main results could be driven by information dissemination, which increases awareness about cybersecurity risk. We test this conjecture by considering (i) explicit warnings about cybersecurity risk that bond issuers provide to investors in their official statements, and (ii) investor attention toward cybersecurity risk as evident in SVI data from Google Trends.

4.4.1 Bond issuer awareness

We identify explicit warnings about cybersecurity risk for all the official statements found in the Municipal Securities Rulemaking Board (MSRB). Specifically, we first randomly read 500 official statements and based on the relevant descriptions of cybersecurity risk we compile a list of keywords and/or phrases, such as "cybersecurity", "hacking", "hacker", and "unauthorized access", which directly describe cybersecurity risk. As a caveat, we identify additional keywords, such as "attack", "terrorism", "security", "threat", "intrusions" and "risk", which are sometimes related to cybersecurity risk, but other times are used in other disclosure contexts. To reduce the noise associated with these keywords, we then require the presence of the keyword "cyber" within the same sentence. We then apply these keywords and/or

phrases to all the official statements and identify instances that contain explicit mentions/warnings about cybersecurity risk.

Out of 191,923 bonds we find the corresponding official statement for 185,027 (or 96.41% of the sample).[15] Among them, 9,797 bonds (or 5.29% of the sample) have official statements with explicit warnings about cybersecurity risk. We manually read the relevant discussion aiming (i) to verify that it relates to cybersecurity risk and (ii) to get an intuitive understanding of how issuers differ when discussing cybersecurity risk. Most issuers (8,170 bonds or 83.39% of the bonds with explicit warnings) have extensive discussions, often in separate paragraphs, where they acknowledge that their entities bear cybersecurity risk (or even experienced threats to their data and systems) and highlight security measures to minimize the potential damage caused by cyberattacks. For instance, many issuers (2,142 bonds or 21.86% of the bonds with explicit warnings) use cybersecurity insurance. Most importantly, however, the issuers emphasize the challenge of defending against every risk. Other issuers (1,627 or 16.61% of the bonds with explicit warnings) have limited discussions, often in conjunction with other disclosures, consistent with being less exposed to cybersecurity risk. We rely on variation in issuer discussion, particularly on the presence of a separate paragraph with discussion about cybersecurity risk and classify bonds into those that do or do not have lengthy discussions about cybersecurity risk. Table A.1 of the Appendix provides relevant examples of the language descriptions.

Intuitively, we would expect our major attacks and major attack news variables to positively correlate with the language features of the discussion. Indeed, Panel A of

[15] Note that the sample for this analysis is constrained by data availability. Specifically, MSRB provides official statements up until May, 2020.

Table 6 displays positive correlations with the presence of explicit warnings (*CS mention*), and with lengthy discussions about cybersecurity risk (*CS section*). Furthermore, we also evaluate whether these language features affect the relationship between major attacks and major attack news with bond yields. Panel B of Table 6 reports results using interaction terms of the language features with major attacks and major attack news. Columns (1) and (3) show that our main results are stronger among bonds with explicit warnings in their official statements. Interestingly, these results, as shown in Columns (2) and (4) are driven by explicit warnings accompanied by lengthy discussions about cybersecurity risk. We prudently interpret these results as consistent with the notion that major attacks and major attack news (partly) capture issuer awareness about cybersecurity risk.

4.4.2 Investor awareness

We identify months of abnormal attention toward cybersecurity risk using "search topics" of SVI data from Google Trends during our sample period. Drake, Roulstone and Thornock (2012) and Da, Engelberg and Gao (2011) argue that SVI data are reliable measures of investor attention and demand for information.

Because Google Trends does not provide SVI data at a county level, we cautiously use instead data at a state level. To capture attention more comprehensively, we use relevant topics which exhibit the greatest intensity; these include "hacker", "data breach", "cyberattacks" and "cybercrime". Similar to Florackis et al., (2023) we estimate monthly abnormal SVI by scaling each monthly SVI with the average SVI estimated during the past 12 months to adjust for potential seasonality. For each of the "search topics", we define extreme attention months when the monthly abnormal SVI

is greater than the mean abnormal SVI plus 3 standard deviations, both estimated during the past 12 months (on a rolling basis each month).[16,17] Then, to improve the accuracy of our signal of extreme attention towards cybersecurity risk, we consider extreme attention months only if a month is identified as extreme by at least two of the "search topics". Finally, because attention could have a "memory" effect we cumulate extreme attention months over time for each state.

It is reasonable to anticipate our major attacks and major attack news variables to positively correlate with the state-level investor attention measure (*SVI shock*). Panel A of Table 6 confirms this expectation. Furthermore, the investor attention measure should strengthen the relationship between major attack and major attack news with bond yields. Panel C of Table 6, columns (1) and (2) show that our primary results are stronger among bonds issued in states with at least an extreme attention month. We also generate interaction terms by combining the state-level investor attention measure with our key independent variables, distinguishing between high and low investor attention based on the top 10% of its distribution. As depicted in Columns (3) and (4) the effect is primarily driven by bonds in states with higher attention months. While we interpret these findings cautiously, they are consistent with major attacks and major attack news (partly) reflecting investor awareness about cybersecurity risk.

[16] An exception concerns "data breach" which its distribution exhibits positive skewness and fat tails. To account for this issue, we require that the monthly abnormal SVI is greater than the mean abnormal SVI plus 5 standard deviations.
[17] The results remain qualitative similar using a 6 month rolling window for the parameters estimations.

4.4.3 Additional results

Our evidence suggests that cyberattacks lead to coverage by the press that, in turn, increase bond issuer and investor awareness about cybersecurity risk, resulting in greater yields as a cybersecurity risk premium. To further substantiate this interpretation of the results, in this section, we perform a placebo test whereby information about cyberattacks is unlikely to reach bond issuers and investors. We construct two independent variables: (*i*) the cumulative number of county-level attacks that have not received public attention (*Private_Attacks*) and (*ii*) the cumulative number of attacks reported *only* in smaller, not-so-widely read news outlets (*Non_Major_Attacks*). We then add these variables into our baseline analysis. Panel A of Table 7 presents the results. In line with our previous interpretation that information dissemination about cyberattacks through major news sources is crucial, Columns (1)-(3) show that *Private_Attacks* and *Non-Major_Attacks* neither do relate with bond yields nor do they affect our main results.

Our last analysis breaks down the time period of our analysis into three sub-periods, 2012-2015, 2016-2018, 2019-2021. It is well accepted that awareness about cybersecurity risk has increased over time, in part due to media amplification. In this vein, data breaches began receiving more coverage and attention in part based on regulatory actions following the Equifax breach in 2017.[18] Accordingly, we expect that

[18] Starting in 2016 following several cybersecurity incidents, the U.S. federal government began integrating cybersecurity as a larger pillar in its national and economic security strategy. For example, the Office of Management and Budget (OMB) signed a memorandum to promote its Federal Cybersecurity Strategy. In subsequent years, the OMB began requiring federal agencies to adhere to new regulatory cybersecurity guidance. Although prior guidance had been released as early as 2012 by the National Institute of Standards and Technology (NIST) with their NICE Framework, and revised in 2014, it was not until 2017 that the Department of Homeland Security and NIST began working with the Office of the Secretary of Defense in another iteration. Equifax was subject to $575 million in a settlement with the Federal Trade Commission, Consumer and Financial Protection Bureau, and affected states.

time indicators would moderate the relation between major attack and major attack news with bond yields. We test this idea by re-running the baseline analysis after including time interaction terms with the major attack and major attack news variables. Panel B of Table 7 presents the results. As expected, the effect strengthens over time and is statistically significant only in the two latest sub periods.

4.5 Prevalence of cybersecurity risk

In the previous section, we provide evidence consistent with cyberattack press coverage, through information dissemination, increases awareness about cybersecurity risk something that cause increases in bond yields. Such interpretation, however, also assumes the prevalence of cybersecurity risk. If so, is expected that rational entities would implement proactively security measures to pre-empt cybersecurity threats. One effective defence mechanism is to invest in human capital, aiming to enhance expertise and knowledge about cybersecurity.

Accordingly, we explore the impact of such investment on the relationship between major attacks and major attack news with bond yields. To capture the extent of investments in human capital we use job postings data from Lightcast. We focus on aggregated, at the county level, cyber-related job postings and job posting cyber-related skills per 100,000 persons. Cyber-related job postings are the number of job postings that Lightcast tagged with Cybersecurity-related SOC codes.[19] Cyber-related skills postings are the number of job postings that Lightcast tagged with Cybersecurity-

[19] Examples of SOC job postings codes: 151122: 'Information Security Analysts', 151121: 'Computer Systems Analysts', 151152:'Computer Network Support Specialists', 151141 : 'Database Administrators', 151142 : 'Network and Computer Systems Administrators', 151143 : 'Computer Network Architects'.

related skill clusters.[20] If organizations actively seeking cybersecurity professionals with specialized skills are more vulnerable to cyber threats, then cumulating cyber-related job postings and cyber-related skills postings over time (*Cyber job postings* and *Cyber skills postings*, respectively), could provide a reasonable proxy of time-varying county-level prevalence of cybersecurity risk. We also use these variables to create interaction terms with our key independent variables under high and low prevalence of cybersecurity risk, based on the top 10% of their corresponding distribution.

Table 8 presents results supporting the view that the prevalence of cybersecurity risk plays a crucial role in shaping the relationship between major attacks and major attack news with bond yields. Specifically, Columns 1 to 4 show that most of the major attack and major attack news effects concentrate among counties with higher cyber job postings (p=0.001 and p=0.003, respectively) and higher cyber skills postings (p=0.001 and p=0.002, respectively). These results are consistent with Bana et al. (2023) who show that firms increase their cybersecurity job postings after a data breach, suggesting that firms respond by making human capital investments.

4.6 Which municipal bonds are affected?

In the previous sections, we show that major attacks and major attack news cause increases in bond yields and that both investor awareness about cybersecurity risk and the prevalence of cybersecurity risk likely drive the observed increases in yields. In this section, we explore which bonds are mostly affected by focusing on a major determinant of bond yields: default risk (Wang, Wu, Zhang, 2008; Schwert, 2017).

[20] Examples of skill clusters: 'Cybersecurity', 'Network Security', 'Technical Support', 'Database Administration', 'Data Management', 'Information Security', 'Application Security', 'Internet Security'.

More specifically, the realization of cybersecurity risk, namely cyberattacks, have substantial economic impact on municipalities. For instance, in 2020 alone, ransomware attacks against U.S. government organizations caused about $18.88 billion in downtime due to service disruption and recovery costs[21]. In addition, cybersecurity attacks, and especially the risk of an attack encompass the challenge of allocating capital to prevent future attacks. Overall, cyberattacks are costly and potentially could disrupt the local economy and increase default risk. If so, then awareness of cybersecurity risk should impact riskier bonds. Building on this idea, we exploit two bond characteristics to sharpen the identification of our main results and establish the relationship between cyberattacks and bond yields through the channel of default risk.

First, we consider a bond's insurance status. The cash flows of insured bonds are backed by the insurer in the event of default. As a result, awareness of cybersecurity risk should have a limited impact on the yields of insured bonds. In contrast, uninsured bonds do not have a third-party protection in the event of default, and therefore awareness of cybersecurity risk is more likely to have an important impact on yields. Second, we consider a bond's time to maturity. Long (short) maturity bonds should be more (less) sensitive to potential economic implications arising from cybersecurity attacks, and thus the impact of awareness of cybersecurity risk on bond yields should be more (less) prominent.

We explore these ideas by running variants of the baseline analysis. Panel A of Table 9 presents results after considering each bond characteristic independently. Specifically, in Columns 1 and 2 (3 and 4) we segregate the effect of the variables of

[21] The Economic Impact of Cyber Attacks on Municipalities, white paper, KnowBe4.com

interest into the insured and uninsured status (long and short maturity status), respectively. As expected, the effect of both the cumulative number of attacks and cumulative number of attack news concentrates among uninsured (p=0.036 and p=0.041, respectively) and long maturity (p=0.021 and p=0.028, respectively) bonds. No statistically significant effect exists for insured and short maturity bonds. Interestingly, the difference in the effect between uninsured and insured bonds, shown at the bottom of Panel A, is not statistically significant, but the difference between long and short maturity bonds is statistically significant (p=0.002 and p=0.033, respectively).

In Panel B of Table 9, we consider simultaneously the effects of the insurance and maturity status of the bonds by segregating the effect of the variable of interest into the one by uninsured and long maturity bond status relative to the rest bonds. The results show that the effect concentrates among uninsured and long-maturity bonds (p=0.015 when the main independent variable is the cumulative number of attacks, and p=0.011 when the main independent variable is the cumulative number of attack news). The difference between insured and long-maturity bonds relative to the rest bonds is statistically significant (p=0.023 when the main independent variable is the cumulative number of attacks, and p=0.016 when the main independent variable is the cumulative number of attack news).

Overall, the results suggest that default risk is an important determinant of the awareness of cybersecurity risk effect on bond yields.

4.7 Capital market consequences

4.7.1 Cyberattacks and bond issuance

After establishing the causal effect of cyberattacks on yields, in this section, we consider how cyberattacks affect municipal finance through the quantity of bonds issued. Because awareness of cybersecurity risk increases the cost of financing, municipalities hit by more cyberattacks should face greater challenges in raising capital. We investigate this idea, by employing a difference-in-differences framework, similar to Equation (1). The dependent variable of interest is the aggregate amount of issuance (logged) or the likelihood of issuance (a dummy variable that equals 1 if there is an issuance and zero otherwise), both measured at the county-year-semester level. The main variables of interest remain the cumulative number of cyberattacks and the cumulative number of cyberattack news. Control variables include county-level characteristics (but not bond-level characteristics).

Table 10 presents the results. Panel A shows that cyberattacks cause a significant reduction in the quantity of bonds issued. To provide an indication about the economic significance of our results, a 1% change in the cumulative number of cyberattacks is associated with a 1.17% decrease in the total amount of issuance per county (p=0.003). For the average semi-annual issuance amount of $49 million per county, among counties that have at least one issuance during the semester, this decrease in issuance translates to a $4.9 million reduction in the quantity of bonds issued semi-annually by each county.

Panel B of Table 10 shows that the effect of the cumulative number of cyberattacks on the probability of issuance is negative and significant. A 1% change in the cumulative number of cyberattacks is associated with a 0.32% decrease in the

probability of bond issuance (p=0.030). The effect of the cumulative number of attack news on the probability of issuance, although negative, is not statistically significant. Overall, cyberattacks affect both the amount and the probability of issuance, but they have a statistically and economically stronger impact on the amount of issuance.

Thus far, the results show that awareness of cybersecurity risk increase yields and decreases bond issuance. We interpret these results as consistent with the view that as the supply of capital becomes more costly, this makes it harder for municipalities to raise capital through bond issuance. Beyond such a supply of capital explanation, however, it is plausible that the decrease in bond issuances is also related to a decrease in the demand for capital.[22] Because we cannot rule out the decrease in the demand for capital explanation, in this section, we provide additional results which improve the identification of a supply of capital explanation. Specifically, we exploit differential effects of awareness of cybersecurity risk on bond issuance in relation to the supply of capital-relevant characteristics. If there is no systematic relation between the demand of capital and the supply of capital-relevant characteristics, then significant heterogeneity of the treatment effects would strengthen the view that (at least part of) the results are attributed to the supply of capital.

Building on prior literature, we design the heterogeneity of the treatment effects in relation to investor clientele, particularly on investor preferences for local investing. Dominated by retail investors, the municipal bond markets are heavily affected by a home bias which may arise both from monetary and non-monetary incentives to invest in the local community. For instance, Cornaggia et al. (2021) suggest that homeowners,

[22] Note, however, that such an explanation is difficult to reconcile with the documented increase in yields.

who benefit from public goods such as better schools, hospitals, public infrastructure and services, are more vested in local communities. As a result, they are more willing to invest in local municipal bonds to meet borrowing needs. Likewise, Babina et al. (2021), argue that investors in high state income tax rates and state income exemptions applicable to only home state municipality bonds have more incentives to invest in the local municipal bond market. Broadly, such investor clientele effects segment the municipal bond market. As a result, a supply of capital explanation would predict that the awareness of cybersecurity risk would have greater effects on bond issuances when investor clientele is weakest.

We investigate these ideas, first, by gathering from Census county-level information on the fraction of owner-occupied housing units to occupied housing units. Then, we define counties that belong in the bottom 10% (top 90%) of the distribution as having low (high) home bias. Second, we use information from Babina et al. (2021) about the tax privilege status of states and assume that states with zero (positive) tax privilege provide fewer (more) incentives to invest in the local municipal bond market. Finally, we use high/low home bias and no tax/tax privilege dummy variables to segregate the effect of awareness of cybersecurity risk on bond issuance. Table 11 presents the results. Both monetary and non-monetary incentives to invest in the local community appear to moderate the effect of awareness of cybersecurity risk on bond issuance. More specifically, no tax privilege and low home bias appear to amplify the effect and dampen both the amount of financing and the probability of issuance.

Overall, these results highlight the importance of investors, as the suppliers of capital, for the link between awareness of cybersecurity risk and bond issuances.

4.7.2 Cyberattacks and municipality financials

In this section, we analyze municipal government financial statements to investigate whether awareness of cybersecurity risk affects municipal activities. Given that awareness of cybersecurity risk impedes municipalities' access to capital, we expect municipalities to behave as if they are financially constrained. Specifically, limited access to external financing should force municipalities to exhaust internal financing such as cash holdings. In addition, it should negatively affect municipalities' expenditures, particularly investments, as captured by total capital outlays.

However, not all investments are of equal importance. For instance, investments in health, education and public utilities may be more difficult to reduce, because they are largely inelastic. In contrast, investments for parks, recreation, and public infrastructure such as the creation of highways are easier to delay or even cancel, and thus municipalities should reduce such elastic investments.

We empirically examine these ideas using a difference-in-differences framework, similar to Equation (1). The dependent variables of interest are the cash holdings (logged), total expenditures (logged), capital outlay (logged), capital outlay elastic (logged) and capital outlay inelastic expenditures (logged). The main variables of interest are the cumulative number of cyberattacks (logged) and the cumulative number of cyberattack news (logged). Control variables include county-level characteristics (but not bond-level characteristics).

Panel A of Table 12 presents the results of cash holdings. Column 1 shows that a 1% increase in major attacks lead to 0.133% decrease in cash holdings (p=0.002). For the average county, this represents a decrease of approximately $1.8 million. Similar patterns exist when using the major attack news (see column 2).

Panel B of Table 12 presents the results for total expenditures and capital outlays. Cyberattacks seem to also bear out negative repercussions for the total expenditures of the municipality. Column 1 shows that the coefficient of major attack is negative and significant (p=0.009). For the average county, the coefficient estimate implies that a 1% increase in major attacks results in a decrease in total expenditures of approximately $430 thousands. Interestingly, in Column 3 the decrease in capital expenditures is also reflected in significantly lower capital outlays (p=0.020). For the average county, the coefficient estimate implies a decrease of approximately 190 thousand in capital outlays. Breaking down the capital outlays into elastic and inelastic investments we find that the reduction in total capital outlays is mainly driven by a substantial reduction in inelastic investments. Column 5 shows in about 219 thousand less elastic investment (p=0.000); Inelastic investments are not affected. Columns 2, 4, 6, and 8 display similar patterns for major attack news.

Overall, the results suggest that the awareness of cybersecurity risk hurts municipalities because it lowers their ability to access capital. In response, municipalities utilize cash to support their activities, but not successfully; still, we observe reductions in total expenditures and total capital outlays, which concentrate on more elastic capital outlays.

5. Conclusions

Data breaches and cyberattacks by malicious actors have become major threats over the past decade for not only private sector firms, but also local municipalities and the federal government. Such attacks on the public sector could have large and adverse multipliers on society because of the resulting effects on public spending and provision

of services. Using the municipal bond market setting, we provide new evidence about the impact of information dissemination about cyberattacks, through major newswires, on municipalities' access to finance. Employing a difference-in-differences approach to identify causal effects, we find that county-level cyberattacks and related public news articles cause increases in new offer yields. The result is robust to methodological issues related to our estimation approach and is not driven by selection effects associated with cyberattacks in a county, or from the underlying economic conditions.

We then focus on the mechanism through which cyberattacks influence new offer yields and find that both bond issuers and investors become more aware of cybersecurity. Specifically, we find positive correlations between county-level cyberattacks and explicit warnings about cybersecurity risk in official statements issued by municipalities. In addition, there is a noticeable surge in investor attention toward cybersecurity risk, as reflected in state-level monthly search volume index (SVI) data from Google Trends. Crucially, we find that both explicit warnings and heightened investor attention act as moderating factors in the relationship between cyberattacks and bond yields. Reassuringly, a placebo test with county-level attacks that exhibit limited potential to reach investors does not relate to bond yields; this underscores the importance of the information transmission through press coverage for our results.

We also examine the types of bonds that are most affected, finding that awareness of cybersecurity risk is concentrated among riskier bonds. This mostly affects uninsured bonds, whose cash flows are not backed by a third party, and long-maturity bonds, whose cash flows are more sensitive to potential cybersecurity attack implications.

After establishing the causal effect of major attacks on yields, we focus on the implications arising from the increase in the cost of financing using (i) bond issuance aggregated at the county level and (ii) municipal government financial statements. Our results suggest that municipalities hit by more major attacks face greater difficulties in raising capital. Consistent with a capital supply channel, we find heterogeneous effects related to investor clientele and monetary and non-monetary incentives. Specifically, we find that counties with no tax privilege and a low investor home bias show the largest reductions in both the amount of financing and the probability of issuance.

Municipalities respond to such financing shortages by drawing upon their cash holdings. Despite utilizing more cash, financing shortages affect their investment activities as well. We find a negative relationship between awareness of cybersecurity risk and total capital outlays, driven by declines in their more elastic capital outlays.

Overall, the results highlight the role of information dissemination about cyberattacks in the municipal bond market. Furthermore, awareness about emerging risks, such as cybersecurity, impedes municipalities' access to capital and their ability to provide public services and infrastructure. Our findings emphasize the need for robust cybersecurity measures, not only for safeguarding data but also for preserving the financial health of municipalities across the country. In the age of cyber risks, policymakers, regulators, and municipalities must pay careful attention to the increasing demand for cybersecurity skills, the unseen costs of cyberattacks, and the role of media in shaping investor behaviour.

References

Ahern, K. R., & Peress, J. (2022). The Role of Media in Financial Decision-Making. *Handbook of Financial Decision Making, Editors Gilles Hilary and David McLean, Forthcoming*.

Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2021). Hacking corporate reputations. *Rotman School of Management Working Paper*, (3143740).

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*, 1177-1206.

Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, *97*(2), 1-24.

Babina, T., Jotikasthira, C., Lundblad, C., & Ramadorai, T. (2021). Heterogeneous taxes and limited risk sharing: Evidence from municipal bonds. *The Review of Financial Studies*, *34*(1), 509-568.

Baker, C. A., Larcker, F. D., Wang, C.Y. C. (2022). How much should we trust difference-in-differences estimates?. *Journal of Financial Studies*, *144*(2), 370-395.

Bana, S., Brynjolfsson, E., Wang, J., Steffen, S., Wang, X. (2022). Human Capital Acquisition in Response to Data Breaches. *SSRN working paper*

Barber, B. M., & Odean, T. (2008). All that glitters: The effect of attention and news on the buying behavior of individual and institutional investors. *The Review of Financial Studies*, *21*(2), 785-818.

Belenzon, S., & Schankerman, M. (2013). Spreading the word: Geography, policy, and knowledge spillovers. *Review of Economics and Statistics*, *95*(3), 884-903.

Ben-Rephael, A., Da, Z., & Israelsen, R. D. (2017). It depends on where you search: Institutional investor attention and underreaction to news. *The Review of Financial Studies*, *30*(9), 3009-3047.

Bergstresser, D, & Cohen, R. (2018). Changing patterns in household ownership of municipal debt: Evidence from the 1989-2013 Surveys of Consumer Finances. Brandeis University and MIT Working paper.

Bertrand, M., & Mullainathan, S. (2003). Enjoying the quiet life? Corporate governance and managerial preferences. *Journal of Political Economy*, *111*(5), 1043-1075.

Binfarè, M., (2020). The Real Effects of Operational Risk: Evidence from Data Breaches. SSRN working paper.

Cengiz, D., Dube, A., Lindner, A., Zipperer, B. (2019). The Effect of Minimum Wages on Low-Wage Jobs. *The Quarterly Journal of Economics*, *134*(3), 5532-5557.

Cornaggia, J. N., Cornaggia, K. J., & Israelsen, R. D. (2020). Where the heart is: Information production and the home bias. *Management Science*, *66*(12), 5532-5557.

Cornaggia, K., Hund, J., Nguyen, G., & Ye, Z. (2022). Opioid crisis effects on municipal finance. *The Review of Financial Studies*, *35*(4), 2019-2066.

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432-448.

Da, Z., Engelberg, J., & Gao, P. (2011). In search of attention. *The Journal of Finance*, *66*(5), 1461-1499.

Drake, M.S., Roulstone, D.T., & Thornock, J.R. (2012). Investor Information Demand: Evidence from Google Searches Around Earnings Announcements. Journal of Accounting Research, *50*(4), 1001-1040.

Engelberg, J. E., & Parsons, C. A. (2011). The causal impact of media in financial markets. *the Journal of Finance*, *66*(1), 67-97.

Fang, L., & Peress, J. (2009). Media coverage and the cross-section of stock returns. *The Journal of Finance*, *64*(5), 2023-2052.

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351-407.

Gao, P., Lee, C., & Murphy, D. (2020). Financing dies in darkness? The impact of newspaper closures on public finance. *Journal of Financial Economics*, *135*(2), 445-467.

Goodman – Bacon A., (2021). Difference-in-differences with variation in treatment timing. *Journal of Econometrics*, *225*(2), 254-277.

Grossman, S. J., & Stiglitz, J. E. (1980). On the impossibility of informationally efficient markets. *The American Economic Review*, *70*(3), 393-408.

Harris, L. E., & Piwowar, M. S. (2006). Secondary trading costs in the municipal bond market. *The Journal of Finance*, *61*(3), 1361-1397.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: who cares?. *Georgetown McDonough School of Business Research Paper*, (2852519).

Iacus, S. M., King, G., & Porro, G. (2012). Causal inference without balance checking: Coarsened exact matching. *Political analysis*, *20*(1), 1-24.

Jamilov, R., Rey, H., & Tahoun, A. (2021). *The anatomy of cyber risk* (No. w28906). National Bureau of Economic Research.

Jiang, H., Khanna, N., Yang, Q., & Zhou, J. (2020). The cyber risk premium. *Available at SSRN 3637142*.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749.

Kang, J. K., & Kim, J. M. (2008). The geography of block acquisitions. *The Journal of Finance*, *63*(6), 2817-2858.

Kedia, S., & Rajgopal, S. (2009). Neighborhood matters: The impact of location on broad based stock option plans. *Journal of Financial Economics*, *92*(1), 109-127.

Lerner, J. S., & Keltner, D. (2001). Fear, anger, and risk. *Journal of Personality and Social Psychology*, *81*(1), 146.

Makridis, C. A. (2021). Do Data Breaches Damage Reputation? Evidence from 43 Companies Between 2002 and 2018. Journal of Cybersecurity, 7(1).

Makridis, C. A. and Dean, B. (2018). Measuring the Economic Effects of Data Breaches on Firm Outcomes: Challenges and Opportunities. Journal of Economic and Social Measurement, 43: 59-83.

Makridis, C., Maschmeyer, L., and Smeets, M. (2022). If it Bleeps it Leads? – Media Coverage on Cyber Conflict and Misperception. SSRN working paper.

Mathur, K.N., Ruhm, J.C. (2023). Marijuana legalization and opioid deaths. *Journal of Health Economics, 88, 102728.*

Merton, R. C. (1987). A simple model of capital market equilibrium with incomplete information.

Peress, J. (2014). The media and the diffusion of information in financial markets: Evidence from newspaper strikes. *The Journal of Finance*, *69*(5), 2007-2043.

Schultz, P. (2013). State taxes, limits to arbitrage and differences in municipal bond yields across states. *Unpublished working paper. University of Notre Dame*.

Schwert, M. (2017). Municipal bond liquidity and default risk. *The Journal of Finance*, *72*(4), 1683-1722.

Smith, J., McCarthy, J. D., McPhail, C., & Augustyn, B. (2001). From protest to agenda building: Description bias in media coverage of protest events in Washington, DC. *Social Forces*, *79*(4), 1397-1423.

Solomon, D. H., Soltes, E., & Sosyura, D. (2014). Winners in the spotlight: Media coverage of fund holdings as a driver of flows. *Journal of Financial Economics*, *113*(1), 53-72.

Sun, L., Abraham, S. (2021). Estimating dynamic treatment effects in event studies with heterogeneous treatment effects. *Journal of Econometrics, 225*(2), 175-199.

Tetlock, P. C. (2007). Giving content to investor sentiment: The role of media in the stock market. *The Journal of Finance, 62*(3), 1139-1168.

Tetlock, P. C. (2014). Information transmission in finance. *Annu. Rev. Financ. Econ., 6*(1), 365-384.

Tetlock, P. C. (2015). The role of media in finance. *Handbook of media Economics*, *1*, 701-721.

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795.

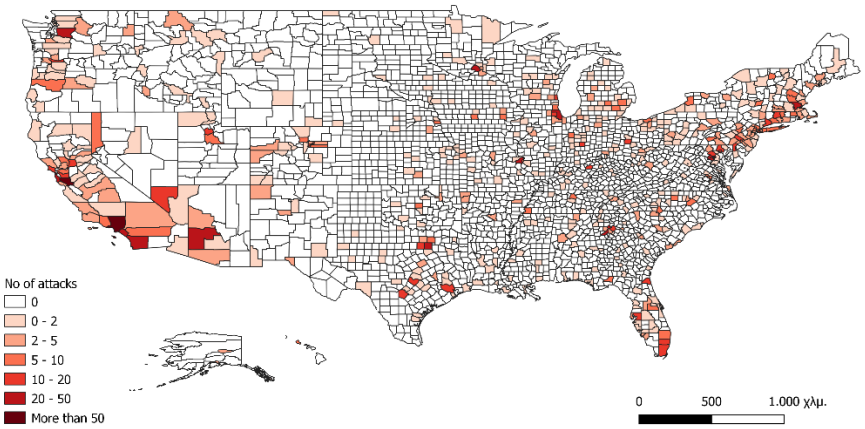
Wang, J., Wu, C., & Zhang, F. X. (2008). Liquidity, default, taxes, and yields on municipal bonds. *Journal of Banking & Finance, 32*(6), 1133-1149.

World Economic Forum. (2021). To make it cybersecure, CEOs must truly get to know their business. https://www.weforum.org/agenda/2021/06/cybersecurity-ceos/

Figure 1: Geographic Distribution of Cyberattacks by County

This figure plots cyberattacks across counties over the period 2005-2019. Cyberattacks are from the privacyrights.org. Panel A plots all cyberattacks whereas Panel B plots cyberattacks covered by major newswires.

Panel A: All cyberattacks



Panel B: Cyberattacks covered by major newswires

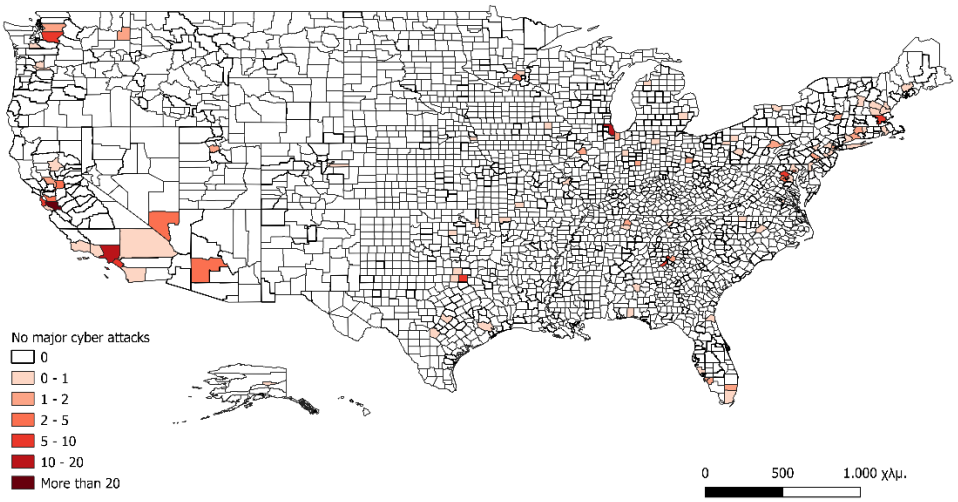


Figure 2: Number of cyberattacks by year

This graph displays the number of cyberattacks by year.

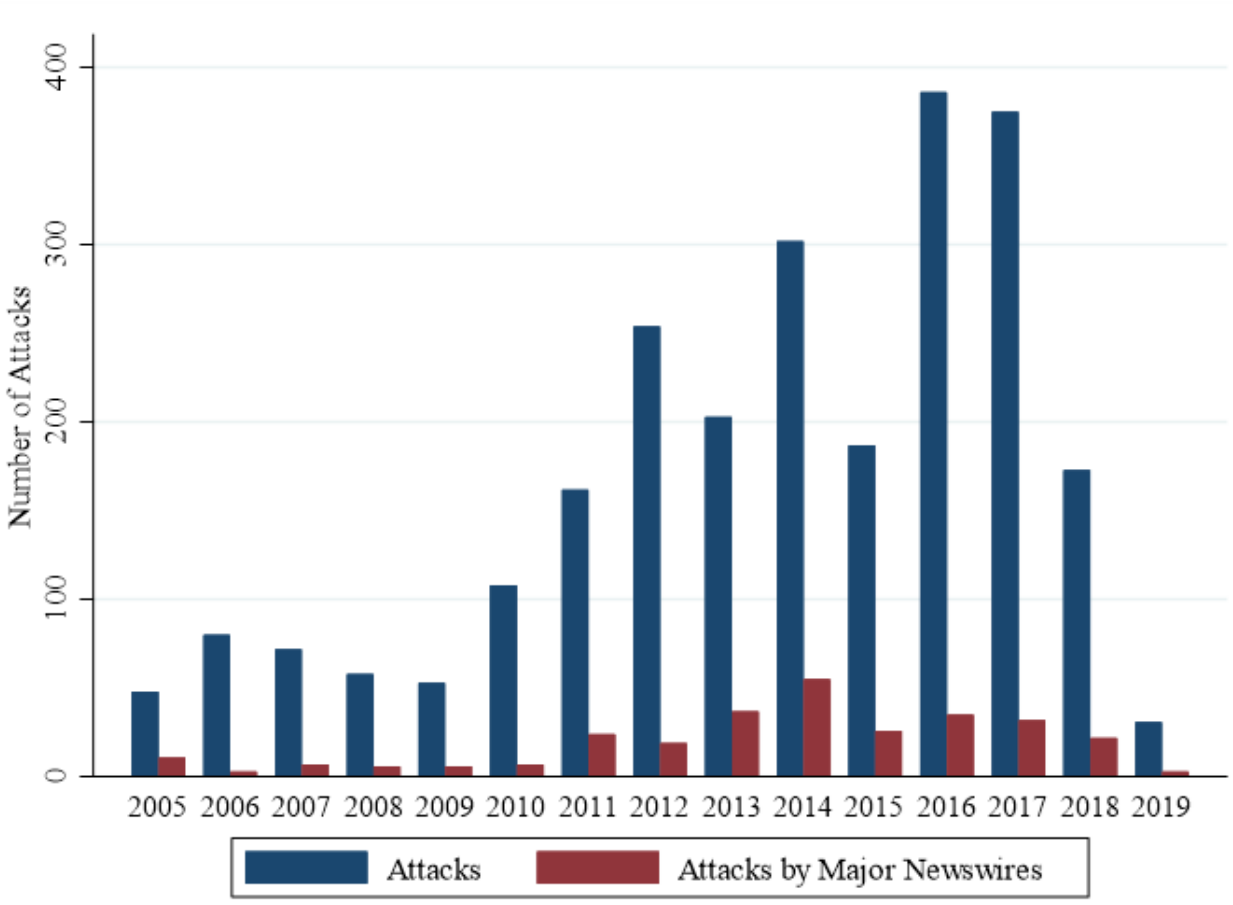


Figure 3: Parallel Trends Test

This graph reports the results of the test for the parallel trend assumption in our difference-in-differences setup. Considering the first attack in each county as the treatment we adopt a placebo test using pseudo-attack dummies in the two years before the attack, and post attack dummies in the years following the first attack. The estimates are expressed as changes relative to year -1 (i.e., the year prior to the treatment), the estimates for which are normalized to 0. Reported are the 95% confidence intervals of their estimated coefficients in the pre-attack and the post attack periods.

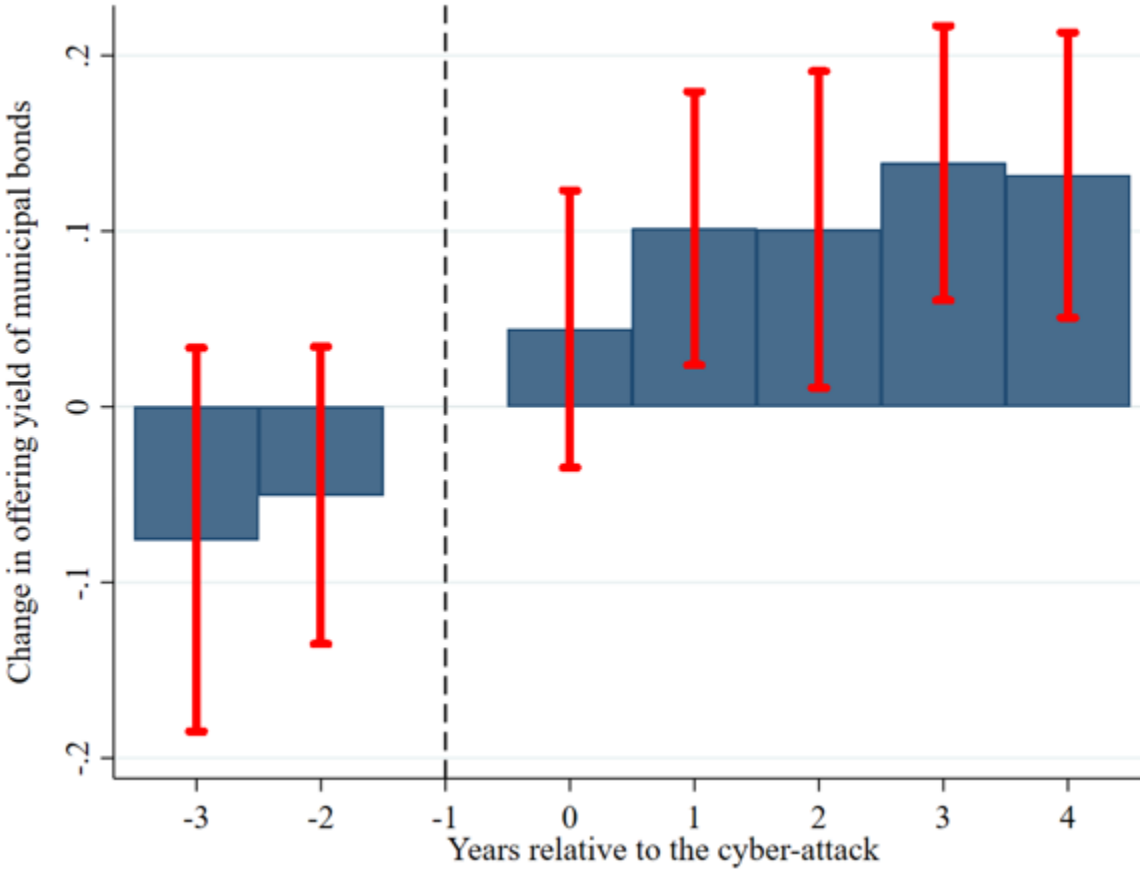


Table 1

Information about Sample Construction

This table provides information about the sample construction. Panel A provides information on the bond-level sample, Panel B provides information on the county-level sample. Panel C provides information on the county finances sample.

Panel A: Sample for Bond-level Analysis

Steps	Data Filter	Observations
1	All bonds in Mergent FISD	4,465,887
2	Bonds issued between Jan 2012 to Dec 2021	1,433,348
3	Bonds issued for new borrowing (i.e., excluding refunding)	706,882
	Bonds issued through conventional channels only (i.e., excluding bonds issued by the U.S. government or under tobacco agreement and tuition agreement, Build America bonds, notes, certificates, and taxable bonds)	608,473
4	Bonds with non-missing offering yield, rating at issuance, coupon rate, or maturity date	450,370
5	Bonds with non-missing county FIPS code	316,151
6	Bonds issued after 2012 matched with PRC Database	313,567
7	GO bonds	229,628

Panel B: Sample for County-level Analysis

Steps	Data Filter	Observations
1	County – Semester observations for the counties that issue bonds during 2012-2021	42,360
2	County – Semester with non-missing economic control variables	42,360

Panel C: Sample for County Finances Analysis

Steps	Data Filter	Observations
1	County – Year observations for the 758 counties that were fully reported in Census during 2012-2019	6,064
2	County – Semester with non-missing economic control variables	5,956

Table 2

Summary Statistics

This table reports summary statistics. The sample covers the period 2012-2021. Panel A reports summary statistics of the bond-level sample. Panel B reports summary statistics for the county-level sample. Panel C reports summary statistics for the county finances sample. All the variables are defined in the Appendix.

Panel A: Bond-level sample

	No Observations	Mean	Std. Dev	P50
Dependent Variable				
Yield (%)	229,628	2.115	1.008	2.090
Main Variables of Interest				
Major_Attacks	229,628	1.547	6.175	0.000
Major_Attacks_News	229,628	16.344	87.870	0.000
Control Variables				
Bond Characteristics				
Rating	229,628	17.184	2.270	17.000
Coupon rate (%)	229,628	3.221	1.174	3.000
Maturity	229,628	10.330	6.642	9.303
Maturity inverse	229,628	0.215	1.241	0.107
Amount (ln)	229,390	13.150	1.396	13.082
Insured	229,628	0.249	0.432	1.000
Call	229,628	0.520	0.500	0.000
Risk free rate (%)	229,441	1.884	0.837	1.980
County Characteristics				
Population	229,628	1,068,950	1,746,795	497,046
Per capita income ($)	229,628	53,449	15,899	50,530
Employment growth (%)	229,628	0.008	0.028	0.011

Panel B: County-level sample

	No Observations	Mean	Std. Dev	P50
Dependent Variable				
Total issuance ($)	45,840	16,305,898	87,453,101	0.000
Main Variables of Interest				
Major_Attacks	45,840	0,066	0,746	0.000
Major_Attacks_News	45,840	1,029	18,804	0.000
Control Variables				
Population	45,840	129,672	375,060	35,489
Per capita income ($)	45,840	42,669	11,950	40,451
Employment growth (%)	45,840	0.001	0.033	0.005

Panel C: County-level sample

	No Observations	Mean	Std. Dev	P50
Dependent Variable				
Total expenditures (th. $)	5,960	1,198,519	4,998,726	384,141
Cash (th. $)	5,960	1,346,956	6,976,280	277,742
Asset (th. $)	5,960	968,360	3,250,311	261,963

Capital Outlay (th. $)	5,690	150,289	608,662	43,249
Capital Outlay Inelastic (th. $)	5,960	58,983	341,953	10,924
Capital Outlay Elastic (th. $)	5,960	91,306	329,574	28,198
Main Variables of Interest				
Major_Attacks	5,960	0,186	1.225	0.000
Major_Attacks_News	5,960	2.838	31.018	0.000
Control Variables				
Population	5,960	324,513	599,909	158,243
Per capita income ($)	5,960	45,005	12,855	42,240
Employment growth (%)	5,960	0.010	0.020	0.010

Table 3

Cyberattacks and Bond Yields

This table reports results from a bond-level analysis using data over the period 2012-2021. The results are estimated using difference-in-differences OLS panel regressions. The dependent variable is the offering yield of municipal GO bonds in the primary market. The main independent variables are the cumulative number of major cyberattacks (Major_Attacks) and the cumulative number of major cyberattack news (Major_Attacks_News), measured at the county level. The variable Major_Attacks_News_High (Low) is a dummy variable that takes the value of 1 if the cumulative number of major cyberattack news is at the top (bottom) 10% (90%) of its distribution. All the remaining bond-specific and county-specific variables are defined in the Appendix. The county-level independent variables are lagged by a period. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

	Offering Yields (%)			
	(1)	**(2)**	**(3)**	**(4)**
Major_Attacks (ln)	0.055**			
	(0.032)			
Major_Attacks_News (ln)		0.024**		
		(0.040)		
Major_Attacks_Low (ln)			0.037	
			(0.206)	
Major_Attacks_High (ln)			0.059**	
			(0.030)	
Major_Attacks_News_Low (ln)				0.016
				(0.246)
Major_Attacks_News_High (ln)				0.027**
				(0.046)
Rating	-0.006*	-0.006*	-0.006*	-0.006*
	(0.064)	(0.061)	(0.063)	(0.059)
Coupon Rate	0.025**	0.025**	0.025**	0.025**
	(0.038)	(0.037)	(0.038)	(0.037)
Maturity	0.097***	0.097***	0.097***	0.097***
	(0.000)	(0.000)	(0.000)	(0.000)
Maturity Inverse	-0.012**	-0.012**	-0.012**	-0.012**
	(0.041)	(0.041)	(0.041)	(0.041)
Amount (ln)	-0.063***	-0.063***	-0.063***	-0.063***
	(0.000)	(0.000)	(0.000)	(0.000)
Insured	-0.119***	-0.120***	-0.119***	-0.120***
	(0.000)	(0.000)	(0.000)	(0.000)
Call	0.306***	0.306***	0.306***	0.306***
	(0.000)	(0.000)	(0.000)	(0.000)
Risk Free	0.001	0.001	0.001	0.001
	(0.540)	(0.539)	(0.539)	(0.533)
Per capita Income (x1000)	0.005***	0.005***	0.006***	0.006***
	(0.009)	(0.006)	(0.009)	(0.009)
Population (x1000)	-0.001***	-0.001***	-0.001***	-0.001***
	(0.003)	(0.003)	(0.005)	(0.007)
Employment Growth	0.105	0.107	0.107	0.106
	(0.723)	(0.717)	(0.719)	(0.719)
Time fixed effects	Yes	Yes	Yes	Yes
Issuer fixed effects	Yes	Yes	Yes	Yes
State X Year fixed effects	Yes	Yes	Yes	Yes
Clustered SE	County	County	County	County
Observations	229,089	229,089	229,089	229,089
R^2	0.884	0.884	0.884	0.884

Table 4

Cyberattacks and Bond Yields: Robustness Check

This table reports results from a bond-level analysis using data over the period 2012-2021. The results are estimated using difference-in-differences OLS regressions. The dependent variable is the offering yield of municipal GO bonds in the primary market. The main independent variables are the cumulative number of cyberattacks (Major_Attacks) and the cumulative number of cyberattack news (Major_Attacks_News), measured at the county level. Panel A reports results from stacked regressions to control for possible bias in staggered 2WFE difference-in-difference OLS estimates. Panel B reports results using difference-in-differences OLS panel regressions after controlling for cyberattack selection using a Coarsened Exact matching (CEM) approach based on county characteristics. All the remaining bond-specific and county-specific variables are defined in the Appendix. The county-level independent variables are lagged by a period. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

Panel A: Stacked regressions

	Offering Yields (%)	
	(1)	**(2)**
Major_Attacks (ln)	0.128***	
	(0.000)	
Major_Attacks_News (ln)		0.057***
		(0.000)
Stacked X Time fixed effects	Yes	Yes
Stacked X Issuer fixed effects	Yes	Yes
State X Year fixed effects	Yes	Yes
Clustered SE	County	County
Observations	7,741,474	7,723,226
R^2	0.887	0.883

Panel B: Coarsened Exact Matching

	Offering Yields (%)	
	(1)	**(2)**
Major_Attacks (ln)	0.046**	
	(0.033)	
Major_Attacks_News (ln)		0.020*
		(0.056)
Time fixed effects	Yes	Yes
Issuer fixed effects	Yes	Yes
State X Year fixed effects	Yes	Yes
Clustered SE	County	County
Observations	202,914	202,914
R^2	0.892	0.892

Table 5

Cyberattacks and Bond Yields: Deteriorating Economic Conditions

This table reports results from a bond-level analysis using data over the period 2012-2021. The results are estimated using difference-in-differences OLS panel regressions. The dependent variable is the offering yield of municipal GO bonds in the primary market. The main independent variables are the cumulative number of cyberattacks (Major_Attacks) and the cumulative number of cyberattack news (Major_Attacks_News), measured at the county level. Panel A reports results relying on within county characteristics variation to identify the effect of cyberattacks on bond yields. County characteristics include the county average per capita income per 100,000, the county population, and the county employment growth. Panel B reports results relying on within adjacent county variation to identify the effect of cyberattacks on bond yields. All the remaining bond-specific and county-specific variables are defined in the Appendix. The county-level independent variables are lagged by a period. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

Panel A: Within county characteristics variation		
	Offering Yields (%)	
	(1)	**(2)**
Major_Attacks (ln)	0.056**	
	(0.012)	
Major_Attacks_News (ln)		0.023**
		(0.034)
Control Variables	Yes	Yes
Time fixed effects	Yes	Yes
Issuer fixed effects	Yes	Yes
State X Year fixed effects	Yes	Yes
Decile fixed effects	Yes	Yes
Adjacent county fixed effects	No	No
Clustered SE	County	County
Observations	229,092	229,092
R^2	0.884	0.884

Panel B: Within adjacent county variation		
	Offering Yields (%)	
	(1)	**(2)**
Major_Attacks (ln)	0.046**	
	(0.043)	
Major_Attacks_News (ln)		0.019*
		(0.056)
Control Variables	Yes	Yes
Time fixed effects	Yes	Yes
Issuer fixed effects	Yes	Yes
State X Year fixed effects	Yes	Yes
Decile fixed effects	No	No
Adjacent county fixed effects	Yes	Yes
Clustered SE	County	County
Observations	1,587,226	1,587,226
R^2	0.885	0.885

Table 6

Cyberattacks and Bond Yields: Mechanism

This table reports results from a bond-level analysis using data over the period 2012-2021. The results are estimated using difference-in-differences OLS regressions. The dependent variable is the offering yield of municipal GO bonds in the primary market. The main independent variables are the cumulative number of major cyberattacks (Major_Attacks) and the cumulative number of major cyberattack news (Major_Attacks_News), measured at the county level. Panel A presents the correlation coefficients between our two main measures of cybersecurity risk and the proxies for issuers awareness derived from MSRB official statements and civilian awareness obtain from SVI of Google Trends. All (No) CS reference(s) is a dummy variable that takes the value of 1(0) if there is any (no) kind of reference to the cybersecurity risk (either separate section or simple mention) in the official statements. CS section is a dummy variable that takes the value of 1 if there is a separate section related to the cybersecurity risk in the official statements. CS mention is a dummy variable that takes the value of 1 if there is any kind of mention related to the cybersecurity risk in the official statements. SVI shocks are the cumulative number of extreme attention months over time for each state. Panel B reports regression results of our main cyberattack independent variables on municipal bond yields moderated by the issuer awareness as proxied by variables extracted from the official documents at the time of bonds' issuance. Panel C reports regression results of our main cyberattack independent variables on municipal bond yields moderated by civilian awareness as proxied by the presence or not of shocks defined using Google trends. .High (Low) SVI shock is dummy variable that take the value of 1(0) if the cumulative number of months identified as extreme attention months is at the top (bottom) 10% (90%) of its distribution The county-level independent variables are lagged by a period. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

Panel A: Correlations		
	Major_Attacks (ln)	Major_Attacks_News (ln)
Issuer Awareness		
i) All CS references	0.031***	0.030***
ii) CS section	0.027***	0.020***
iii) CS mention	0.014***	0.026***
Civilian Awareness		
i) SVI shocks (ln)	0.049***	0.044***

Panel B: Issuer Awareness

	Offering Yields (%)			
	(1)	**(2)**	**(3)**	**(4)**
Major_Attacks (ln) X All CS references	0.093**			
	(0.025)			
Major_Attacks (ln) X No CS reference	0.040	0.039		
	(0.116)	(0.119)		
Major_Attacks News (ln) X All CS references			0.048**	
			(0.026)	
Major_Attacks_News (ln) X No CS reference			0.019*	0.019*
			(0.080)	(0.080)
Major_Attacks (ln) X CS mention		0.055		
		(0.421)		
Major_Attacks_News (ln) X CS mention				0.027
				(0.308)
Major_Attacks (ln) X CS section		0.099**		
		(0.016)		
Major_Attacks_News (ln) X CS section				0.055**
				(0.015)
Control Variables	Yes	Yes	Yes	Yes

Time fixed effects	Yes	Yes	Yes	Yes
Issuer fixed effects	Yes	Yes	Yes	Yes
State X Year fixed effects	Yes	Yes	Yes	Yes
Clustered SE	County	County	County	County
Observations	184,794	184,794	184,794	184,794
R^2	0.870	0.870	0.870	0.870

Panel C: Civilian Awareness

	Offering Yields (%)			
	(1)	**(2)**	**(3)**	**(4)**
Major_Attacks (ln) X No SVI Shock	0.051		0.051	
	(0.149)		(0.149)	
Major_Attacks (ln) X SVI Shock	0.055**			
	(0.042)			
Major_Attacks_News (ln) X No SVI Shock		0.013		0.011
		(0.385)		(0.474)
Major_Attacks_News (ln) X SVI Shock		0.025**		
		(0.036)		
Major_Attacks (ln) X Low SVI Shock			0.042*	
			(0.081)	
Major_Attacks (ln) X High SVI Shock			0.058**	
			(0.035)	
Major_Attacks_News (ln) X Low SVI Shock				0.017
				(0.081)
Major_Attacks_News (ln) X High SVI Shock				0.025**
				(0.029)
Control Variables	Yes	Yes	Yes	Yes
Time fixed effects	Yes	Yes	Yes	Yes
Issuer fixed effects	Yes	Yes	Yes	Yes
State X Year fixed effects	Yes	Yes	Yes	Yes
Clustered SE	County	County	County	County
Observations	229,089	229,089	229,089	229,089
R^2	0.884	0.884	0.884	0.884

Table 7

Cyberattacks and Bond Yields: Additional Results

This table reports results from a bond-level analysis using data over the period 2012-2021. The results are estimated using difference-in-differences OLS panel regressions. The dependent variable is the offering yield of municipal GO bonds in the primary market. The main independent variables are the cumulative number of major cyberattacks (Major_Attacks) and the cumulative number of major cyberattack news (Major_Attacks_News), measured at the county level. Panel A reports results based on the type of attack. The variable Private_Attacks represents the cumulative number of all cyberattacks with no media coverage, measured at the county level. The variable Non_Major_Attacks represents the cumulative number of all cyberattacks with media coverage only on local media, measured at the county level. Panel B reports results using time period dummies. The variable Time Dummy$_{2012\text{-}2015}$ (Time Dummy$_{2016\text{-}2018}$, Time Dummy$_{2019\text{-}2021}$) is a dummy variable that takes the value of one if the bond is issued during the year 2012-2015 (2016-2018, 2019-2021). The county-level independent variables are lagged by a period. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

Panel A: Placebo test

	Offering Yields (%)		
	(1)	**(2)**	**(3)**
Private_Attacks (ln)	-0.001	-0.006	-0.004
	(0.901)	(0.599)	(0.697)
Non_Major_Attacks (ln)	-0.019	0.008	0.010
	(0.365)	(0.695)	(0.646)
Major_Attacks (ln)		0.054**	
		(0.049)	
Major_Attacks_News (ln)			0.023*
			(0.054)
Control Variables	Yes	Yes	Yes
Time fixed effects	Yes	Yes	Yes
Issuer fixed effects	Yes	Yes	Yes
State X Year fixed effects	Yes	Yes	Yes
Clustered SE	County	County	County
Observations	229,089	229,089	229,089
R^2	0.884	0.884	0.884

Panel B: Time effect

	Offering Yields (%)	
	(1)	**(2)**
Major_Attacks (ln) X Time Dummy$_{2012\text{-}2015}$	0.040	
	(0.145)	
Major_Attacks (ln) X Time Dummy$_{2016\text{-}2018}$	0.052*	
	(0.064)	
Major_Attacks (ln) X Time Dummy$_{2019\text{-}2021}$	0.057**	
	(0.034)	
Major_Attacks_News (ln) X Time Dummy$_{2012\text{-}2015}$		0.014
		(0.284)
Major_Attacks_News (ln) X Time Dummy$_{2016\text{-}2018}$		0.025**
		(0.050)
Major_Attacks_News (ln) X Time Dummy$_{2019\text{-}2021}$		0.028**
		(0.025)
Control Variables	Yes	Yes
Time fixed effects	Yes	Yes
Issuer fixed effects	Yes	Yes
State X Year fixed effects	Yes	Yes

Clustered SE	County	County
Observations	229,085	229,085
R^2	0.884	0.884

Table 8

Cyberattacks and Bond Yields: Prevalence of Cybersecurity Risk

This table reports results from a bond-level analysis using data over the period 2012-2021. The results are estimated using difference-in-differences OLS regressions. The dependent variable is the offering yield of municipal GO bonds in the primary market. The main independent variables are the cumulative number of major cyberattacks (Major_Attacks) and the cumulative number of major cyberattack news (Major_Attacks_News), measured at the county level. The variable High (Low) cyber job postings is a dummy variable that take the value of 1 if the number of job postings tagged with Cybersecurity per 100,000 population at the county level is at the top (bottom) 10% (90%) of its distribution. The variable High (Low) cyber skill postings is a dummy variable that take the value of 1 if the number of job postings tagged with Cybersecurity-related skill clusters per 100,000 population at the county level is at the top (bottom) 10% (90%) of its distribution. The county-level independent variables are lagged by a period. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

	Offering Yields (%)			
	(1)	**(2)**	**(3)**	**(4)**
Major_Attacks (ln) X Low cyber job postings	0.041*			
	(0.093)			
Major_Attacks (ln) X High cyber job postings	0.085***			
	(0.001)			
Major_Attacks_News (ln) X Low cyber job postings		0.018		
		(0.122)		
Major_Attacks_News (ln) X High cyber job postings		0.039***		
		(0.003)		
Major_Attacks (ln) X Low cyber skills postings			0.040*	
			(0.099)	
Major_Attacks (ln) X High cyber skills postings			0.088***	
			(0.001)	
Major_Attacks_News (ln) X Low cyber skills postings				0.017
				(0.131)
Major_Attacks_News (ln) X High cyber skills postings				0.040***
				(0.002)
Difference:	0.044***	0.022***	0.046***	0.023***
	(0.00)	(0.001)	(0.000)	(0.000)
Control Variables	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes
Issuer fixed effects	Yes	Yes	Yes	Yes
State X Year fixed effects	Yes	Yes	Yes	Yes
Clustered SE	County	County	County	County
Observations	229,007	229,007	229,007	229,007
R^2	0.884	0.884	0.884	0.884

Table 9

Cyberattacks and Bond Yields: Bond Risk Characteristics

This table reports results from a bond-level analysis using data over the period 2012-2021. The results are estimated using difference-in-differences OLS panel regressions. The dependent variable is the offering yield of municipal GO bonds in the primary market. The main independent variables are the cumulative number of major cyberattacks (Major_Attacks) and the cumulative number of major cyberattack news (Major_Attacks_News), measured at the county level. Panel A reports results based on individual bond characteristics. The variable Insured (Uninsured) is a dummy variable that takes the value of 1 if the bond is insured (uninsured). The variable Short (Long) Maturity is a dummy variable that takes the value of 1 (0) if a bond has a maturity date less (more) than 5 years. Panel B reports results based on combined bond characteristics. The variable Long Maturity X Uninsured (Others) is a dummy variable that takes the value of 1 (0) if a bond has a maturity date more (less) than 5 years and (or) is uninsured (insured). The county-level independent variables are lagged by a period. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

Panel A: Individual bond characteristics				
	Offering Yields (%)			
	(1)	**(2)**	**(3)**	**(4)**
Major_Attacks (ln) X Insured	0.053			
	(0.124)			
Major_Attacks (ln) X Uninsured	0.055**			
	(0.036)			
Major_Attacks_News (ln) X Insured		0.019		
		(0.273)		
Major_Attacks_News (ln) X Uninsured		0.026**		
		(0.041)		
Major_Attacks (ln) X Short Maturity			0.038	
			(0.129)	
Major_Attacks (ln) X Long Maturity			0.061**	
			(0.021)	
Major_Attacks_News (ln) X Short Maturity				0.014
				(0.179)
Major_Attacks_News (ln) X Long Maturity				0.028**
				(0.028)
Difference:	0.002	0.006	0.023***	0.014**
	(0.954)	(0.727)	(0.002)	(0.033)
Control Variables	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes
Issuer fixed effects	Yes	Yes	Yes	Yes
State X Year fixed effects	Yes	Yes	Yes	Yes
Clustered SE	County	County	County	County

Observations	229,092	229,092	229,092	229,092
R^2	0.884	0.884	0.884	0.884

Panel B: Combined bond characteristics

	Offering Yields (%)	
	(1)	**(2)**
Major_Attacks (ln) X Others	0.041*	
	(0.097)	
Major_Attacks (ln) X Long Maturity X Uninsured	0.064**	
	(0.015)	
Major_Attacks_News (ln) X Others		0.015
		(0.169)
Major_Attacks_News (ln) X Long Maturity X Uninsured		0.031***
		(0.011)
Difference:	0.023***	0.016***
	(0.004)	(0.001)
Control Variables	Yes	Yes
Year fixed effects	Yes	Yes
Issuer fixed effects	Yes	Yes
State X Year fixed effects	Yes	Yes
Clustered SE	County	County
Observations	229,085	229,085
R^2	0.884	0.884

Table 10

Cyberattacks and Capital Access: Financing Activity

This table reports results from a bond-level analysis using data over the period 2012-2021. The results are estimated using difference-in-differences OLS panel regressions. Panel A reports results about the amount of financing. The dependent variable is the total issuances of all municipal bonds in the primary market per county and year-semester. Panel B reports results about the probability of issuance. The dependent variable is a dummy variable that takes the value of 1 if the county issued bonds in a certain year-semester, and zero otherwise. The main independent variables are the cumulative number of major cyberattacks (Major_Attacks) and the cumulative number of major cyberattack news (Major_Attacks_News), measured at the county and year-semester level. All the remaining bond-specific and county-specific variables are defined in the Appendix. The county-level independent variables are lagged by a period. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

Panel A: Amount of financing		
	Total Issuance (ln)	
	(1)	**(2)**
Major_Attacks (ln)	-1.172***	
	(0.003)	
Major_Attacks_News (ln)		-0.415*
		(0.060)
Control Variables	Yes	Yes
Time fixed effects	Yes	Yes
County fixed effects	Yes	Yes
State X Year fixed effects	Yes	Yes
Clustered SE	County	County
Observations	45,840	45,840
R^2	0.414	0.414

Panel B: Probability of financing		
	Issuance > 0	
	(1)	**(2)**
Major_Attacks (ln)	--0.319**	
	(0.030)	
Major_Attacks_News (ln)		-0.090
		(0.217)
Control Variables	Yes	Yes
Time fixed effects	Yes	Yes
County fixed effects	Yes	Yes
State X Year fixed effects	Yes	Yes
Clustered SE	County	County
Observations	43,742	43,742

Table 11

Cyberattacks and Bond Issuances: A Supply Effect

This table reports results from a bond-level analysis using data over the period 2012-2021. The results are estimated using difference-in-differences OLS panel regressions. Panel A reports results for the total issuance amount of all municipal bonds in the primary market per county and year - semester. Panel B reports results of the probability of issuance of municipal bonds in the primary market per county and year - semester. The main independent variables are the cumulative number of cyberattacks (Major_Attacks) and the cumulative number of cyberattack news (Major_Attacks_News), measured at the county level. Low (High) home bias is a dummy variable that takes the value of 1 (0) if a county belongs to the bottom (top) 10% (90%) of the distribution of home ownership of all counties. Tax (No Tax) Privilege is a dummy variable that takes the value of 1 (0) if a county belongs (does not belong) to a state with tax privilege based on Babina et al. (2021). All the remaining bond-specific and county-specific variables are defined in the Appendix. The county-level independent variables are lagged by a period. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

Panel A: Amount of financing

	Total Issuance (ln)			
	(1)	**(2)**	**(3)**	**(4)**
Major_Attacks (ln) X Low Home Bias	-1.858***			
	(0.000)			
Major_Attacks (ln) X High Home Bias	-0.142			
	(0.813)			
Major_Attacks_News (ln) X Low Home Bias		-0.855***		
		(0.001)		
Major_Attacks_News (ln) X High Home Bias		0.204		
		(0.489)		
Major_Attacks (ln) X No Tax Privilege			-2.437***	
			(0.000)	
Major_Attacks (ln) X Tax Privilege			-0.713*	
			(0.080)	
Major_Attacks_News (ln) X No Tax Privilege				-1.021***
				(0.000)
Major_Attacks_News (ln) X Tax Privilege				-0.262
				(0.270)
Difference:	-1.716***	-1.059***	-1.723**	-0.758**
	(0.018)	(0.005)	(0.020)	(0.022)
Control Variables	Yes	Yes	Yes	Yes
Time fixed effects	Yes	Yes	Yes	Yes
County fixed effects	Yes	Yes	Yes	Yes
State X Year fixed effects	Yes	Yes	No	No
Clustered SE	County	County	County	County
Observations	45,840	45,840	45,140	45,140
R^2	0.414	0.414	0.404	0.404

Panel B: Probability of Issuance

	Issuance > 0			
	(1)	**(2)**	**(3)**	**(4)**
Major_Attacks (ln) X Low Home Bias	-0.588***			
	(0.004)			
Major_Attacks (ln) X High Home Bias	-0.039			
	(0.840)			
Major_Attacks_News (ln) X Low Home Bias		-0.269***		
		(0.006)		

Major_Attacks_News (ln) X High Home Bias		0.062		
		(0.397)		
Major_Attacks (ln) X No Tax Privilege			-1.096***	
			(0.002)	
Major_Attacks (ln) X Tax Privilege			-0.215	
			(0.124)	
Major_Attacks_News (ln)X No Tax Privilege				-0.513***
				(0.008)
Major_Attacks_News (ln) X Tax Privilege				-0.007
				(0.293)
Difference:	-0.549**	-0.331***	-0.880**	-0.443**
	(0.039)	(0.005)	(0.020)	(0.029)
Control Variables	Yes	Yes	Yes	Yes
Time fixed effects	Yes	Yes	Yes	Yes
County fixed effects	Yes	Yes	Yes	Yes
State X Year fixed effects	Yes	Yes	No	No
Clustered SE	County	County	County	County
Observations	43,180	43,180	43,180	43,180

Table 12

Implications for Municipalities

This table reports the results from a difference-in-differences OLS panel regression of county financing variables on the cumulative number of cyberattacks and the cumulative number of cyberattack news, measured at the county level, and control variables. All the dependent variables are in logged values. The sample period is 2012-2019. The unit of analysis is county year. All the independent variables are lagged by a period. The main independent variables are the cumulative number of cyberattacks (Major_Attacks (ln)) and the cumulative number of cyberattack news (Major_Attacks_News (ln)), measured at the county level. Panel A reports results for Cash (ln) and the Cash relative to the Total Assets as proxied for financially constrained counties. Panel B reports results for Total Expenditures (ln), Capital Outlay (ln), Capital Outlay Inelastic (ln) and Capital Outlay Elastic (ln), as proxied for financially constrained counties. County and year fixed-effects are included in all specifications. Standard errors are clustered by county and t-statistics are reported in parentheses. $*p < 0.1$, $**p < 0.05$, $***p < 0.01$.

Panel A: Financial Constraints		
	Cash (Ln)	
	(1)	**(2)**
Major_Attacks (ln)	-0.133***	
	(0.002)	
Major_Attacks_News (ln)		-0.047***
		(0.007)
Population (x10.000)	0.004	0.003
	(0.306)	(0.481)
Per capita Income (x10.000)	0.058*	0.061*
	(0.097)	(0.082)
Employment Growth	-0.586*	-0.576*
	(0.094)	(0.100)
Year fixed effects	Yes	Yes
County fixed effects	Yes	Yes
Clustered SE	County	County
Observations	5,938	5,938
R2	0.954	0.953

Panel B: Implication of Financial Constraints

	Total Expenditure (Ln)		Capital Outlay (Ln)		Capital Outlay Inelastic (Ln)		Capital Outlay Elastic (Ln)	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Major_Attacks (ln)	-0.036***		-0.127**		0.001		-0.240***	
	(0.009)		(0.020)		(0.099)		(0.000)	
Major_Attacks_News (ln)		-0.014***		-0.051**		0.001		-0.105***
		(0.008)		(0.025)		(0.978)		(0.000)
Population (x10.000)	0.008***	0.009***	0.010**	0.009**	0.017**	0.017**	0.012**	0.011**
	(0.000)	(0.000)	(0.018)	(0.030)	(0.035)	(0.039)	(0.010)	(0.021)
Percapita Income (x10.000)	0.048***	0.048***	0.074**	0.072**	0.100*	0.100*	0.100*	0.097*
	(0.009)	(0.010)	(0.037)	(0.042)	(0.071)	(0.075)	(0.023)	(0.026)
Employment Growth	-0.556*	-0.554*	-0.321	0.314	0.616	0.616	-0.481	-0.471
	(0.085)	(0.086)	(0.620)	(0.627)	(0.450)	(0.450)	(0.569)	(0.577)
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
County fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Clustered SE	County	County	County	County	County	County	County	County
Observations	5,938	5,938	5,929	5,929	5,927	5,927	5,848	5,848
R2	0.990	0.990	0.911	0.911	0.873	0.873	0.877	0.877

APPENDIX

Variable Definition

Dependent Variables

Offering Yield: Yield to maturity at the time of issuance of G.O. Municipal Bonds, based on the coupon and any discount or premium to par value at the time of sale. This variable is created using Mergent Municipal Bond Securities Database.

Total Issuance (Ln): The natural logarithm of the total amount of municipal bonds' issuance per county in a year-semester basis. This variable is created using Mergent Municipal Bond Securities Database.

Probability of Issuance: The probability of issuance a municipal bond per county in a year - semester basis. This variable is created using Mergent Municipal Bond Securities Database.

Cash: The natural logarithm of the total cash holdings per county in a year basis. This variable is created using Census Bureau Database.

Total Expenditure (Ln): The natural logarithm of the total expenditures per county in a year basis. This variable is created using Census Bureau Database.

Capital Outlay Inelastic (Elastic) (Ln): The natural logarithm of the capital outlays for health, education and utilities (other) purposes per county in a year basis. This variable is created using Census Bureau Database.

Main Independent Variables

Major Attacks (ln): The natural logarithm of the cumulative number of cyberattacks covered by major newswires, measured at the county level. This variable is created using Privacy Rights Clearinghouse (PRC) and Factiva.

Major Attacks High (Low) (ln): A dummy variable that takes the value of 1 if the cumulative number of major cyberattacks is at the top (bottom) 10% (90%) of its distribution. This variable is created using Privacy Rights Clearinghouse (PRC) and Factiva.

Major Attacks News (ln): The natural logarithm of the cumulative number of cyberattack news articles covered by major newswires, measured at the county level. This variable is created using Privacy Rights Clearinghouse (PRC) and Factiva.

Major Attacks News High (Low) (ln): A dummy variable that takes the value of 1 if the cumulative number of major cyberattack news is at the top (bottom) 10% (90%) of its distribution. This variable is created using Privacy Rights Clearinghouse (PRC) and Factiva.

All (No) CS reference(s): A dummy variable that takes the value of 1(0) if there is any (no) kind of reference to the cybersecurity risk (either separate section or simple mention) in the official statements. This variable is created using the official statements provided by Municipal Securities Rulemaking Board (MSRB).

CS section: A dummy variable that takes the value of 1 if there is a separate section related to the cybersecurity risk in the official statements. This variable is created using the official statements provided by Municipal Securities Rulemaking Board (MSRB).

CS mention: A dummy variable that takes the value of 1 if there is any kind of mention related to the cybersecurity risk in the official statements. This variable is created using the official statements provided by Municipal Securities Rulemaking Board (MSRB).

SVI shocks (ln): The natural logarithm of the cumulative number of extreme attention months over time for each state. Relevant topics which exhibit the greatest intensity are used; these include "hacker", "data breach", "cyberattacks" and "cybercrime". We estimate monthly abnormal SVI by scaling each monthly SVI with the average SVI estimated during the past 12 months to adjust for potential seasonality. For each of the "search topics", we define extreme attention months when the monthly abnormal SVI is greater than the mean abnormal SVI plus 3 standard deviations, both estimated during the past 12 months (on a rolling basis each month). We

consider extreme attention months only if a month is identified as extreme by at least two of the "search topics". This variable is created using Google Trends.

High (Low) SVI shock: A dummy variable that take the value of 1(0) if the cumulative number of months identified as extreme attention months is at the top (bottom) 10% (90%) of its distribution. This variable is created using Google Trends.

Private Attacks (ln): The natural logarithm of the cumulative number of all cyberattacks with no media coverage, measured at the county level. This variable is created using Privacy Rights Clearinghouse (PRC) and Factiva.

Non-Major Attacks (ln): The natural logarithm of the cumulative number of all cyberattacks with media coverage only on local media, measured at the county level. This variable is created using Privacy Rights Clearinghouse (PRC) and Factiva.

Time Dummy2012-2015: A dummy variable that takes the value of one if the bond is issued during the year 2012-2015. This variable is created using Mergent Municipal Bond Securities Database.

Time Dummy2016-2018: A dummy variable that takes the value of one if the bond is issued during the year 2016-2018. This variable is created using Mergent Municipal Bond Securities Database.

Time Dummy2019-2021: A dummy variable that takes the value of one if the bond is issued during the year 2019-2021. This variable is created using Mergent Municipal Bond Securities Database.

High (Low) cyber job postings: A dummy variable that take the value of 1 (0) if the number of job postings tagged with Cybersecurity per 100,000 population at the county level is at the top (bottom) 10% (90%) of its distribution. This variable is created using Lightcast Data.

High (Low) cyber skill postings: A dummy variable that take the value of 1 (0) if the number of job postings tagged with Cybersecurity-related skill clusters per 100,000 population at the county level is at the top (bottom) 10% (90%) of its distribution. This variable is created using Lightcast Data.

Insured (Uninsured): The variable Insured (Uninsured) is a dummy variable that takes the value of 1 if the bond is insured (uninsured). This variable is created using Mergent Municipal Bond Securities Database.

Short (Long) Maturity: The Short (Long) Maturity is a dummy variable that takes the value of 1 (0) if a bond has a maturity date less (more) than 5 years. This variable is created using Mergent Municipal Bond Securities Database.

Low (High) home bias: Low (High) home bias is a dummy variable that takes the value of 1 (0) if a county belongs to the bottom (top) 10% (90%) of the distribution of home ownership of all counties. This variable is created using Census Database.

Low (High) privilege: High (Low) Privilege is a dummy variable that takes the value of 1 (0) if a county belongs to a state with tax privilege. This variable is created using information from Babina et al. (2021).

Bond – level control variables

Coupon Rate: The current applicable annual interest rate of a bond. This variable is created using Mergent Municipal Bond Securities Database.

Maturity: The time period in years before the bond issuer must repay the original bond value to the bond holder. The variable is created by deducting the maturity date from the settlement date and divided by 360 days, using Mergent Municipal Bond Securities Database.

Maturity Inverse: The arithmetical inverse of the Maturity.

Rating: The long-term rating assigned to each individual bond (or the issuer if the bond rating is missing) by the three main credit rating agencies. We convert character ratings into numeric ratings with 21 corresponding to the highest credit quality and 1 the lowest. When rating information is available from multiple rating agencies, we

employ the harshest rating. In analysis of bond yields, we use the insured rating for insured bonds and the underlying rating for uninsured bond s.

Amount: The principal amount of the maturity's original offering that the issuer has to pay back to the bond holder at the maturity date. This variable is created using Mergent Municipal Bond Securities Database.

Insured: A dummy variable that takes the value of one if the bond is insured and zero otherwise. This variable is created using Mergent Municipal Bond Securities Database.

Call: A dummy variable that takes the value of one if the bond is callable and zero otherwise. This variable is created using Mergent Municipal Bond Securities Database.

Risk Free: The interest rate of the corresponding Treasury bond at the settlement date. This variable is created using U.S. Department of the Treasury.

County– level control variables

Population: The number of civilians measured at county-level in a year basis. This variable is created using data from the Census Bureau.

Per capita Personal Income: The personal income of a specific area, earned by or on behalf of all of the persons who live in the area in a year basis. This measure of income is calculated as the personal income of the residents of a given area divided by the resident population of the area. This variable is created using data from the U.S. Bureau of Economic Analysis (BEA).

Employment Growth: The percentage change of employed person per county in a year basis. The variable is created using per county data from the U.S. Bureau of Labor Statistics (LBS).

Table A.1
Excerpts from Cybersecurity-risk of MSRB official statements

Panel A: Excerpts for Cybersecurity Sections		
Municipality	**Bond Series**	**Text from Cybersecurity Risk Disclosures**
PERRIS UNION HIGH SCHOOL DISTRICT (Riverside County, California)	General Obligation Bonds, Series A/2019	The District, like many other public and private entities, relies on computer and other digital networks and systems to conduct its operations. As a recipient and provider of personal, private or other electronic sensitive information, the District is potentially subject to multiple cyber threats including, but not limited to, hacking, viruses, malware and other attacks on computer and other sensitive digital networks and systems. Entities or individuals may attempt to gain unauthorized access to the District's systems for the purposes of misappropriating assets or information or causing operational disruption or damage. The District has never had a major cyber breach that resulted in a financial loss. No assurance can be given that the District's efforts to manage cyber threats and attacks will, in all cases, be successful or that any such attack will not materially impact the operations or finances of the District. The District is also reliant on other entities and service providers, such as the County Treasurer, for the levy and collection of special taxes and ad valorem property taxes, and various trustees, fiscal agents and dissemination agents. No assurance can be given that the District may not be affected by cyber threats and attacks against other entities or service providers in a manner which may affect the Bond Owners, e.g., systems related to the timeliness of payments to Bond Owners or compliance with disclosure filings pursuant to the Continuing Disclosure Certificate.
COUNTY OF NEW HANOVER, NORTH CAROLINA	General Obligation School Bonds, Series 2020	The County, like many other large public and private entities, relies on a large and complex technology environment to conduct its operations and faces multiple cybersecurity threats involving, but not limited to, hacking, phishing viruses, malware and other attacks on its computing and other digital networks and systems (collectively, "Systems Technology"). As a recipient and provider of personal, private, or sensitive information, the County may be the target of cybersecurity incidents that could result in adverse consequences to the County and its Systems Technology, requiring a response action to mitigate the consequences. Cybersecurity incidents could result from unintentional events, or from deliberate attacks by unauthorized entities or individuals attempting to gain access to the County's Systems Technology for the purposes of misappropriating assets or information or causing operational disruption and damage. To mitigate the risk of business operations impact and/or damage from cybersecurity incidents or cyber-attacks, the County invests in multiple forms of cybersecurity and operational safeguards. While the County's cybersecurity and operational safeguards are periodically tested, no assurances can be given by the County that such measures will ensure against other cybersecurity threats and attacks. Cybersecurity breaches

		could cause material disruption to the County's finances or operations. The costs of remedying any such damage or obtaining insurance related thereto, or protecting against future attacks could be substantial and insurance (if any can be obtained), may not be adequate to cover such losses or other consequential County costs and expenses. Further, cybersecurity breaches could expose the County to material litigation and other legal risks, which could cause the County to incur material costs related to such legal claims or proceedings.

Panel B: Excerpts for Cybersecurity Mentions

Municipality	Bond Series	Text from Cybersecurity Risk Disclosures
TOWN OF WAKE FOREST, NORTH CAROLINA	General Obligation Public Improvement Bonds, Series 2018A	Power Agency and its Participants, including the Town, are facing a changing and challenging electric utility industry. The most significant of those changes and challenges being increased competition, in both wholesale and retail markets and the greater use of alternative and renewable energy resources and demand response. In addition, the industry faces challenges due to greater public and regulatory agency awareness and concern regarding the siting and construction of generation and transmiseion facilitics; the need to improve security against natural and new manmade threats to physical and cyher security, including protection of critical infrastructure facilities from damage or attack; and concerns about employee safety and environmental factors such air, water quality and land use.
CITY AND COUNTY OF SAN FRANCISCO	General obligation Bonds, Series 2016F	Seismic events, wildfires, tsunamis, and other natural or man-made events such as cybersecurity breaches may damage City infrastructure and adversely impact the City's ability to provide municipal services.

Panel C: Excerpts for Cybersecurity Insurance and Actions		
Municipality	**Bond Series**	**Text from Cybersecurity Risk Disclosures**
WILLIAMSON COUNTY, TENNESSEE	General Obligation public improvement and school bonds, Series 2019	The County utilizes various computer systems and network technology to perform many of its vital operations. Such operations often include the storage and transmission of sensitive information, and as a result, the County may be the target of cyberattacks attempting to gain access to such information. In addition to intentional attacks, information breaches may occur due to unintentional employee error. A successful cyberattack or unintentional breach may require the expenditure of an unknown amount of money or time to resolve, substantially interrupt municipal services and operations and subject the County to legal action. The County has no knowledge of, nor historical record of any successful cyber-security breach or related attack. Attempted cyber-security attacks, whether anonymous or targeted, occur on a periodic frequency that is not uncommon to organizations or agencies of similar characteristics. To mitigate against such risks, the County has instituted various policies and procedures to protect its network infrastructure, including a cyber-security training requirement for certain departments, as well as general cyber-security training and awareness for all employees. The County also maintains insurance against cyber-security incidents, up to a coverage maximum of $5,000,000. Despite the County's measures to safeguard its network infrastructure, there are no guarantees that such measures will be successful.
STATE OF UTAH	General Obligation School Bonds, Series 2020	Cybersecurity incidents could result from unintentional events, or from deliberate attacks by unauthorized entities or individuals attempting to gain access to the State's systems technology for the purposes of misappropriating assets or information or causing operational disruption and damage. To mitigate the risk of business operations impact and/or damage by cybersecurity incidents or cyberattacks, the State invests in multiple forms of cybersecurity and operational safeguards including: (i) $7.8 million annual budget for security operations and security privacy and compliance; (ii) a Chief Information Security Officer reporting directly to the State's Chief Information Officer; (iii) a security team of 18 employees; (iv) a self–assessment every two years in cooperation with the Department of Homeland Security using National Institute of Standards and Technology standards; (v) compliance audits regularly performed by the Internal Revenue Service, Federal Bureau of Investigation, Medicaid and Medicare, and the Office of the Inspector General; and (vi) a Cyber Center that provides a central location for multiple agencies to share intelligence and tactics, and respond to events in a coordinated fashion. In addition, the State has a $10 million liability insurance policy regarding cybersecurity.

Panel D: Excerpts for Cyber Events		
Municipality	**Bond Series**	**Text from Cybersecurity Risk Disclosures**
CITY OF LAWTON, OKLAHOMA	General Obligation School Bonds, Series 2019	On August 22, 2017, the City experienced a malware event that infiltrated and crippled its digital systems. Upon discovery of the infiltration, the City, in conjunction with its information technology staff and third-party vendors, followed standard virus protocol and identified the software virus. The City conducted digital scans and cleaned servers and computers, with the initial focus being to restore all network and application systems. On August 24, 2017, the City engaged outside assistance and support from the State of Oklahoma's Cyber Security Team. The State's Cyber Security Team working alongside the State's internet service provider formed a strategic plan to (i) determine the impact on the City, (ii) provide additional support to the City in its investigation of the infiltration, (iii) rebuild network infrastructure, (iv) implement additional security measures, and (v) fully recover from the incident. In the days following the infiltration, the City began its remediation efforts and the recovery process, which included (i) quarantining infected portions of the City network, (ii) reimaging machines, (iii) configuring a new firewall, (iv) securing user accounts, (v) reviewing and filtering all network traffic, (vi) restoring backup images of virtualized and physical servers, (vii) reloading work stations, (viii) restoring drives, and (ix) carrying out data transactions for nearly 900 computers throughout the City. Following many months, each of the foregoing was accomplished and the City's digital systems have fully recovered from the infiltration. To date, recovery and remediation costs to the City have totaled more than $100,000 in services and equipment.
SAN FELIPE DEL RIO CONSOLIDATED INDEPENDENT SCHOLL DISTRICT	Unlimited tax school building bonds, series 2020	The District was the victim of a cyber attack that resulted in the loss of District funds and the delinquent payment of principal and interest due certain of the District's outstanding bonds. On February 14, 2020, the District submitted payment for on such debt service. On the February 18 bondholder payment date, the paying agent for such debt obligations notified the District that it had not received the payments. Upon immediate investigation, the District determined that due to a phishing email scam, the payments were erroneously sent to a fraudulent bank account and, therefore, were not received by the paying agent as intended. The District immediately a notified and solicited the assistance of law enforcement, including local authorities and the U.S. Federal Bureau of Investigation, as well as its depository bank to assist with the matter and the investigation. The District held a special meeting of its Board of Trustees (the "Board"),which convened on February 24, 2020 and authorized the appropriation from its 1ts general fund reserves to make the delinquent debt service payments. On February 26, 2020, the District delivered a check to the paying agent which will fully pay the balance due for the affected principal and interest payments due February 18, 2020. The District has made a material event filing in relation to the delinquent debt service payment for the

affected series of outstanding obligations. The investigation by the District and law enforcement agencies into the cyber phishing incident is ongoing. The District intends to use all available legal means to recoup the stolen funds. There is no assurance at this time that any amount will be able to be recovered.

As a result of this incident, the District, with the assistance of its advisors, is currently preparing additional safeguards and will provide training to the entire finance department as soon as possible while eliminating the use of wiring for outgoing payments in the interim. The District will also be reviewing its internal accounting controls and information technology systems to establish strategies, procedures and protocols to mitigate future risk and exposure to cybersecurity incidents in the future.